UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"ANALISIS OPERATIVO DE LAN SWITCHES EN ATM"

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

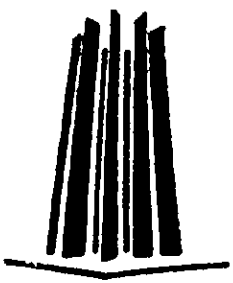
INGENIERO MECANICO ELECTRICISTA

(ELECTRICO ELECTRONICO)

P R E S E N T A N :

PEREZ GONZALEZ LUIS ALFONSO

RODRIGUEZ JUAREZ ESTEBAN



DIRECTOR DE TESIS: ING. DAVID BERNARDO ESTOPIER BERMUDEZ

SAN JUAN DE ARAGON ESTADO DE MEXICO 1998.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

A mis padres, que han hecho innumerables sacrificios para que yo tuviera la oportunidad de realizar lo que ahora esta a un paso de concluirse ; sin el apoyo de mi ellos, esto hubiera sido doblemente difícil. Mamá, gracias.

A mis hermanos Damian, Erick, Jose Apolinar y Martín ; este logro es también de ellos.

A mi hermana Alejandra, esperando que esto sea un incentivo para hacer más cosas en menos tiempo.

A toda mi familia, por su comprensión y cariño.

A Luis Alfonzo, por darme la oportunidad de desarrollar este trabajo de tesis juntos, su perseverancia y dedicación fueron de vital importancia para llevar a buen termino este trabajo.

A mi novia Janet, por que se que siempre da lo mejor de ella para lograr sus metas, y una de ellas es dedicar su tesis a su familia.

A la UNAM, a la DGSCA y a la DTD por haberme dado la oportunidad de hacer mi carrera y ahora de ejercerla, gracias... siempre doy mi mejor esfuerzo.

Dedico este trabajo.

A Dios por darme la oportunidad de vivir

A mis padres Luis Alfonso y María Eugenia por todo el amor que me han brindado durante todos estos años y que siempre han sacrificado su propio bienestar por el mío.

A mi hermano Ramón por toda su ayuda ya que en ester trabajo ha sido una parte muy importante.

A toda la familia por su apoyo desinteresado.

Al Ing. Victor Villalba por su paciencia y por la gran oportunidad que me brindo.

A mis compañeros de Lucent por su invaluable soporte a lo largo de estos meses.

Y a todas aquellas personas que en algun momento me han tendido la mano para salir adelante.

Queremos agradecer muy especialmente a nuestro asesor,

Ing. David B. Estopier Bermúdez

Por todo el apoyo que siempre nos ha brindado, tanto en sus clases como en la realización de este trabajo.

También agradecemos a los profesores,

Ing. Raúl Barrón
Ing. Juan Gastaldi
Ing. Silvia Vega
Ing. Narciso Acevedo

Por todas las facilidades que nos dieron para la realización de este trabajo.

MUCHAS GRACIAS

INDICE

INTRODUCCION

La comunicación de datos se ha convertido en una parte fundamental de la computación. Las redes globales reúnen datos sobre temas diversos, como las condiciones atmosféricas, la producción de cosechas y el tráfico aéreo. Algunos establecen listas de correo electrónico para poder compartir información de interés común. Las personas que tienen pasatiempos intercambian programas para sus computadoras temporales. En el mundo científico, las redes de datos son esenciales pues permiten a los científicos enviar programas y datos hacia supercomputadoras remotas para su procesamiento, recuperar los resultados e intercambiar información con sus colegas.

Por desgracia, la mayor parte de las redes son entidades independientes, establecidas para satisfacer las necesidades de un solo grupo. Los usuarios escogen una tecnología de hardware apropiada a sus problemas de comunicación. De manera más importante, es imposible construir una red universal desde una sola tecnología de hardware, debido a que ninguna red satisface todas las necesidades de uso. Algunos usuarios necesitan una red de alta velocidad para conectar máquinas, pero dichas redes no se pueden expandir para abarcar grandes distancias. Otros establecen una red de menor velocidad que conecta máquinas que se encuentran a miles de kilómetros de distancia.

Durante los pasados 15 años, ha evolucionado una nueva tecnología que hace posible interconectar muchas redes físicas diferentes y hacerlas funcionar como una unidad coordinada. Esta tecnología, llamada internetworking, unifica diferentes tecnologías de hardware subyacentes al proporcionar un conjunto de normas de comunicación y una forma de interconectar redes heterogéneas. La tecnología de red de redes oculta los detalles del hardware de red y permite que las computadoras se comuniquen en forma independiente de sus conexiones físicas de red.

Actualmente estamos en el punto definitivo en la evolución del mercado de internetworking y el gran ambiente de negocios que lo envuelve. El tremendo crecimiento en las capacidades de las tecnologías de computo en la pasada década

ha creado la oportunidad para muchos negocios de literalmente reinventarse ellos mismos usando los nuevos modos de operación, nuevos tipos de productos y los nuevos tipos de servicios. Tenemos en efecto, ir más allá usando la tecnología para automatizar nuestras practicas actuales de negocios para permitir redefinir un nuevo arreglo de practicas de negocios.

El estado actual de la red puede ser atribuido a un tópico particular: la inhabilidad de soportar el uso de nuevas aplicaciones que ya emergieron o que están prontas a emerger en el mercado. El impacto de estas nuevas aplicaciones puede ser sentido en muchas áreas, tales como la ausencia de ancho de banda entre estaciones, demasiado retardo entre los sistemas de redes y la ausencia de manejabilidad de la infraestructura de red completa.

La ausencia de ancho de banda puede ser notado fácilmente con nuevas aplicaciones que involucran transferencias de archivos masivamente a través de la red.

Otro punto importante es la característica de retardo. Muchas de las aplicaciones recientes involucran el uso de tecnologías interactivas . Esto va más allá que vídeo bidireccional e incluye aplicaciones tales como aplicaciones isosincronas, diseño interactivo y herramientas de modelado y pizarrones interactivos. Donde aparecen las aplicaciones interactivas, el retraso en la red (latencia) se convierte en un punto importante. Alta latencia en la red se puede traducir en vídeo de baja calidad o ausencia de sincronización audio/vídeo.

Además de todo lo anterior la administración de la red es un problema muy grande actualmente. Conforme las redes han crecido, el equipo de red se ha complicado técnicamente. Estos dispositivos a menudo llevan un encabezado para administración muy caro, requiriendo un gran número de personas de soporte técnico para supervisión y reparación de fallas.

La reacción inicial para algunos de estos problemas sería incrementar el ancho de banda en la red. Esto generalmente resuelve solo parcialmente el problema y puede incrementar otros problemas. Mucho se ha dicho acerca del desarrollo y la implementación de tecnologías LAN de 100Mbps tales como FastEthernet y FDDI/CDDI. Y mientras estas tecnologías ciertamente otorgan ancho de banda adicional, desafortunadamente no proporcionan solución al problema de la administración y al del retraso.

Tomado en cuenta todos los factores anteriores hemos creado este documento para realzar, algo que consideramos un punto muy importante en el mercado de la redes; el surgimiento de la tecnología de LAN switch. Adicionalmente, hemos tratado de hacer énfasis la importancia de esta tecnología y los puntos significativos de arquitectura que existen en este tipo de productos. Explicamos, en términos básicos, las características únicas de algunas tecnologías LAN y de switch.

Este documento no evalúa o recomienda productos específicos o arquitecturas especificas, debido a que esto sería practicamente imposible, dado que la mayoría de las arquitecturas de los vendedores esta todavía emergiendo y su aplicación variara considerablemente entre diferentes usuarios. En este punto no existe un LAN switch, una arquitectura o fabricante que vaya a resolver todos los problemas en el mercado de las redes. Hemos tratado, no obstante, de proporcionar los fundamentos adecuados para la comprensión de los LAN switches, que aún se encuentran un poco malentendidos o complejos para muchos usuarios.

CAPITULO 1

INTRODUCCION A LAS REDES

1.1 Concepto de Red

Debido al tremendo impacto de las computadoras y las redes de computadoras en nuestra sociedad durante la pasada década, este período en la historia se ha sido llamado "era de la información" . La productividad y conveniencia de organizaciones e individuos han sido unidos por estas herramientas revolucionarias . Difícilmente un día transcurre sin el uso de una red de computadoras para llevar a cabo negocios personales o profesionales. Esta tendencia esta acelerándose conforme las empresas y los hogares descubren el poder de las computadoras y las redes de comunicaciones. Las transacciones de cada día en las tiendas departamentales, bancos, hoteles y otros negocios son dependientes de las redes de computadoras. Esta Era de la Información es igualmente dependiente de las computadoras y sus redes.

Qué es una red de computadoras? Se han aceptado muchas definiciones en la industria. Posiblemente la más simple es: Un número de computadoras (y usualmente terminales) interconectadas por una o más rutas de transmisión. La ruta de transmisión es muy a menudo la línea telefónica, debido a su conveniencia y presencia universal. Las redes existen para llevar a cabo una sola tarea: la transferencia e intercambio de datos entre las computadoras y terminales . Este intercambio de datos proporcionado por la mayoría de los servicios basados en computadoras que a menudo tomamos para nuestro uso diario, tales como las máquinas de los cajeros bancarios, terminales de punto de venta, dispositivos de revisión y verificación e incluso la guía de naves espaciales.

Las redes de computadoras proporcionan muchas ventajas para las empresas y los particulares.

- Las organizaciones modernas están ampliamente dispersas, con oficinas localizadas en diversas partes de la nación o del mundo . Muchas de las computadoras y terminales localizadas en los lugares necesarios para el intercambio de información y datos diarios. Una red proporciona los medios

para el intercambio de datos entre estas computadoras y para hacer programas y datos disponibles para toda la gente de la organización.

- La interconexión de computadoras permite compartir los recursos de las máquinas. Por ejemplo, si una computadora se satura con demasiado trabajo en un sitio, el trabajo puede ser cargado a través de las rutas de la red hacia otra computadora en la red. Tal carga compartida permite una mejor utilización de los recursos.

- La red también proporciona la crítica tarea función de respaldo. En el caso de que una computadora falle, su contraparte puede asumir sus funciones y carga de trabajo. La capacidad de respaldo es especialmente importante en actividades tales como el control de tráfico aéreo. En el caso de que una computadora falle, las computadoras de respaldo rápidamente asumirán el control de las operaciones sin poner en peligro los vuelos.

- El uso de una red permite un ambiente de trabajo muy flexible. Los empleados pueden trabajar en casa usando terminales enlazadas a través de la red a una computadora en su oficina. Muchos empleados ahora transportan sus terminales y PC´s portátiles en viajes y se enlazan a sus redes a través de los teléfonos de los hoteles. Otros empleados viajan a oficinas remotas y usan el teléfono y las redes para transmitir y recibir ventas urgentes, oficios administrativos, e investigan datos de los computadoras en las oficinas centrales de su compañía.

La era de la información es nombrada correctamente, para nuestra sociedad ahora esta era de la información implica una reducción de los costos en la producción de satisfactores así como para mejorar la calidad de vida. Los sistemas de comunicación y las redes proporcionan un rápido intercambio de información en computadoras existentes a través de todo el mundo.

En resumen, podemos decir que la habilidad para intercambiar información es una buena razón para interconectarse. Los usuarios de computadoras no trabajan aislados y necesitarán obtener ciertos benéficios proporcionados por un sistema central. Este incluye la habilidad de intercambiar mensajes con otros usuarios, la habilidad de accesar a datos desde muchas fuentes en la preparación de un documento o para un análisis, y la oportunidad de que muchos usuarios puedan compartir información en un archivo común.

Para apreciar la segunda razón, consideremos que conforme el costo del equipo de procesamiento de datos tiende a la baja, el costo de equipo electromecánico esencial, como lo son el almacenamiento a granel y las impresores en línea, permanece alto. En el pasado, con una facilidad centralizada de procesamiento de datos, estos dispositivos podían ser conectados directamente al host central. Actualmente con la potencia de computo dispersa, estos dispositivos deben ser compartidos

1.2 Clasificación de Redes

Las redes de computadoras se pueden clasificar en dos grandes grupos:

- Redes de Área local (LAN del inglés Local Área Network)
- Redes de Área Ancha (WAN del inglés Wide Área Network).

Una red de área local, LAN, es una red de computadoras confinada a un área limitada, tal como una habitación, un edificio o un campus universitario. Una red de área ancha WAN, por otra parte, es una red de computadoras que se extiende a mayores distancias.

Típicamente, las LAN´s se comunican a velocidades más altas que las WAN´s. Las WAN´s que se comunican vía satélite o por enlace de microondas pueden alcanzar similares velocidades, pero la mayoría dellas utilizan el lento método de la comunicación por red telefónica.

Si analizamos más profundamente esta clasificación nos llevara a una clasificación más especifica. Las corporaciones actualmente necesitan una LAN para permitir el trabajo entre redes entre dispositivos de cómputo distribuidos; y las LAN´s de las corporaciones han excedido los límites de su existencia local y ahora necesitan conectividad a través de una área geográfica más grande. Las LAN´s dispersas ahora tienen la opción de un rango de conectividad proveniente de circuitos dedicados al transporte vía una red de área amplia o metropolitana conmutada. De tal forma que la decisión de servicios y tecnología va más allá del simple costo.

Así una clasificación de redes podría ser:

- LAN - Local Area Network - Menos de 3Km de distancia; proporciona usualmente conectividad dentro de un edificio.

- MAN - Metropolitan Area Network - Menos de 50Km; proporciona conectividad regional típicamente dentro de un campus o una área geográfica pequeña.

- WAN - Wide Area Network - No tiene límites en distancia; proporciona conectividad nacional.

- GAN - Global Area Network - No tiene límites de distancia; proporciona conectividad global.

El tráfico de datos esta creciendo actualmente en rangos cercanos al 30% anual, además los puentes, ruteadores y compuertas hacen crecer las LAN's de una forma más fácil y más barata. La necesidad de expandir las redes locales usualmente cae en una o más de las siguientes categorías:
- Incremento de las velocidades en el trabajo de redes LAN
- Altas velocidades de transmisión
- Aplicaciones funcionales
- Capacidades de acceso a dominios
- Intercambio de facilidades entre áreas locales hacia áreas amplias
- Bajos costos de instalación
- Facilidad de expansión.

Tratemos de profundizar un poco más en las diferencias y aplicaciones de cada red. Si hablamos de redes WAN estas consisten de DSE's (switching computers) conectadas juntas por canales asignados (por ejemplo, 56 kbits/s por línea). Cada DSE usa un protocolo responsable de enrutar los datos y también de proporcionar soporte para las computadoras de los usuarios finales y las terminales enlazadas a el. Las funciones de soporte del DTE son llamadas a menudo PAD (ensamblado/desensamblado del paquete). El DSE actúa como el PAD hacia adentro y hacia afuera de la red para los DTE's. El centro de control de la red (NCC) es responsable por la eficiencia de las operaciones de la red. En algunos sistemas, el NCC controla el ruteo llevado a cabo en los DSE's.

En la Figura (1.1) note la diversidad de conexiones de los DTE'S dentro del PAD/switch:

A) Un usuario es conectado al DSE a través de un protocolo asíncrono, con discado de líneas analógicas hacia un puerto dedicado DSE (un puerto reservado exclusivamente para el usuario).

B) Un usuario con un procesador front-end es conectado al DSE a través de un protocolo síncrono, con líneas digitales dedicadas de 56 kbits/s usando unidades de servicio de datos (DSUs).

C) Una terminal de usuario asíncrona (o computadora persona es conectada a el DSE, con líneas analógicas hacia un puerto del DSE no dedicado.

D) Un usuario tiene premisas en un DSE dedicado, conectada la red usando líneas digitales (56kbits/s) de red privada con unidades de servicio de datos (DSUs).

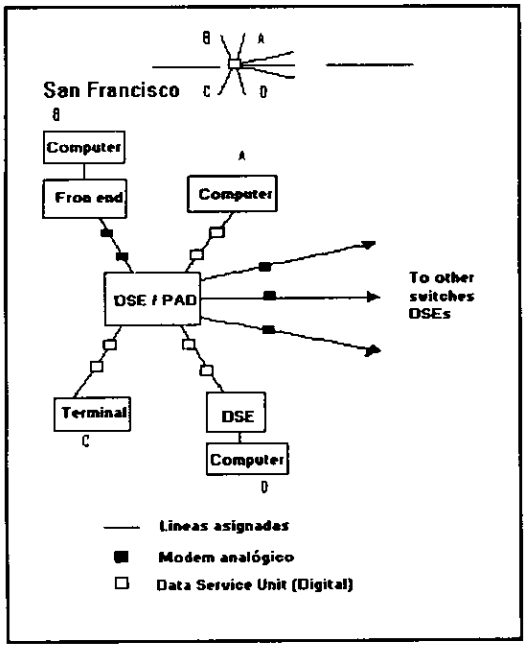


Figura. 1.1 PAD Switch.

Esta es una topología típica de una WAN que nos permite hablar ahora acerca de las redes orientadas a conexión y a no conexión.

Los DTE's de la Figura se comunican a través del DSE/PAD de la red por una de estas dos técnicas. La primera técnica es la orientada a la conexión; la segunda es a no conexión. Como se ilustra en la Figura 1.2, una red orientada a

conexión es en la cual no existe inicialmente conexión entre los DTE´S y la red. La conexión en la red entre dos DTE´S está en un estado ocioso. Para comunicarse, las computadoras y las terminales, dentro de una red orientada a conexión, deben establecer una comunicación, que es llamada " saludo".

Una vez que esta conexión es establecida, el estado de transferencia de datos es enterado; los datos son intercambiados a través de un protocolo preestablecido. Los DTE´S llevarán a cabo subsecuentemente una liberación de la conexión, después de lo cual regresarán al estado ocioso.

La red orientada a conexión proporciona un monto substancial de cuidado para los datos del usuario. El procedimiento requiere reconocimientos específicos de que la conexión se estableció o la red informará al DTE solicitante si la conexión no se estableció. El control del flujo (para asegurarse que todos los datos llegaron correctamente, en orden, y no saturaron los DSE´s y DTE´S en varias partes de la red), también se requiere por parte de la red. El chequeo de errores se realiza tan bien como la recuperación de errores. Las redes orientadas a conexión mantienen una falta de conocimiento global y continua de todas las sesiones de DTE a DTE, y tratan de asegurar que los datos del usuario no están perdidos en la red. El cuidado proporcionado por este tipo de red requiere una considerable supervisión debido a las muchas funciones que soporta.

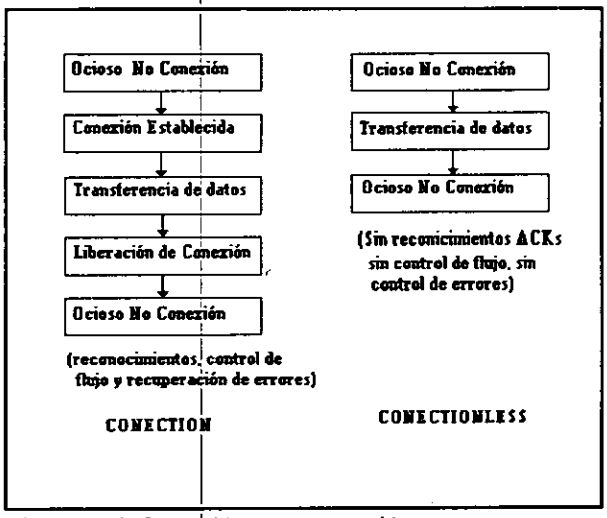


Figura. 1.2 Conexión y no conexión.

La red de no conexión (también llamada datagrama) va directamente de un estado ocioso (las dos DTE's no están conectadas lógicamente entre ellas) a un modo de transferencia de datos, seguido diractamente por la condición de estado ocioso. La mayor diferencia es la ausencia de una fase de establecimiento de conexión y una fase de liberación de la conexión. Por otra parte, una red de no conexión no tiene reconocimientos en la red, control de flujo, o recuperación de errores, no obstante estos servicios son proporcionados en un fundamento de enlace-por-enlace. Obviamente, las redes de no conexión involucran menos supervisión.

Las redes orientadas a conexión son comparadas a menudo conceptualmente al sistema telefónico (tanto líneas asignadas o de discado). El que llama sabe cuando se hace una conexión porque el esta llamando a alguien al otro lado de la línea. La red orientada a no conexión es comparada a poner en el correo una carta. La carta se envía a través del sistema postal asumiendose que llegará a su destino. La carta usualmente llega sin problemas, pero el que la envía nunca lo sabrá. La oficina postal no regresa nada para decirle al emisor que la carta llegó. El receptor de la carta debe iniciar una respuesta indicando su aceptación, usualmente en forma de otra carta, lo cual, en términos de comunicaciones, es llamado protocolo de alto nivel.

Las redes orientadas a conexión han dominado las redes de computadoras de área amplia (WAN) debido a la naturaleza inherente de propensión a errores de la línea telefónica. Consecuentemente, los sistemas usando el canal telefónico realizan muchas funciones para asegurar que la integridad de los datos se mantenga entre los dispositivos de comunicación. Una red de no conexión tiene más sentido con una red de área local (LAN). Un canal de LAN esta usualmente asociado con un edificio de pertenencia privada. Basada en está tecnología, un LAN es mucho menos sujeta a errores. Es relativamente inusual que los datos se distorsionen en un canal LAN. Un canal típico telefónico conectado con una WAN experimenta rangos de error de entre 1:1E-3 a 1:1E-5 un bit en error en cada 1000 ó 100000 bits transmitidos. Una LAN típicamente experimenta un rango de error de aproximadamente 1:10. El rango de error entre las LAN y las WAN difiere por mucha magnitud. Consecuentemente, puede tener poco sentido en una red de no conexión (especialmente si es una LAN) llevar a cabo las costosas opciones de supervisión o control de flujo, control de errores y recuperación; debido a la poca ocurrencia de un error no es necesario el gasto de evitarlos.

Dicho todo lo anterior, podemos clasificar más particularmente a las redes de computadoras. En la Figura 1.3 se muestra una clasificación más exacta y con más datos.

◆ **WAN**

Las redes de área amplia han sido consideradas tradicionalmente aquellas que cubren una gran área geográfica, como ya vimos anteriormente. Recientemente las WAN's han proporcionado solo modesta capacidad a los subscriptores. Para la conexión de datos, tanto para redes de conmutación de paquetes como para redes de conmutación de circuitos por medio de un modem, los rangos de datos de 9600 bps o incluso menos han sido comunes. Los subscriptores pueden ahora obtener rangos más altos, con un servicio conocido como T1, el cual opera a 1.544 Mbps. El descubrimiento más importante que ha mejorado el desempeño de las WAN ha sido la implementación de la Red Digital de Servicio Integrados (ISDN), que proporciona los servicios de conmutación de circuitos y conmutación de paquetes a velocidades arriba de los 1.544 Mbps (2.048 Mbps en Europa). La interface básica de usuario para ISDN es la conmutación de circuitos usando par torcido.

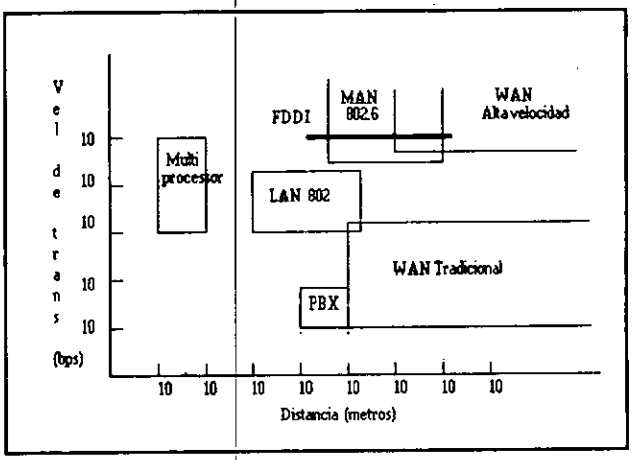


Figura. 1.3 Clasificación de redes.

La continua mejora en las aplicaciones de la fibra óptica ha llevado a la estandarización de velocidades mucho más altas para las WAN's, y podemos esperar que estos servicios estén ampliamente disponibles en los próximos años. Estas WAN's de alta velocidad proporcionan al usuario conexiones entre los díez

y los cien Mbps. El esfuerzo más importante se refiere a la estandarización de una red digital de servicios integrados de banda ancha (B-ISDN) que usa relevadores de celdas más que conmutación de circuitos.

- **LAN**

Para describirlas utilizaremos la definición oficial del IEEE(90). Las LAN's descritas aquí se distinguen de otros tipos de redes de datos en que estas se optimizan para tamaños moderados de áreas geográficas tales como edificios, almacenes o campus. La LAN IEEE802 es una red de comunicaciones de medio compartido que envía información para todas las estaciones receptoras. Como consecuencia, no es inherente que proporcione privacia: La LAN activa estaciones para comunicar directamente usando un medio físico común en una base punto a punto sin que se requiera un nodo de conmutación intermedio. La red es generalmente usada, operada implementada por una sola organización. Esto en contraste a una WAN que da facilidades de interconexión en diferentes partes de un país o se usa como de utilidad pública.

- **MAN**

Como su nombre lo sugiere, una MAN ocupa todo lo que esta entre las LAN's y las WAN's. El interés en las MAN se ha dado debido al resultado de reconocer que las técnicas tradicionales de punto a punto y conmutación usadas en WAN's pueden ser inadecuadas para las crecientes necesidades de las organizaciones. Mientras la banda ancha de ISDN con relevadores de celdas, promete un amplio rango para necesidades de alta velocidad, existe un requerimiento actual para redes públicas y privadas que proporcionen alta capacidad a bajo costo sobre una gran área. El uso de medios compartidos a alta velocidad de los estándares de las LAN proporciona un gran número de benéficos que pueden realizarse a escala metropolitana.

Después de muchos años de investigación en las MAN's. Un gran número de alternativas han sido exploradas y rechazadas. Una aproximación ha emergido que ha sido recibida con gran soporte por parte de los proveedores y los usuarios y que ha sido estandarizada por el comité IEEE 802 como el IEEE 802.6.

Una MAN es la optimización de una LAN para una gran área geográfica, desde varias cuadras a una ciudad completa. Como las redes locales, las MAN's también dependen de los canales de comunicación de rangos de datos de moderados a altos. Rangos de error y retrasos pueden ser ligeramente más altos que los obtenidos en una LAN. Una LAN puede ser poseída y operada por una

sola organización, pero también lo puede ser por muchos individuos y organizaciones. Las MAN´s también pueden ser propiedad, y ser operadas por entidades públicas. Estas redes a menudo proporcionan medios para el trabajo entre redes locales. No obstante es requerido para todas las LAN´s, la capacidad para llevar trabajo entre redes de dispositivos que integren voz y datos es considerada una función opcional para una LAN. Asimismo, tales capacidades en una red que cubre una área metropolitana son funciones opcionales de una MAN.

RED	Vel. de transmisión	Distancia
Red de Area Local (IEEE 802)	1-20 Mbps	< 25 km
FDDI	100 Mbps	< 200 km
Red de Area Metropolitana (IEEE 802.6)	30 Mbps-1 Gps	< 160 km
WAN Tradicional	10 kbps-1.5 Mbps	ilimitada
WAN de Alta Velocidad	50 Mbps-1 Gps	ilimitada

Fig. 1.4 Características de LANs, MANs y WANs

1.3 Topología de Redes

Los principales factores de tecnología que determinan la naturaleza de una LAN o MAN son:

- Topología
- Medio de Transmisión
- Técnica de control de acceso al medio

Todos estos elementos determinan de gran manera el tipo de datos que pueden ser transmitidos , la velocidad y eficiencia de las comunicaciones, e incluso el tipo de aplicaciones que puede soportar la red.

El término Topología, en el contexto de una red de comunicaciones, se refiere al modo en que las terminales de la red se interconectan. Una topología se define por el trazo de los enlaces y conmutación de los elementos, y determina las trayectorias de los datos que pueden ser usadas entre cualquier par de estaciones.

Una pregunta que podríamos hacernos es, ¿Porqué es necesario una serie de enlaces entre las estaciones, en vez de conectar directamente dos dispositivos? , así no necesitaríamos una red con dispositivos intermedios.

Tenemos una aproximación de este problema en la Figura 1.5. Cada dispositivos tiene un enlace directo y dedicado, llamado enlace punto a punto, con uno de los otros dispositivos. Si hay N dispositivos, entonces se requieren N(N-1) enlaces y cada dispositivo requiere (N-1) puertos de entrada/salida (I/O). Así, el costo del sistema, en términos de instalación del cable y equipo de I/O, crece con el cuadrado del número de dispositivos.

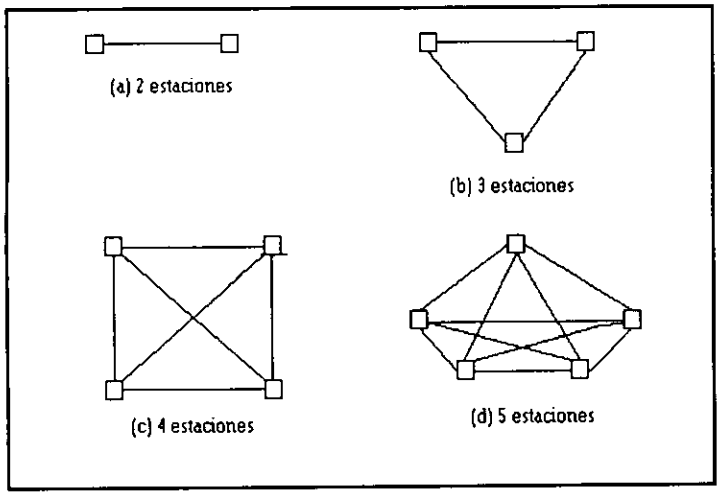


Figura. 1.5 Enlaces entre estaciones

La imposibilidad de esto, conocida algunas veces como el enredo de las topologías, fue reconocido tempranamente por las comunicaciones de área amplia, la solución se muestra en la Figura 1.6, y fue el introducir una red con conmutación de nodos que tienen la habilidad de enrutar mensajes, creando enlaces lógicos y eliminando la necesidad de tantas conexiones físicas directas. En esta aproximación, cada dispositivo o estación se conecta directamente a un nodo de comunicación de la red y se comunica a otra estación vía la red.

Esta aproximación -el uso de una colección de nodos conmutados- no se usa generalmente para redes locales. Debido a que las distancias son pequeñas, el gasto de nodos conmutados puede ser evitado.

Cuatro topologías se describirán a continuación: bus, árbol, anillo y estrella (Figura. 1.6). Estas son comúnmente usadas, tal cuales, para construir LAN's y MAN's. También pueden ser usadas como bloques en un edificio para redes con topologías más complejas.

- **Topología en anillo.**

En la topología en anillo, la red consiste de un arreglo de repetidores unidos por enlaces punto a punto en un círculo. Por lo tanto cada repetidor participa en dos enlaces. El repetidor es un dispositivo comparativamente simple, capaz de recibir datos en un enlace y transmitirlos, bit por bit, en el otro enlace tan pronto como los recibe, sin tener un buffer en el repetidor. Los enlaces son unidireccionales; esto es, los datos son transmitidos en una dirección solamente y todos son orientados en la misma dirección. Así los datos circulan alrededor del anillo en una dirección (en sentido horario o antihorario).

Cada estación une a la red con el repetidor. Los datos se transmiten en paquetes. Así, por ejemplo, si la estación X desea transmitir un mensaje a la estación Y, dividirá el mensaje en paquetes. Cada paquete contiene una porción de datos más alguna información de control, incluyendo las direcciones de Y. Los paquetes son insertados dentro del anillo uno por uno y circulan a través de los otros repetidores. La estación Y reconoce su dirección y toma los paquetes como vienen.

Debido a que múltiples dispositivos comparten el anillo, se necesita control para determinar en que momento cada estación puede insertar sus paquetes. Este es casi siempre realizado con alguna forma de control distribuido. Cada estación contiene acceso lógico que controla la transmisión y la recepción.

- **Topologías Bus y Arbol**

Con la tecnología en bus, la red de comunicación es simplemente el medio de transmisión, sin repetidores ni switches. Todas las estaciones se unen, a través de interfaces apropiadas, directamente a un medio de transmisión lineal, o BUS. Una transmisión de cualquier estación se propaga a lo largo del medio y puede ser recibida por las demás estaciones.

La topología de árbol es una generalización de la topología de Bus. El medio de transmisión es un cable bifurcado sin circuitos. El arreglo árbol inicia en un punto conocido como headend. Uno o más cables parten del headend, y en cada uno de estos puede tener bifurcaciones. Las bifurcaciones en cambio pueden tener bifurcaciones adicionales para permitir arreglos bastante complejos. Otra vez, una transmisión de cualquier estación se propaga a lo largo del medio y puede ser recibida por todas las otras estaciones. Para ambas topologías, el medio es referido como multipunto.

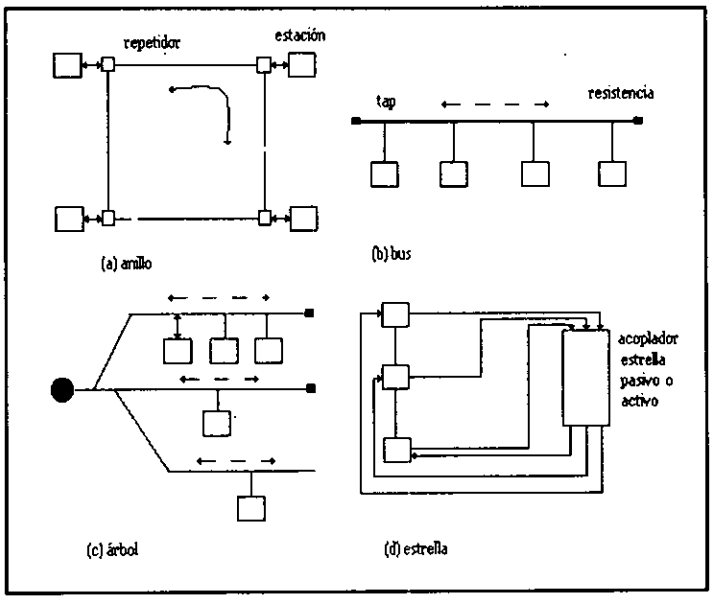


Figura. 1.6 Topologías físicas.

Debido a que todos los nodos en Bus o Arbol comparten un enlace común de transmisión, solo una estación puede transmitir a la vez. Alguna forma de control de acceso se requiere para determinar cual estación transmitirá enseguida.

Como en el anillo, el empaquetamiento para la transmisión es usado para la comunicación. Una estación deseando transmitir divide el mensaje en paquetes y los envía uno a la vez. Para cada paquete que una estación desea transmitir, espera su siguiente turno y envía otro. La estación destino reconocerá su dirección

conforme pasa el paquete y lo copiará. No existen nodos intermedios ni están involucrados repetidores o conmutadores.

- **Topología en Estrella**

En la topología en estrella, cada estación está conectada directamente a un switch común central. Un ejemplo del uso de esta tecnología es el caso en el cual el switch central usa tecnología de conmutación de circuitos. El switch digital de datos y la bifurcación digital privada son ejemplos de esta topología.

La topología en estrella también se emplea para implementar un LAN que envía paquetes en broadcasting. En este caso, cada estación se une a un nodo central, referido como el acoplador estrella, vía dos enlaces punto a punto, uno para cada dirección de transmisión. Una transmisión de cualquier estación pasa al nodo central y es retransmitido a todos los enlaces de salida. Así, por lo tanto el arreglo es fisicamente una estrella, y lógicamente un Bus: una transmisión de cualquier estación es recibida por todas las demás estaciones, y solamente una estación a la vez puede transmitir exitosamente. Por lo tanto, las técnicas de control de acceso al medio usadas para los paquetes en la topología en estrella son las mismas que para Bus y Árbol.

Existen dos formas de implementar el acoplador estrella (concentrador). En el caso de un acoplador pasivo, existe un enlace electromagnético en el acoplador, así que cualquier transmisión de llegada pasa fisicamente a todos los enlaces de salida. En el caso de fibra óptica, este acoplamiento es llevado a cabo al soldar determinado número de fibras, así que la luz de llegada es pasada automáticamente entre las fibras de salida. En el caso de cable coaxial o par torcido, se usa acoplamiento por transformador para pasar la señal de llegada.

El otro tipo de acoplador estrella es el acoplador activo. En este caso, existe lógica digital en el nodo central que actúa como repetidor. Conforme llegan los bits en cada línea de entrada, son regenerados automáticamente y repetidos a todas las líneas de salida. Si muchas señales de entrada llegan simultáneamente, se transmite una señal de colisión a todas las líneas de salida

- **Elección de una Topología**

El elegir una topología depende de una variedad de factores, incluidos formalidad, escalabilidad, y desempeño. Esta elección es parte de la labor del diseño de una red local.

La topología Bus/Árbol aparece como la más flexible. Y es posible de manejar un amplio rango de dispositivos, en términos del número de dispositivos, velocidad de transmisión y tipo de datos. Permite un gran ancho de banda. Porque el medio es pasivo, parecería a primera vista ser altamente segura. Pero como veremos, este no es necesariamente el caso. En particular, una ruptura en el cable puede desactivar una gran parte de la red.

Enlaces muy rápidos se pueden usar entre los repetidores de un anillo. Por lo tanto, el anillo tiene el potencial de proveer el mejor medio de todas las topologías. Existen limitaciones prácticas, en términos del número de dispositivos y variedad de los tipos de datos. Finalmente, el problema de la formalidad es obvio: una falla del repetidor o enlace podría desactivar toda la red.

La topología estrella, usando conmutación de circuitos, integra con facilidad voz con tráfico de datos. Trabaja fácilmente con dispositivos de baja velocidades de transmisión (< 64 kbps). La topología estrella es buena para requerimientos de terminales intensivas debido al peso mínimo del procesamiento que impone a los dispositivos conectados.

1.4 Medios de Transmisión

El medio de transmisión es la vía física entre el transmisor y el receptor en una red de comunicaciones. La Figura 1.7 muestra los elementos básicos de un sistema de transmisión.

El medio de transmisión puede ser clasificado como guiado o no guiado. En ambos casos, la comunicación es en forma de ondas electromagnéticas. Con un medio guiado, las ondas son guiadas a lo largo de un camino físico. Ejemplos de medios guiados son el par torcido, cable coaxial, y fibra óptica, que son usados en redes locales. La atmósfera y el espacio exterior son ejemplos de medios

no guiados, que proporcionan los medios para transmitir ondas electromagnéticas pero no las guían. Varias formas de transmisión a través de la atmósfera se utilizan para conexiones de edificio a edificio.

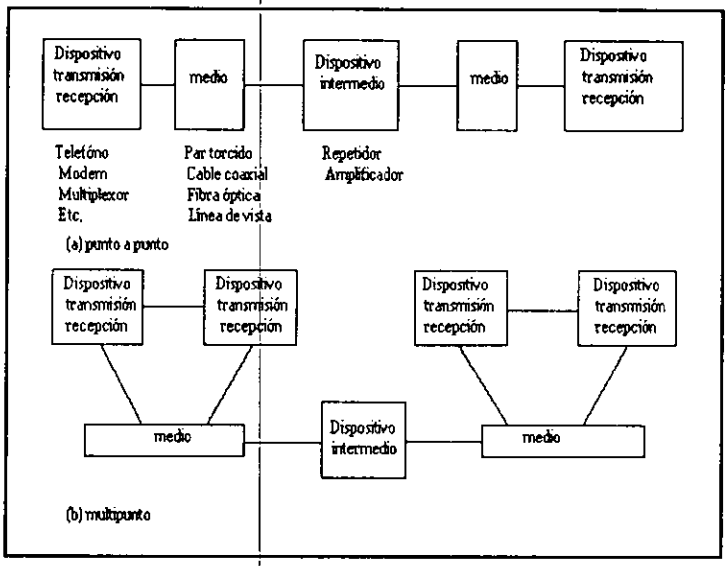


Figura. 1.7 Elementos básicos de un sistema de transmisión.

Para describir los medios anteriores usaremos las siguientes características:

- ***Descripción física*:** la naturaleza del medio de transmisión
- **Características de transmisión:** se utiliza señalización analógica o digital, técnica de modulación, capacidad, y la frecuencia a la que ocurre la transmisión
- **Uso geográfico:** la máxima distancia entre puntos en la red; se utiliza para intramuros, internuros, o ambos.
- **Inmunidad al ruido:** resistencia del medio a la contaminación de los datos transmitidos.
- **Costo relativo:** basado en el costo de los componentes, instalación, y mantenimiento.

♦ **Par Torcido**

Por mucho el medio de transmisión más común, tanto para datos digitales o analógicos, es el par torcido. El cableado dentro de un edificio que conecta los teléfonos es el par torcido, cableado en forma de circuitos locales que conectan todos los teléfonos en un área geográfica hacia una central de intercambio.

- **Descripción física.** Un par torcido consiste en dos alambres aislados arreglados en espiral. Los alambres son de cobre o acero cubiertos con cobre. El cobre proporciona conductividad; el acero puede ser usado para dar fuerza. Un par de alambres actúa como un enlace individual. Típicamente, un número de estos pares son atados juntos dentro de un cable al envolverlos en una funda protectora. Para largas distancias, los cables pueden contener cientos de pares. El apareamiento de pares individuales minimiza la interferencia electromagnética entre los pares. Los alambres en un par tienen un grosor de .016 a .036 pulgadas.

- **Características de transmisión**. Los cables pareados pueden ser usados para transmitir tanto señales analógicas como digitales. Para señales analógicas, se requieren amplificadores aproximadamente cada 5 o 6 km. Para señales digitales, se usan repetidores cada 2 o 3 km.

- **Utilidad.** El uso más común de los pares es la transmisión analógica de voz. No obstante que los componentes de frecuencia de voz se pueden encontrar entre 20 Hz y 20kHz, un ancho de banda más angosto se requiere para reproducciones de voz inteligibles. El ancho de banda estándar de un canal de voz full-duplex es de 300 a 3400Hz. Canales de voz múltiple pueden ser multiplexados, usando FDM, en un solo apr. Un ancho de banda de 4kHz por canal proporciona separación adecuada entre canales. El par torcido tiene una capacidad de más de 24 canales de voz usando un ancho de banda superior a 268kHz. Los datos digitales pueden ser transmitidos sobre un canal de voz analógico usando un modem. Con un modem de diseño común, son prácticas velocidades arriba de los 19.2kbps usando PSK. En un par de 24 canales, la velocidad de transmisión agregada es 230kbps.También es posible usar señalización digital o en banda base en un par torcido. Bell ofrece un circuito T1 usando par torcido que maneja 24 canales de voz PCM, para un aumento en la velocidad de 1.544Mbps. Velocidades más altas son posibles dependiendo de la distancia. Una velocidad de 4 Mbps representa un límite superior razonable.

- **Conectividad.** El par torcido puede ser usado para aplicaciones punto a punto o multipunto. Como un medio multipunto, el par torcido es menos caro, es una alternativa de menor desempeño que el cable coaxial pero soporta menos estaciones. Usos punto a punto son más comúnes.

- **Uso geográfico.** El par torcido puede proporcionar fácilmente transmisión de datos punto a punto en un rango de 15km o más. El par torcido se usa en LAN's para un solo edificio o solo algunos más.

- **Inmunidad al ruido.** Comparado con otros medios guiados, el par torcido es limitado en distancia, ancho de banda y velocidad de transmisión. El medio es bastante susceptible a interferencia y ruido debido a su fácil acoplamiento con campos electromagnéticos. Por ejemplo, un alambre corre paralelo a una línea de AC y captara 60Hz de energía. Las señales en los pares adyacentes de cables pueden interferir uno con otro, este fenómeno se llama Cross-talk.

- **Costo.** El par torcido es menos caro que, tanto, el cable coaxial o la fibra óptica en términos de costo por pie. Así que debido a sus limitaciones de conectividad, los costos de la instalación pueden ser cercanos a los de otro medio.

◆ **Cable Coaxial**

El medio de transmisión más versátil es el cable coaxial. Existen dos tipos de cable coaxial actualmente usados en LAN's: el cable de 75 ohms, que es utilizado en televisión por cable (CATV), y el cable de 50 ohms. El cable de 50 ohms es usado solamente para señalización digital, llamada banda base; el cable de 75 ohms es usado para señalización analógica con FDM, llamada banda amplia, y para señales digitales de alta velocidad y señales analógicas en las que no es posible el FDM.

- **Descripción física.** El cable coaxial, como el par torcido, consiste de 2 conductores, pero esta construida diferentemente para permitir el uso de un amplio rango de frecuencias. Consiste de un conductor cilíndrico hueco que rodea un conductor interior. El conductor interno puede ser sólido o retorcido; el conductor externo puede ser sólido o trenzado. El conductor interno es colocado en su lugar tanto por anillos aislados espaciados regularmente o un

material sólido dieléctrico. El conductor externo es cubierto con un protector. Un cable coaxial tiene un diámetro de .4 a aproximadamente 1 pulgada.

- **Características de transmisión.** El cable de 50 ohms es usado exclusivamente para transmisión digital. Se utiliza típicamente codificación Manchester y la velocidad de transmisión puede llegar a 10Mbps.

El cable CATV es usado tanto para señales analógicas o digitales. Para señales analógicas, son posibles frecuencias arriba de 300 o 400MHz. Datos analógicos, como video y audio, pueden ser manejados en el cable CATV en la misma forma en que se transmite TV y radio. Los canales de TV son colocados en 6 MHz de ancho de banda; cada canal de radio requiere mucho menos. Por lo tanto un gran número de canales pueden ser llevados en el cable usando FDM.

Cuando se utiliza FDM, el cable CATV es referido como de banda amplia. El espectro en frecuencia del cable es dividido en canales, que llevan señales analógicas. Además de los datos analógicos, también pueden ser transportados datos digitales en un canal. Varios esquemas de modulación han sido usados para datos digitales, incluyendo ASK, FSK, y PSK. La eficiencia del modem determinará el ancho de banda requerido para soportar una velocidad de transmisión dada. Una buena regla de utilidad es asumir 1Hz por bps para velocidades de 5Mbps y alrededor de 2Hz por bps para velocidades más bajas. Por ejemplo, un velocidad de 5Mbps puede llevarse a cabo en un canal de TV de 6MHz, mientras un modem de 4.8kbps podría usar alrededor de 10kHz. Con la tecnología actual, una velocidad de aproximadamente 20Mbps es posible; a esta velocidad, la eficiencia del ancho de banda puede exceder 1bps/Hz.

Para lograr velocidades de aproximadamente 20Mbps, 2 propuestas se han dado. Ambas requieren que todo el ancho de banda del cable de 75 ohms sea dedicado a esta transferencia de datos; no se utiliza FDM. Una propuesta es el uso de señales digitales en el cable, como se ha hecho para el cable de 50 ohms. Una velocidad de 50 Mbps ha sido realizado con este esquema. Una alternativa es el uso de un sistema simple PSK; usando una portadora de 156MHz. Velocidades más bajas son logradas usando FSK.

- **Conectividad.** El cable coaxial es aplicable a conFiguraciones punto a punto y multipunto. El cable de 50 ohms puede soportar, en banda base, 100 dispositivos por segmento, logrando grandes sistemas por el enlace de segmentos con repetidores. El cable de 75 ohms de banda amplia puede

soportar miles de elementos. El uso de cable de 75 ohms a alta velocidad (50Mbps) introduce problemas técnicos que limitan el número de dispositivos de 20 a 30.

- **Uso geográfico.** Las máximas distancias permitidas en un cable de banda base están limitadas a unos pocos kilómetros. Las redes de banda amplia pueden abrirse a decenas de kilómetros. La diferencia tiene que ver con la integridad de la señal analógica o digital. La transmisión de alta velocidad (50Mbps), digital o analógica es limitada a 1 km. Debido a la alta velocidad de transmisión, la distancia física entre señales en el bus es muy pequeña. Así muy poca atenuación o ruido puede ser tolerado antes de que los datos se pierdan.

- **Inmunidad al ruido.** La inmunidad al ruido para el cable coaxial depende de la aplicación y la implementación. En general, es superior al par torcido para frecuencias altas.

- **Costo.** El costo de una instalación de cable coaxial cae entre el par torcido y la fibra óptica.

♦ **Cable de fibra óptica.**

Uno de los descubrimientos tecnológicos más importantes en transmisión de información han sido los sistemas de fibra óptica. La fibra óptica todavía disfruta de un uso considerable en telecomunicaciones de larga distancia, y su uso en aplicaciones militares esta creciendo.

Las continuas mejoras en el desempeño han declinado su precio, junto con las ventajas inherentes de la fibra óptica, la han hecho atractiva para las redes locales. Las siguientes características distinguen a la fibra óptica del par torcido y el cable coaxial:

1. Mayor capacidad, el potencial ancho de banda, y por lo tanto la velocidad de transmisión, de las fibras ópticas es inmensa ; la velocidad de transmisión de 2Gbps en cientos de kilómetros han sido probados. Comparando esto con los cientos de Mbps. en aproximadamente 1 km. para el cable coaxial y solo unos pocos Mbps. sobre 1 km. de par torcido.

2. Menor tamaño y menos paso, las fibras ópticas son considerablemente más angostas que el cable coaxial o el par torcido cuando menos de una magnitud menor para capacidades de transmisión comparables. Para conductores estrechos en edificios y enterrados a lo largo de vías públicas, la ventaja del pequeño tamaño es considerable. La reducción en peso reduce los requerimientos de soporte estructural.

3. Menor atenuación, la atenuación es significativamente menor para fibra óptica que para el cable coaxial y el par torcido y es constante sobre un amplio rango.

4. Aislamiento electromagnético, los sistemas de fibra óptica no son afectados por campos electromagnéticos externos. Por lo cual el sistema no es vulnerable a interferencias, ruido impulsivo, o cross-talk. Asimismo, las fibras no radian energía causando poca interferencia con otro equipo y proporcionan un alto grado de seguridad contra espionaje.

- **Descripción física.** Una fibra óptica es un medio angosto (2 a 125 μm), flexible y capaz de conducir un rayo óptico. Varios vidrios y plásticos puede usarse para hacer fibras ópticas. Las menores pérdidas han sido obtenidas usando fibras de silica fundida ultrapura. La fibra ultrapura es difícil de manufacturar; las fibras de vidrio de multimodo son más económicas y proporcionan buen desempeño. La fibra plástica es más barata y puede ser usada para enlaces cortos y tienen pérdidas aceptables. Un cable de fibra óptica tiene una forma cilíndrica y consiste de 3 secciones concéntricas: el alma, el revestido y el forro. El alma es la parte más interna, y consiste de una o más cuerdas muy delgadas, o fibras hechas de vidrio o plástico. Cada fibra esta rodeada por su propio revestimiento, una cubierta de vidrio o plástico que tiene propiedades ópticas diferentes de las del alma. La capa más externa, que rodean una o varias fibras revestidas, es el forro. El forro está compuesto de plástico y otros materiales puestos en capas para proteger en contra de la humedad, abrasión, ruptura y otros peligros ambientales.

- **Características de transmisión.** La fibra óptica transmite un rayo de luz con una señal codificada por medio de la reflexión interna total. La reflexión total interna puede ocurrir en cualquier medio transparente que tenga un alto índice de refracción que rodee el medio. En efecto, la fibra óptica actúa como guía de onda para frecuencias en el rango, que cubre el espectro visible y parte del espectro infrarojo. Actualmente, una portadora es usada para transmisión en fibra óptica. Avances futuros permitirán sistemas prácticos FDM, también

conocidos como multiplexaje por división de longitud de onda o multiplexaje por división de color.

- **Conectividad.** El uso más común para la fibra óptica es para enlaces punto a punto. Sistemas experimentales multipunto usando una tecnología de bus han sido construidos, pero son muy caros para ser prácticos. En principio, no obstante, un solo segmento de fibra óptica podría soportar muchas más caídas que el par torcido y el cable coaxial, debido a pocas pérdidas de potencia, características de baja atenuación, y gran potencial de ancho de banda.

- **Uso geográfico**. La tecnología actual soporta la transmisión en distancias de 6 a 8 kms. sin repetidores. Por lo que la fibra óptica se puede utilizar para enlazar LAN's en muchos edificios vía enlaces punto a punto.

- **Inmunidad al ruido.** La fibra óptica no es afectada por la interferencia electromagnética o el ruido. Esta característica permite altas velocidades de transmisión en gran distancia y da excelente seguridad.

- **Costo.** Los sistemas de fibra óptica son más caros que el par torcido y el cable coaxial en términos de costo por pie y requiere componentes (transmisores, receptores, conectores). Mientras que el costo del par torcido y el cable coaxial no es probable que bajen, los avances en Ingeniería reducirán el costo de la fibra óptica para ser competitiva con los otros medios.

- **Línea de Vista**

Analizando 3 técnicas para transmitir ondas electromagnéticas a través de la atmósfera: microondas, luz infraroja y el láser. Las tres requieren una línea de vista entre transmisor y receptor.

Debido a los valores de alta frecuencia a los cuales operan estos dispositivos (microondas, 10^6 a 10^9 Hz; la luz infraroja, 10^{11} a 10^{13} Hz; laser, 10^{15} a 10^{17} Hz), existe el potencial de altas velocidades de transmisión. Los sistemas prácticos para enlaces cortos han sido construidos con velocidades de muchos megabits por segundo.

Estas técnicas de transmisión son útiles conectando redes locales que están en edificios separados. La dificultad de cablear entre edificios, o bajo tierra,

especialmente si el espacio entre estos es público. Las técnicas de línea de vista requieren equipo solo en cada edificio.

Los enlaces infrarojos consisten en un par de transmisores/receptores (transreceptores) que modulan luz infraroja no coherente. Los transreceptores deben estar en una línea de vista, instalada en el techo o en una ventana adyacente exterior. El sistema es altamente direccional; esto es, es muy difícil de interceptar, inyectar datos o interferir tales sistemas. No se requiere licencia y el sistema puede ser instalado en unos cuantos días. Son prácticos sobre unos cuantos kilómetros y la velocidad de transmisión puede ser de algunos megabits por segundo.

Un sistema parecido puede ser instalado con transreceptores laser usando modulación de luz coherente. La mayor diferencia es que la Administración de Alimentos y Drogas (FDA) requiere que el equipo de laser, que emite bajos niveles de radiación, sea aislado adecuadamente. Una licencia tarda entre 2 y 6 meses.

Tanto la luz infraroja como el laser son susceptibles a interferencia ambiental, como lluvia y niebla. Un sistema menos sensible son las microondas. Como en el caso del láser y la luz infraroja, la instalación es relativamente fácil; la mayor diferencia es que los transreceptores de microondas pueden ser montados solo externamente en un edificio. Las microondas es menos direccional que el laser y la luz infraroja; por lo que existe un problema de seguridad de privacidad, inserción, o interferencia. Como todos los sistemas de radio frecuencia, las microondas requieren licencia de la Comisión Federal de Comunicaciones (FCC), que toma entre 2 y 3 meses. Y pueden lograrse distancias y velocidades similares a los laseres y la luz infraroja. La tabla 1.8 resume las principales características de estas técnicas e incluye, para comparación, el uso de cable para enlaces de edificio a edificio.

La elección del medio de transmisión es determinada por un número de factores. Es, como veremos, condicionante la topología de la red. Otros factores también juegan un papel importante como:

- **Capacidad:** soporta el tráfico esperado en la red.
- **Confianza**: permite llevar a cabo todos los requerimientos.
- **Tipos de datos soportados:** de acuerdo al tipo de aplicación.
- **Influencia ambiental:** presta servicio sobre el amplio rango de ambientes requeridos.

Medio	Facilidad de instalación	Velocidad de transmisión	Facilidad de mantenimiento
Infrarrojo	1-2 días, fácil	1-3 Mbps	Excelente
Laser	1-2 días, fácil	1-3	Excelente
Microondas	1 semana, fácil	1-3	Excelente
F. Optica/ c. coaxial subterraneo	1-18 meses moderada a difícil	10+	Buena
F. Optica/ c. coaxial aereo	1-6 meses moderada	10+	Buena

Figura. 1.8 Medios de Tx para LAN a través de propiedad pública.

El par torcido no es caro, y es un medio bien conocido. Usualmente, los edificios de oficina son cableados anticipadamente para soportar la demanda del sistema telefónico más un margen que se aprovecha. Comparado con el coaxial, el ancho de banda es limitado. El par torcido es probablemente el medio más adecuado para un red LAN que ocupe un solo edificio con bajo tráfico. Un sistema de automatización de la oficina, con preponderancia de terminales tontas y/o estaciones de trabajo inteligentes más algunas minis, es un buen ejemplo.

El cable coaxial es más caro que el par torcido, pero tiene una gran capacidad. Para un rango amplio de requerimientos de LAN/MAN, y con la excepción de sistemas de terminales intensivas, es el medio a elegir. Para la mayoría de los requerimientos, una red local basada en coaxial puede ser diseñada para cumplir con una demanda de expansión a un costo razonable. El sistema de cable coaxial es excelente cuando hay muchos equipos y un tráfico considerable. Los ejemplos incluyen instalaciones de gran procesamiento de datos y sistemas sofisticados de automatización de oficina, el cual puede incluir máquinas de facsímile, copiadoras inteligentes, y equipo de gráficos a color.

En las condiciones actuales, los enlaces de fibra óptica se situan en comunicaciones punto a punto. Por lo que no puede competir con el cable coaxial.

La única excepción son las redes en topología de anillos. No obstante, cuando el costo de la fibra óptica multiusos se vuelva competitivo con el cable coaxial, sus ventajas -poca susceptibilidad al ruido, pocas pérdidas, tamaño pequeño y poco peso- la convertirán en un serio contendiente para muchas aplicaciones de redes.

El enlace por línea de vista no es muy utilizado para redes locales. Pero son, no obstante, buenas elecciones para enlaces punto a punto entre edificios, los cuales tienen redes locales basadas en cable coaxial o par torcido.

1.5 Arquitectura OSI (IEEE)

El concepto de sistema abierto esta basado en el concepto de aplicaciones distribuidas cooperantes. En el modelo OSI, un sistema consiste de una computadora, todo su software, y dispositivos periféricos unidos a ella, incluyendo las terminales. Una aplicación distribuida es una actividad que involucra el intercambio de información entre dos sistemas de información.

OSI se relaciona con el intercambio de información entre sistemas abiertos y no con las funciones internas de cada sistema individual. Específicamente, tiene que ver con la capacidad del sistema para cooperar en el intercambio de información y el cumplimiento de las tareas.

El objetivo del esfuerzo OSI es definir un arreglo de estándares que habilitarán a los sistemas abiertos localizados en cualquier parte del mundo a cooperar al ser conectados a través de algunas facilidades de comunicación estandarizadas y al ejecutar protocolos OSI estandarizados. Un sistema abierto puede ser implementado en cualquier manera simplemente cumpliendo con un mínimo de condiciones que permitan la comunicación con otros sistemas abiertos. Un sistema abierto consiste de un número de aplicaciones, sistemas operantes y sistemas de software tales como sistemas de administración de bases de datos y paquetes de manipulación de terminales. Esto también incluye el software de comunicación que cambia un sistema cerrado en un abierto. Diferentes fabricantes implementan sistemas abiertos de diferentes maneras, con el fin de realizar una identidad de producto, que incrementará su cuota de mercado o creará un nuevo mercado. No obstante, virtualmente todos los fabricantes están llamados a proporcionar software de comunicaciones que cumpla con OSI para que sus clientes tengan la habilidad de comunicarse con otros sistemas abiertos.

De manera general las metas del modelo OSI son las siguientes:

- Proporcionar estándares para la comunicación entre sistemas.
- Remover cualquier impedimento técnico para la comunicación entre sistemas.
- Remover lo concerniente con la descripción de la operación interna de un sistema individual.
- Definir los puntos de interconexión para el intercambio de información entre sistemas.
- Reducir las opciones para incrementar la habilidad de comunicarse sin conversiones caras y translaciones entre productos.
- Proporcionar un punto razonable para la salida para los estándares en el caso de que no cumplan las necesidades.

Una técnica de estructuración ampliamente aceptada, y la escogida por ISO, son las capas. Las funciones de comunicaciones son particionadas en arreglos de capas jerárquicos. Cada capa realiza una parte de las funciones requeridas para comunicarse con otro sistema. y confía en la siguiente capa inferior para desempeñar funciones más primitivas y para concertar los detalles de esas funciones. Proporciona servicios a la capa próxima superior. Idealmente, las capas deberían ser definidas de tal forma que los cambios en una capa no requieran cambios en las otras capas. Además existen algunas funciones que deben ser realizadas en un sistema para que este se comunique. Por su puesto, se necesita de dos para poder comunicarse, así que las mismas funciones en capas deben existir en dos sistemas. La comunicación se lleva a cabo al tener capas correspondientes en dos sistemas que se comunican. Las capas se comunican por medio de un arreglo de reglas, o convenciones, conocidas como protocolo.

Los elementos claves del protocolo son:

- **Sintaxis:** La forma en que la información se intercambia (formato, codificación)
- **Semántica:** La interpretación de la información de control para coordinación y manipulación de errores
- **Tiempo:** La secuencia en la cual los eventos de control ocurren

La Figura 1.9 ilustra la arquitectura OSI. La capa más baja en el modelo es llamada capa física. Las funciones relacionadas con esta capa son responsables de la activación, mantenimiento, y desactivación de un circuito físico entre un DTE y un DCE. Existen muchos estándares para la capa física. Pero los más notables son el RS-232-C y V.24. X.21 utiliza un conector de 15 canales DB 15. En el caso de RS-232 el uso más típico es conectar un dispositivo digital a un modem, que se

conecta a una línea telefónica de voz. Nos referiremos a esto describiendo cuatro características.

La característica mecánica pertenece al punto de marcación. Usualmente, este es un conector. RS-232-C especifica un conector de 25 pines, en donde se usan 25 cables para conectar dos dispositivos.

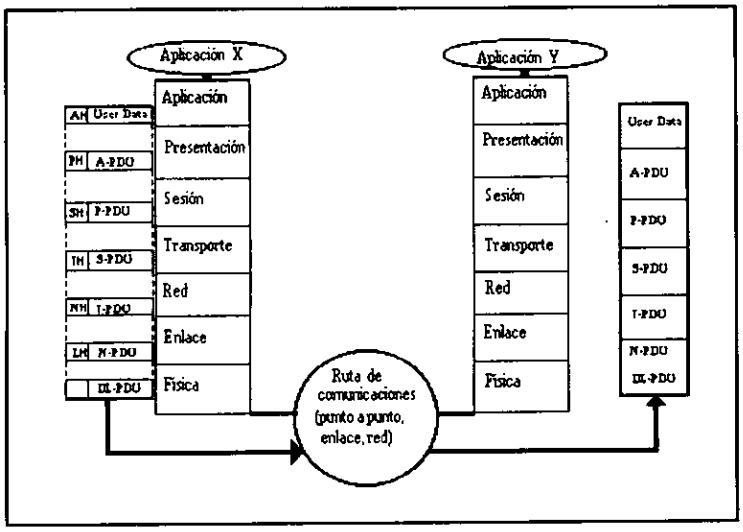


Figura. 1.9 Arquitectura OSI

La característica eléctrica tiene que ver con los niveles de voltaje y el tiempo para los cambios de voltaje. Estas características determinan la velocidad de datos y las distancias posibles.

Las características funcionales especifican las funciones que son realizadas por la interpretación de valores asignados. Para el RS-232-C y para la mayoría de las capas físicas de otros estándares, esto se realiza al especificar la función de cada pin en el conector.

Las características de procedimiento especifican la secuencia de eventos para la transmisión de datos, basados en características funcionales. Para el RS-232-C, el uso de varios pines esta definido.

La **capa física** difiere de otras capas OSI en que no puede dejar en una capa más baja la responsabilidad de transmitir sus PDU´s. Por lo que tiene que hacer

uso del medio de transmisión cuyas características no son parte del modelo OSI. No existe estructura PDU en la capa física como tal, no se utiliza encabezado para información del control del protocolo. El PDU simplemente consiste de un bloque de bits.

La **capa de enlace** de datos es responsable de la transferencia de datos sobre el canal. Proporciona la sincronización de datos para delimitar el flujo de bits de la capa física. También proporciona la identidad de los bits. Asegura que los datos llegarán seguros al DTE receptor. proporciona el control de flujo para asegurar que el DTE no se saturará con demasiada información al mismo tiempo. Una de sus funciones más importantes es el de proporcionar la detección de errores en la transmisión y los mecanismos para recuperarla.

Podemos en este momento definir el HDLC, que es un protocolo asíncrono orientado a bit. Y lo hacemos por dos razones:

1. HDLC es un antecesor del estandar para el protocolo de enlace de capas para LAN's (IEEE 802).
2. Nos ilustrará muchos conceptos concernientes a protocolos.

HDLC, y los protocolos orientados a bit en general, son intentos para lograr las siguientes capacidades:

- Operación independiente al código(transparencia): el protocolo y lo que transporta es independiente.
- Adaptación a varias aplicaciones, conFiguraciones y usos de una manera consistente: por ejemplo pueden ser soportadas conFiguraciones punto a punto, multipunto y lazo.
- Transferencia de datos de dos vías alternada o transferencia de datos de dos vías simultanea (full-duplex).
- Alta eficiencia: el protocolo debe tener un mínimo de bits de sobrecarga. También, debe trabajar eficientemente sobre enlaces con largos retardos y enlaces con alta velocidad de transmisión
- Alta confiabilidad: los datos no deben ser perdidos, duplicados, o desechados.

Con estos requerimientos en mente, pasamos a la descripción del HDLC. Se definen 3 modos de operación: el modo de respuesta normal (NRM), modo de respuesta asíncrono (ARM), y el modo asíncrono balanceado (ABM). Tanto el NRM y el ARM pueden ser usados en conFiguraciones punto a punto y multipunto. Para cada uno hay una estación primaria y otras estaciones secundarias. La estación primaria es responsable de inicializar el enlace, controlar

el flujo de datos de y hacia las estaciones secundarias, recuperar errores y desconectar lógicamente estaciones secundarias. En NRM, una estación secundaria puede transmitir solamente en respuesta de una llamada de la primaria; en ARM la secundaria puede iniciar una transmisión sin llamada previa. NRM se sitúa idealmente para líneas multipunto consistentes de una computadora host y un número de terminales. ARM puede ser necesaria para ciertas clases de conFiguraciones en circuito.

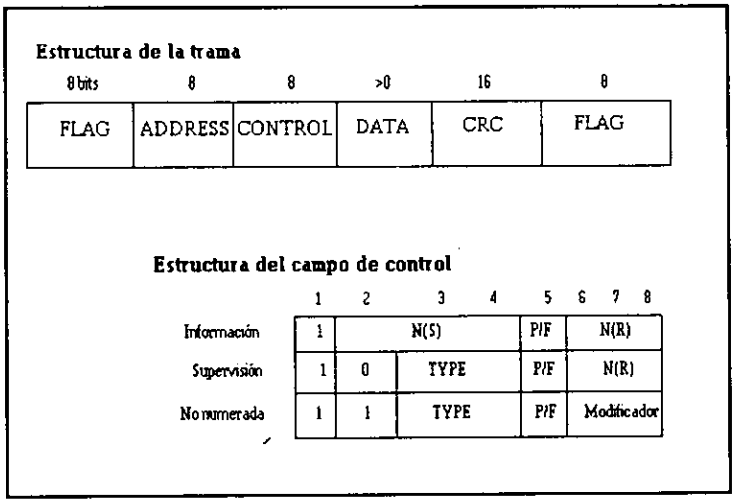


Figura 1.10 Estructura ARM y trama HDLC.

ARM es usada en enlaces punto a punto solamente, y cada estación asume el papel tanto de primaria como secundaria. ARM es más eficiente para líneas punto a punto, porque ambas estaciones pueden iniciar la transmisión. Los datos se transmiten en cadenas de 6 campos (Figura 1.10), que son los siguientes:

- **FLAG:** usada para sincronización, este campo indica el inicio y fin de la trama. El patrón de bandera es, 01111110, se evita en los datos por el rellenado de bits.
- **ADRESS**: este campo identificá la estación secundaria para esta transmisión.
- **CONTROL**: este campo identifica la función y el propósito de la trama.
- **DATA**: este campo contiene los datos a ser transmitidos.
- **CRC**: este es el campo de revisión de secuencia de la trama. Usa un chequeo de redundancia cíclica(CRC). El campo CRC es una función de los contenidos de dirección, control y datos. Es generado por el transmisor y de

nuevo por el receptor. Si el resultado del receptor difiere del campo de CRC, un error en la transmisión ha ocurrido.

Se usan tres tipos de tramas, cada uno con diferente formato en el campo de control. Las cadenas de información llevan los datos. Las cadenas de supervisión proporcionan las funciones básicas de control, y las cadenas sin número llevan a cabo funciones de control de enlace suplementarias.

El bit P/F(poll/final) es usado por una estación primaria para solicitar una respuesta. Más de una trama puede ser enviada en respuesta, con el bit P/F colocado para indicar la última trama. El P/F puede ser usado con supervisión y cadenas sin numeración para forzar una respuesta.

Los campos N(S) y N(R) en la trama de información proporcionan una técnica eficiente tanto para el control de flujo como para el control de errores. Un estación numera las tramas que envía secuencialmente modulo 8, usando el campo N(S). Cuando una estación recibe una trama de información válida, reconoce esta trama con su propia trama de información colocando el campo N(R) en el siguiente número de trama que espera recibir. Esto se conoce como un reconocimento "piggybacked". Los reconocimientos pueden ser enviados también en una trama de supervisión. Este esquema completa tres grandes funciones:

- **Control de flujo:** una vez que la estación a enviado 7 tramas, no puede enviar más hasta que la primera sea reconocida.

- **Control de error:** si una trama tiene un error, una estación puede enviar un NAK (reconocimiento negativo) vía una trama de supervisión que especifique cual fue la equivocada. Esto es realizado en una o dos formas. En el protocolo go-back-n, la estación que envía retransmite la trama con NAK y todas las tramas subsecuentes que ya se han enviado. En la técnica de repetición selectiva, la estación que envía retransmite solo la trama con error.

- **Pipelining**: más de una trama puede ser transmitida en cada instante; esto permite un uso más eficiente de enlaces con gran retraso en la propagación, como los enlaces satélitales.

La técnica N(S)/N(R) es conocida como protocolo de ventana deslizante debido a que la estación que envía mantiene una ventana de mensajes que se envían para que se muevan gradualmente la transmisión y los reconocimientos.

Existen 4 tipos de tramas de supervisión:

1. **Recive Ready (RR):** usada para corregir reconocimientos recibidos de tramas arriba de N(R)-1. Alternativamente, este es un comando que intsruye a la secundaria a iniciar la transmisión con un número de secuencia N(R).

2. **Recive Not Ready (RNR):** usado para indicar una condición de ocupado temporal. N(R) se utiliza para un posible reconocimiento redundante.

3. **Reject (REJ):** usado para indicar un error en la trama N(R) y solicitar la retransmisión de esa y las siguientes tramas.

4. **Selective Reject (SREJ):** se utiliza para solicitar la retransmisión de una sola trama.

La tramas sin numeración no tienen número secuencial y son usadas para un número de propósitos especiales, tales como inicializar una estación, colocar el modo, desconectar la estación, y rechazar un comando.

La **capa de red** especifica la interface del usuario DTE dentro de una red de conmutación de paquetes. También especifica en la red la ruta y las comunicaciones entre redes (internetworking). La capa bastante detallada y rica en funciones. Hay un espectro de posibilidades para intervenir facilidades de comunicación que sean administradas por la capa de red. En un extremo, hay un enlace directo punto a punto entre estaciones. En este caso, podría no ser necesaria una capa de red debido a que la capa de enlace de datos puede desempeñar la función necesaria de administración del enlace.

Note que los protocolos de capa 1 y 2 son locales y soportan el intercambio de información entre en final del sistema y un nodo de la red. Las cuatro capas superiores son protocolos de fin a fin entre los sistemas finales unidos. La capa 3 tiene las características de ambos. El protocolo de capa 3 es fin a fin en el sentido que nos da una dirección para transferir los datos al otro extremo del sistema.

Por otro lado, dos sistemas extremos podrían desear comunicarse pero no están conectados a la misma red. Pero están conectados a redes, que, directamente o indirectamente están conectados entre ellos. En este caso será necesaria alguna técnica de trabajo entre redes.

La **capa de transporte** proporciona la interface entre la red de comunicaciones y las 3 capas superiores (generalmente localizadas en las premisas del usuario). Es la capa que da las opciones de usuario para obtener ciertos niveles de calidad (y costo) de la misma red. Esta diseñada para mantener aislado al usuario de algunos aspectos físicos y funcionales de la red de paquetes.

La **capa de sesión** sirve como interface entre la capa de servicio de transporte. La capa proporciona a través de medios organizados el intercambio de datos entre usuarios, y los usuarios pueden seleccionar el tipo de sincronización y control necesario de la capa, tal como:

- Dialogo alternante de 2 vías o simultaneo de dos vías.
- Puntos de sincronización para revisiones intermedias y recuperación de transferencia de archivos.
- Abortos y reinicios.
- Flujo de datos normal o expedito.

La **capa de sesión** tiene servicios específicos, primitivos, y protocolo de unidades de datos que se definen en documentos ISO y CCITT.

La **capa de presentación** es para la sintaxis de los datos en el modelo, que es, la representación de datos. No tiene que ver con el significado o la semántica de los datos. Su rol principal, por ejemplo, es aceptar los tipos de datos (caracter, entero) de la capa de aplicación y entonces negociar con su capa previa lo relacionado a la representación sintáctica (como ASCII). Por lo que su función es limitada. La capa consiste de muchas tablas de sintaxis (teletipo, ASCII, Videotexto, etc.). La capa de presentación se encarga del despliegue en la terminal y también de los servicios tales como resolver el contenido de un mensaje electrónico de la capa de aplicación y negociar con la capa previa para dar a la capa de aplicación un arreglo específico de la imagen de la página.

La **capa de aplicación** tiene que ver con el soporte de un proceso de aplicación de usuario final. No como la capa de presentación, esta tiene que ver con la semántica de los datos. La capa contiene elementos de servicio para soportar procesamiento de aplicaciones tales como administradores de trabajo, intercambio de datos financieros (ANSI X9); emisores/receptores de lenguaje de programación (ANSI J-Series); y intercambio de datos de negocios (ANSI X12). La capa también soporta la terminal virtual y el concepto de archivo virtual.

El Comité Consultivo de Telegrafía y Telefonía Internacional (CCITT) ha dado a conocer estándares para la conexión de DTE'S a una red de conmutación de paquetes que proporciona equipo de comunicación de datos. El estándar ,X.25 específicamente direcciona capa 3 y engloba estándares para capa 2 y 1. Capa 3 es referida como LAP-B (Protocolo de Acceso al Enlace-Balanceado) y es casi idéntico con el HDLC (Control de Enlace de Datos de Alto Nivel) de ISO y el ADCCP (Control Avanzado de Procedimientos de Comunicación de Datos) de ANSI.

ISO ha editado estándares para capas 4 y 5 y esta en el proceso de editar una variedad de estándares que cubren capa 6 y 7. ISO ha dado a conocer también una subcapa de capa 3 y que tiene que ver con el trabajo interredes, que involucra comunicación a través de múltiples redes.

Un protocolo para trabajo interredes, llamado IP fue dado ha conocer por el Departamento de Defensa (DOD) para sus propias necesidades, mas un Protocolo de Control de Transmisión (TCP). TCP abarca todas las funciones de la capa 4 y algunas de capa 5. DOD intenta introducir estos estándares para su beneficio. Además, DOD ha editado varios estándares de capas superiores. El desacuerdo con los protocolos ISO esta todavía sin resolver.

Para el tipo de redes locales que referimos como redes de área local (LAN), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), a través de su comité 802, ha dado una arquitectura de 3 niveles que corresponde a las capas 1 y 2 del modelo OSI. Un número de estándares han sido dados a conocer por el comité para estas capas. La referencia 802 del IEEE define 3 capas y dos subcapas de operación. En la Figura 1.11 se muestran estas capas del IEEE. La capa 1 es una capa física, la capa 2 esta compuesta por la subcapa de Control de Acceso al Medio (MAC) y la subcapa de Control Lógico de Enlace (LLC), y la capa 3 es la capa de la red.

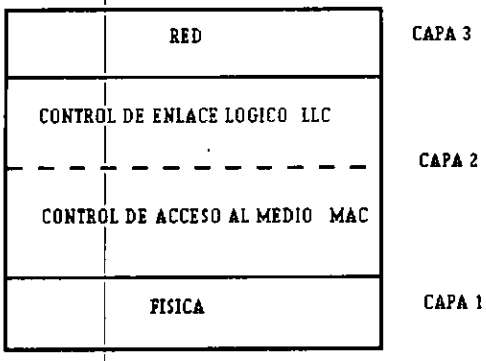


Figura. 1.11 Modelo 802 IEEE.

La Figura 1.12 muestra una comparación de los estandares IEEE 802 contra el modelo OSI.

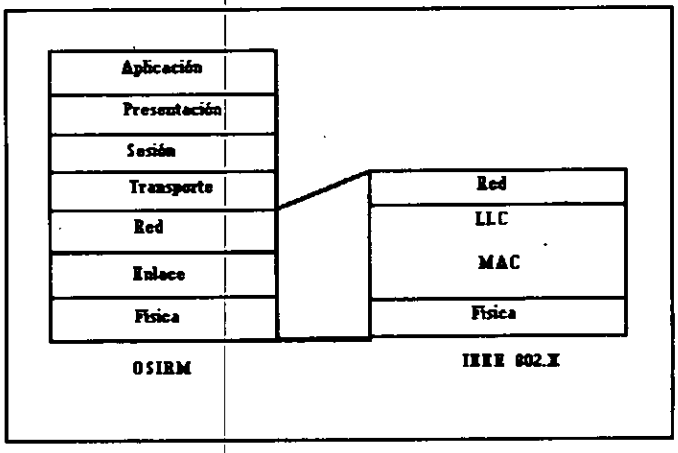


Figura. 1.12 IEEE 802 vs OSI.

También podemos decir que TCP/IP y OSI han sido creados para trabajo entre redes en diversas redes de datos a través de soluciones propias de los fabricantes. Los sistemas de operación de LAN´s también han sido creados teniendo en cuenta propiedades de solución, pero tienden más hacia implementaciones TCP/IP más que a soluciones OSI. En el pasado, se puso particular interés en mejorar la

protocolos intermedios tales como TCP/IP, que han sido probados suficientemente en las redes actuales. Los usuarios quieren el TCP/IP que trabaja hoy es una solución razonable a los problemas inmediatos en vez de esperar por la solución exacta OSI que todavía no existe. Algunos descubrimientos han sido también orientados ha correr OSI en capas más altas que TCP/IP. Parece muy probable que seguiremos con la coexistencia de TCP/IP, OSI y otros protocolos estandarizados hasta el final de la década, con TCP/IP permaneciendo como el protocolo de trabajo interredes dominante. Esto lo confirma el uso de TCP en internet, donde TCP/IP y UNIX rigen.

Los países Europeos y los de la cuenca del Pacífico están estandarizandose en OSI. Debido a que sus redes se están estandarizando a una velocidad más lenta, y con menos competencia entre vendedores, están construyendo lentamente redes de comunicación de datos que cumplen con los estandares OSI y soportan voz y datos. Este movimiento se lleva a cabo tanto por parte gubernamental como por los particulares. Aquí todo el software y el hardware debe cumplir con los estándares OSI. Esta orientación del mercado mundial hacia OSI muestra que se desea una sola arquitectura internacional.

1.6 Arquitectura DARPA.

La historia de los protocolos TCP/IP data de los 60´s cuando la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de lo Estados Unidos (después sería DARPA) inicio las investigaciones acerca de la viabilidad de una tecnología de conmutación de paquetes. Un contrato fue ganado por Bolt, Baranek y Newman (BBN) de Cambridge, Massachusetts para crear ARPANET. El proyecto fue exitoso, y ARPANET inicio operaciones en 1969 conectando 4 lugares: la Universidad de California en Los Angeles (UCLA), la Universidad de California en Santa Bárbara (UCSB), la Universidad de Utah, y el Instituto de Investigaciones de Stanford. Desde el comienzo, ARPANET fue una red de conmutación de paquetes a lo largo del mundo conectando cientos de computadoras desiguales. Además, BBN inicio en 1975 Telenet que se convirtió en la primer red comercial de Conmutación de paquetes.

La investigación de ARPANET engendro redes adicionales que son referidas colectivamente como la Internet DARPA, Internet TCP/IP o simplemente Internet (usaremos el término Internet cuando hagamos referencia a la Internet DARPA y el término internet cuando lo hagamos a la discusión genérica de trabajo de

interredes). La colección de redes interconectadas en Internet es ahora muy diversa. ARPANET fue desmantelada en Junio de 1990, y reemplazada con la Defense Research Internet (DRI), que esta basada en un T1 (1.544Mbps) en vez del ARPAnets con una velocidad de transmisión de 56 kbps.; el tráfico militar ahora tiene su propia red (MILNET) que es parte de la Red de Datos de Defensa (DDN); la Red de la Fundación Nacional de Ciencia (NSFNET) fue construida originalmente para proporcionar acceso a las supercomputadoras NSF; etc.

En la figura 1.13tenemos un esquema de como se encontraba la red en 1983.

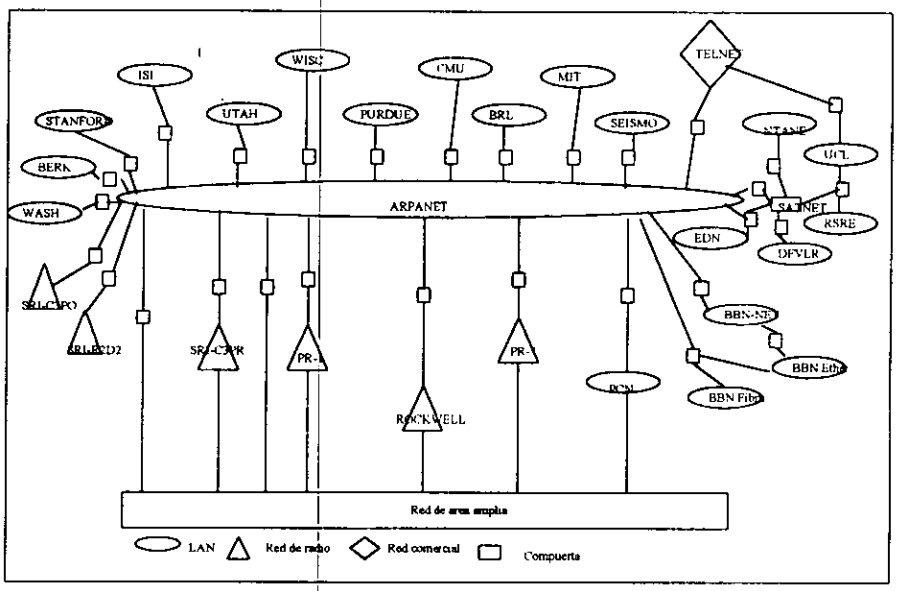


Figura. 1.13 Arquitectura DARPA

El protocolo del Departamento de Defensa (DOD) sigue una arquitectura de 4 capas. Esta incluye el acceso a la red (o capa de red local), la capa Internet, la capa de host-to-host, y la capa de proceso de aplicación. Cuando se comparan DOD y OSI (Figura. 1.14), la capa de red local incluye las capas física y de enlace de datos. La capa Internet incluye la capa OSI de funciones de red. La capa host-to-host proporciona las funciones de la capa de transporte de OSI, y la capa de aplicación DOD incluye las funciones de sesión, presentación y aplicación.

De particular interés para nuestro estudio de interredes es la manera en que se implementan estas capas. La capa de acceso a la red, como su nombre implica, controla el acceso a la LAN o WAN local unida. Esta capa es específica de la red, y puede tener muchas implementaciones a través de la interred. El protocolo de Internet (IP) reside tanto en el host como en las compuertas (actualmente ruteadores)y libera datos del host fuente al host destino. El Protocolo de Control de Transmisión (TCP) reside solamente en los host, y asegura una entrega segura de los datos. Las varias utilidades y aplicaciones tales como Protocolo de Transferencia de Archivos (FTP) y el Protocolo de Simple Transferencia de Correo (SMTP) también residen solo en los hosts.

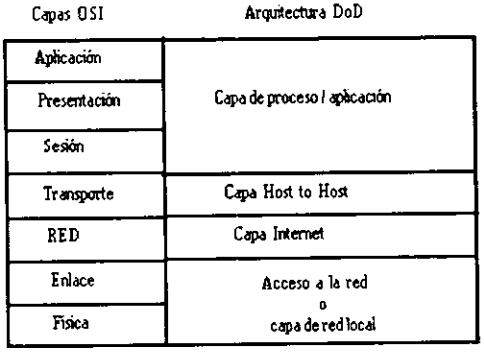


Figura. 1.14 DOD vs OSI.

Todos los protocolos DOD son especificados por los documentos "Request For Comments" (RFC) publicados por el Centro de Información de Defensa de Redes de Datos. Los más importantes de estos protocolos se muestran en la Figura 1.15con relación al modelo OSI.

Debido a las diversas implementaciones en el número de LAN y WAN, la arquitectura DOD no especifica un protocolo particular que se deba usar en la capa de enlace de datos. Existen de cualquier modo estándares, para soportar ETHERNET, IEEE 802, y ARCNET LAN's, y redes públicas de datos por medio de los protocolos X.25. Como se muestra en la Figura 1.15 el procesamiento de datos en el host (FTP, SMTP, TELNET)se pasa a la capa TCP, despúes a la capa IP, y finalmente la capa de acceso a la red, en donde finalmente se completa la trama de capa de enlace de datos con header y trailer para su transmisión en internet.

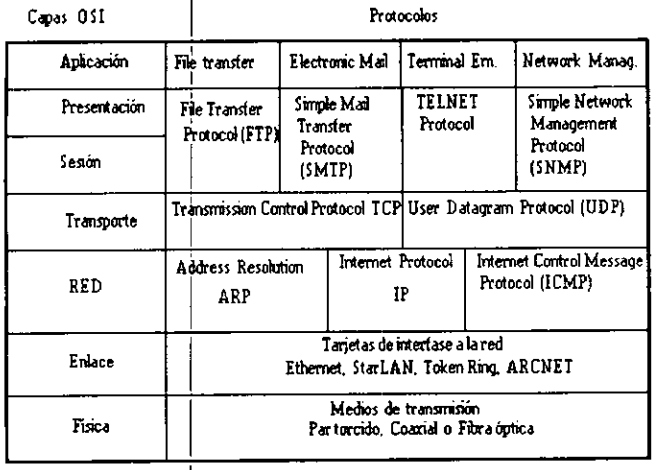


Figura. 1.15 Protocolos en el modelo OSI

CAPITULO 2

REDES LAN

2.1 Elementos de una red

Una red para su funcionamiento, necesita de una serie de elementos que le permiten dar un mejor servicio, los elementos más importantes para la intercomunicación de redes son: repetidores, puentes, ruteadores, compuertas y switches.

Podemos también definir lo que es un sistema intermedio (IS). Un sistema intermedio es un dispositivo usado para conectar dos subredes y permite comunicación entre sistemas finales conectados a diferentes subredes. Partiendo de esta definición del concepto IS podemos definir los elementos de una red.

2.1.1 Repetidor

Los repetidores son simplemente dispositivos que amplifican y reconfiguran la forma de la señal en una red y la pasan a otra. Los repetidores son usados para prolongar las distancias de cable de una red local. Y también conectan redes idénticas al nivel mas bajo de hardware: por ejemplo, Ethernet a Ethernet, Token Ring a Token Ring, StarLAN a StarLAN, etc.

A causa de que los repetidores simplemente repiten señales y no proporcionan ningún tipo de capacidad de filtrado de los paquetes de datos, todo el tráfico en todas las redes conectadas por uno o m{as repetidores se propaga a todos los otros, lo cual puede tener un efecto muy negativo en el óptimo funcionamiento de la red.

2.1.2 Puente (Bridge)

Los "bridges", como los repetidores, conectan redes en el nivel de hardware. Mientras que los repetidores conectan las redes al nivel fisico mas bajo, los

bridges conectan al nivel de hardware más alto, el cual recibe el nombre de nivel MAC (control de acceso al medio).

En general, los "bridges" son específicos del hardware: Ethernet a Ethernet, Token Ring a Token Ring, etc. Por ejemplo, un "bridge" Ethernet permitirá a dos o más redes Ethernet ser conectadas e interoperar juntas, sin depender de los protocolos o sistemas operativo de red que estén siendo usados.

Teóricamente, los bridges pueden usarse para conectar cualquier red que respeta el estándar 802; en la práctica ha sido muy difícil implementar bridges entre Ethernet y Token Ring, a causa de las diferencias entre los dos estándares.

Los "bridges" utilizan tablas de ruta para determinar qué tráfico reexpedir a otros dispositivos a través del "bridge". Esto significa que el tráfico local permanece local, mientras que el tráfico entre redes puede atravesar el bridge. El tráfico local en una red no afectará el funcionamiento en otra red que utilice un bridge.

Para un correcto funcionamiento, un bridge debe conocer las direcciones de todos los dispositivos a los cuales expedir paquetes. La funcionalidad de un bridge es medida normalmente de dos maneras: por el número de paquetes que puede filtrar o examinar y por el número de paquetes que puede reexpedir o pasar a otra red.

El número de filtraje de los productos actuales está entre los 2000 y 25000 paquetes por segundo, mientras que el número de paquetes que se reexpiden está entre 1500 y 15000 paquetes por segundo.

Los bridges pueden ser aparatos independientes del computador, o un hardware y software instalado en una PC.

2.1.3 Ruteador

Los ruteadores operan al nivel de protocolo, y son por lo tanto independientes del hardware. En lugar de reexpedir paquetes, reexpiden los datos en los paquetes. Los ruteadores son específicos de los protocolos: un ruteador debe saber el o los puertos usados por los datos que están siendo reexpedidos.

Ya que los ruteadores operan al nivel de protocolo, pueden usarse para conectar redes no similares, tales como ARCnet y Ethernet, Ethernet y Token Ring. Como los bridges, los ruteadores solo reexpiden el tráfico dirigido al otro lado. Esto significa que el tráfico local en una red no afectará el funcionamiento de otra. También como los puentes, los ruteadores pueden ser dispositivos aislados o un conjunto de hardware y software, para una PC. Los ruteadores son muy útiles para interconectar redes similares y no similares, así como para limitar el tráfico medio de una red.

2.1.4 Switch

Los switches de datos, también conocidos como puertos de selección o dispositivos de contención de puertos, han estado en los ambientes de computo mainframes desde los 70's. Esto permite a un número de usuarios compartir un número relativamente limitado de puertos de uno o más hosts y sus periféricos asociados. Antes de esto las terminales estaban conectadas permanentemente a los puertos. Y los usuarios que requerían acceso a otras computadoras o periféricos tenían que hacerlo a través de otras terminales o hacer el cambio de conexión manualmente. Con los años, los switches han evolucionado de puertos de selección relativamente simples a sofisticados controladores de comunicaciones en LAN's y WAN's.

En contraste con los switches de matriz, los cuales son diseñados para conexiones permanentes bajo el control de un administrador de red, los switches de datos están diseñados para establecer conexiones dinámicas bajo el control de usuarios individuales conforme lo requieran. En los últimos años, los fabricantes de switches de datos han dado grandes pasos para convertir el switch de datos en una herramienta poderosa para la administración multifuncional de la red. Tal sofisticación ofrece una migración económica para las LAN's. Para los usuarios de este tipo de redes, el switch de datos es un eficiente servidor o compuerta para paquetes y redes T1.

2.1.5 Compuerta

Las compuertas operan al nivel de red. Esto les proporciona más flexibilidad, al poder interpretar y traducir direcciones entre redes distintas, pero también trabajan mucho más lentamente.

Las compuertas son usadas principalmente en redes WAN donde no se espera que nadie utilice más de 10000 paquetes por segundo, uno de los requerimientos importantes para un bridge en una red de área local.

Antes de describir las características de las topologías LAN podemos mencionar que el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha establecido seis comités para el desarrollo de estándares para redes de área local -LAN's-. En conjunto, estos grupos son llamados los Comités para Estándares de LAN's IEEE 802:

- **IEEE 802.1** Estándar para redes de área local y urbana. Generalidades y arquitectura. Direccionamiento, funcionamiento interno y gestión de las redes de área local. Higher Layers and Management (HILI).
- **IEEE 802.2** Estándar para redes de área local, control de enlace lógico. Logical Link Control (LLC).
- **IEEE 802.3** CSMA/CD (Ethernet) Método de acceso y especificación del nivel lógico.
- **IEEE 802.4** Bus con paso de testigo, Token Passing Bus. Método de acceso y especificación del nivel físico.
- **IEEE 802.5** Anillo con paso de testigo, Token Passing Rin. Método de acceso y especificación del nivel físico.
- **IEEE 802.6** Estándar para redes de área urbana. Metropolitan Area Networks (MAN).
- **IEEE 802.7** Estándar para red de área local de banda ancha.
- **IEEE 802.8** Estándar para fibra óptica.

La arquitectura LAN fue creada por el comité 802 del IEEE y ha sido adoptada por todas las organizaciones que trabajan en base a los estándares de especificaciones LAN. Y se conoce generalmente como el modelo de referencia IEEE 802.

En este punto definiremos algunos principios relacionados con el estándar 802.2 LLC. Si partimos de la capa más baja del modelo de referencia del IEEE 802 corresponde a la capa física del modelo OSI e incluye funciones tales como:

- Codificación/Decodificación de señales
- Generación de preámbulo/remoción (para sincronización)
- Transmisión de bit/Recepción

Además, la capa física modelo 802 incluye una especificación del medio de transmisión. Generalmente, esta es considerada "más abajo" de la capa inferior del modelo OSI. No obstante, la elección un medio de transmisión es crítica en el diseño LAN, así que se incluye una especificación del medio.

Sobre la capa física están las funciones asociadas a proporcionar servicios a los usuarios LAN. Estos incluyen:

- Proporcionar uno o más puntos de acceso de servicio (SAP's).
- En la transmisión, ensamblar los datos dentro de una trama con campos de dirección y de detección de errores.
- En la recepción, desensamblar las tramas y realizar reconocimiento de direcciones y detección de errores.
- Gobernar el acceso al medio de transmisión de la LAN.

Estas son funciones típicas asociadas con la capa dos de OSI. La primera función, y las demás funciones, están agrupadas en la capa de control de enlace lógico (LLC). Las ultimas tres funciones son tratadas en una capa separada, llamada control de acceso al medio (MAC). Esto se hace por las siguientes razones:

- La lógica requerida para el control del acceso al medio compartido no se encuentra en la tradicional capa dos de control de enlace de datos.
- Para el mismo LLC, muchas opciones de MAC pueden ser proporcionadas.

La capa LLC para las LAN's es similar en muchos aspectos a otras capas de enlaces de uso común. Como todas las capas de enlace; LLC tiene que ver con la transmisión de una unidad de protocolo de datos (PDU) entre dos estaciones, sin la necesidad de un nodo intermedio de conmutación. LLC tiene dos características que no comparte con la mayoría de los otros protocolos de control de enlace:

- Debe soportar el multiacceso, debido a la naturaleza de medio compartido del enlace (esto difiere de una línea multipunto en que no hay un nodo primario).
- Es relevado de algunos detalles del acceso al enlace por la capa MAC.

La figura 2.1 nos ayuda a clarificar los requerimientos para la capa de enlace. Considere dos estaciones que se comunican vía un medio compartido LAN. Las capas altas, más arriba que LLC, proporcionan servicios punto a punto entre las estaciones. La capa LLC es también punto a punto, proporcionando el servicio de la capa 2 de OSI. Debajo de la capa LLC, el MAC proporciona la lógica necesaria para lograr el acceso a la red. Típicamente, las unidades protocolo de datos al nivel MAC, llamadas tramas MAC, son comunicadas punto a punto sin

alteraciones. De cualquier modo, conceptualmente, la capa MAC de una estación interactúa con el medio de la red para llevar a cabo el protocolo de control de acceso.

Como un protocolo punto a punto, existen tres servicios fundamentales que pueden ser realizados por LLC:

- **Servicio no conexión:** un servicio que no requiere establecimiento de una conexión lógica es necesario para soportar un tráfico interactivo alto.
- **Orientado a conexión:** un servicio orientado a conexión es conveniente para soportar ciertos tipos de tráfico.
- **Multiplexaje:** generalmente, un solo enlace físico une una estación a una LAN; podría ser posible llevar a cabo una transferencia de datos con muchos puntos terminales lógicos sobre ese enlace.

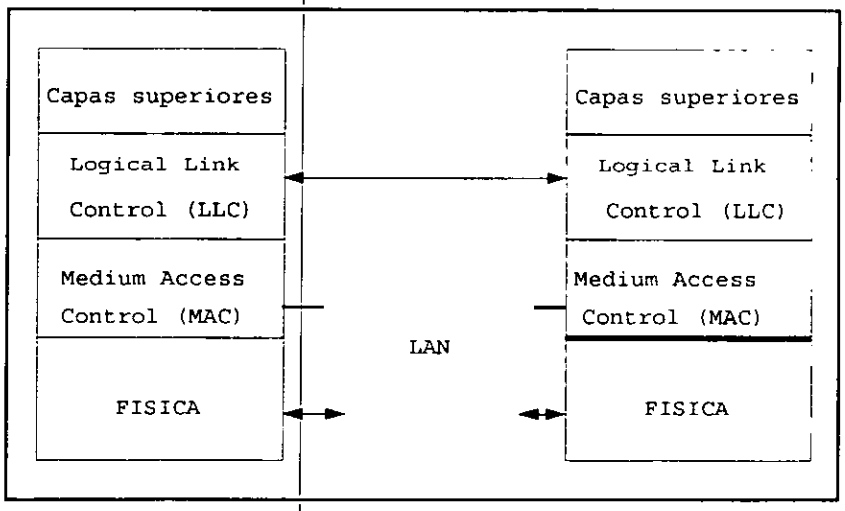


Figura 2.1 Capa de enlace.

El servicio no orientado a conexión es soportado fácilmente al proporcionar la información apropiada de direccionamiento. Debido a que un PDU LLC transmitido puede ser enviado a una de muchas estaciones en el medio, y también porque un PDU LLC recibido puede venir de una de muchas estaciones en el medio, por lo que se requieren tanto las direcciones de destino como las de la fuente.

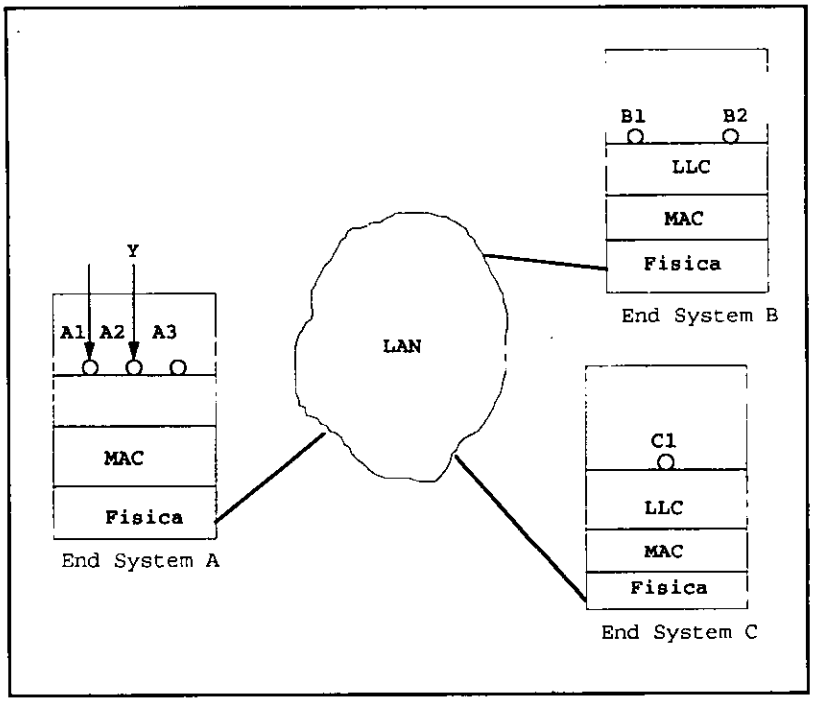


Figura 2.2 Intercambio entre estaciones

Tanto las capacidades del multiplexaje como las de orientado a conexión pueden ser soportadas con el concepto de punto de acceso al servicio (Service Access Point SAP). Un ejemplo nos puede aclarar esto. La figura 2.2 muestra tres estaciones unidas a una LAN. Cada estación tiene una dirección única. Adicionalmente, LLC soporta múltiples SAP's cada uno con su propia dirección LSAP. Asumiendo que el proceso o aplicación en la estación A desea enviar un mensaje a un proceso en la estación C. X puede ser un programa generador de reportes en una estación de trabajo; C puede ser un impresor o un driver de impresor simple. X se une el mismo a un LSAP 1 y solicita una conexión a la estación C, LSAP 1 (C puede tener solamente un LSAP sí solo es una sola impresora). El LLC en A envía a la LAN una solicitud de conexión PDU que incluye la dirección fuente (A,1), la dirección destino (C,1), y algunos bits de control indicando què es una solicitud de conexión. La LAN entrega esta trama a C, la cual, si esta libre, regresa un PDU de aceptación de conexión. En lo sucesivo, todos los datos de X serán transmitidos en PDU's que incluyen las direcciones fuente (A,1) y destino (C,1). Cualquier dato del impresor (por

ejemplo, conocimientos, reportes) serán transmitidos en PDU's que incluyen (A,1) y (C,1) como direcciones de fuente y destino. Al mismo tiempo, el proceso Y podría unir (A,2) e intercambiar datos con (B,1). Este es un ejemplo de multiplexaje. Además, otro proceso en A podría usar (A,3) para enviar PDU's no-conexión a varios destinos.

Una función final de la capa de enlace podría ser incluida en nuestra lista, para tomar ventaja de la naturaleza de medio compartido de las LAN:

- Multicast, broadcast. La capa de enlace puede proporcionar el servicio de enviar un mensaje a muchas estaciones o a todas.

La discusión anterior se refiere tanto a las direcciones de las estaciones como de LLC. Para entender la función de direccionamiento, necesitamos considerar los requerimientos para intercambiar datos.

En términos generales, se puede decir que involucra tres agentes, procesos, estaciones, y redes. Los procesos de los cuales nos ocupamos aquí son aplicaciones distribuidas que involucran el intercambio de datos entre dos sistemas de computo. Estos procesos, y otros se ejecutan en estaciones que pueden soportar a menudo aplicaciones múltiples simultáneas. Un ejemplo es una operación de transferencia de archivo, que involucra un proceso de transferencia de archivos en una estación intercambiando datos con un proceso de transferencia de archivo en otra estación. Otro ejemplo, es el acceso a una terminal remota, en el cual un proceso de emulación de terminal en una estación de trabajo conecta esa estación a un servidor remoto. Las estaciones son conectadas por una red, y los datos a intercambiar son transferidos por la red de una estación a otra. Así, la transferencia de datos de un proceso a otro involucra el obtener primero los datos de la estación en la cual reside el proceso de destino y entonces ponerlo al alcance de la computadora. Estos conceptos sugieren la necesidad para dos niveles de direccionamiento. Consideremos la figura 2.3, que muestra la relación entre Los PDU's LLC y las tramas MAC. Los datos de usuario LLC (por ejemplo un datagrama IP) para ser enviado se pasa hacia LLC, que le coloca un encabezado. Este "header" contiene la información de control que es usada para operar el protocolo entre la entidad local LLC y la entidad remota LLC. La combinación de datos de usuario y el encabezado LLC se refiere como un PDU LLC. Después que el LLC fuente ha preparado un PDU, el PDU es pasado como un bloque de datos hacia la entidad MAC. La entidad MAC coloca tanto un "header" como un "trailer", para llevar a cabo el protocolo MAC. El resultado es un PDU al nivel

MAC. Para evitar confusiones con un PDU al nivel LLC, el PDU MAC es referido usualmente como una trama.

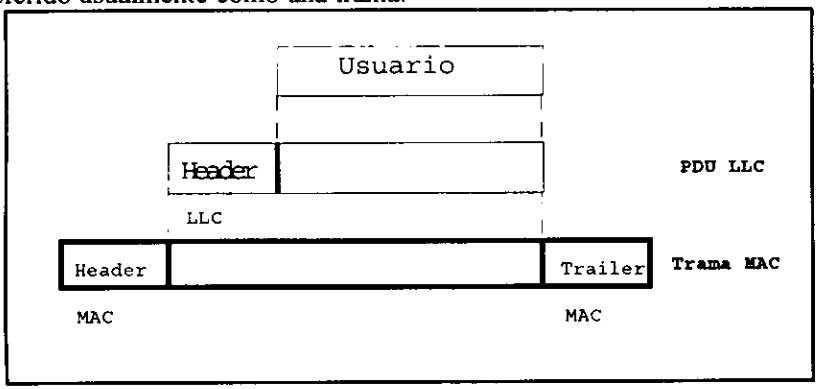


Figura 2.3 Protocolo de control de información LAN

El "header" MAC debe contener una dirección destino que únicamente identifique una estación en la LAN. Esto es necesario debido a que cada estación dentro de la LAN leerá el campo de la dirección destino para determinar si debería capturar la trama MAC. Cuando se captura una trama MAC, la entidad de destino MAC elimina el "header" y el "trailer" MAC y pasa el PDU LLC resultante hacia la entidad LLC. El "header" LLC debe contener una dirección de destino SAP para que el LLC pueda determinar hacia donde deben ser entregados los datos. Por tanto, son necesarios dos niveles de direccionamiento:

- Direccionamiento MAC: identifica una interface física de la estación a la LAN. En la mayoría de los casos hay una relación uno a uno entre las estaciones y las direcciones físicas. En otros casos una estación única puede tener múltiples uniones al mismo medio por razones de desempeño o confiabilidad. En otros casos, tales como un ruteador o puente, una estación puede tener interfaces físicas a más de una LAN.

- Direccionamiento LLC: identifica un usuario LLC. La dirección LLC esta asociada con un usuario en particular dentro de una estación. En algunos casos el SAP se refiere a un proceso ejecutándose en una estación. En otros casos el SAP se puede referir a un puerto hardware. Por ejemplo, un dispositivo de concentración de terminales puede proporcionar uniones a una LAN por múltiples terminales, cada una conectada a un concentrador a través de un puerto físico diferente.

Hemos discutido el uso de direcciones que identifican entidades únicas. Además de estas direcciones individuales; también se utilizan direcciones en grupo. Las direcciones en grupo especifican un conjunto de una o más entidades. Por ejemplo, una podría desear enviar un mensaje a todos los usuarios unidos a un concentrador en particular o a todas las terminales y estaciones de trabajo en la LAN entera. Se utilizan dos tipos de direcciones de grupo. Una dirección broadcast se refiere a todas las entidades dentro de un contexto; cada entidad en ese contexto interpretaría la dirección broadcast como un PDU direccionado al mismo. Una dirección multiestación se refiere a un subarreglo de entidades dentro de algún contexto; cada entidad en ese subarreglo interpretaría la dirección multicast correspondiente como un PDU direccionado hacia allá.

La figura 2.4 ilustra las posibles combinaciones. Las primeras tres combinaciones son directas; se puede direccionar un usuario especifico, o un grupo de usuarios o todos los usuarios de una estación específica pueden ser direccionados. Las alternativas (f) e (i) se pueden también entender fácilmente: Una puede desear direccionar a todos los usuarios en algunas estaciones o todos los usuarios a todas las estaciones.

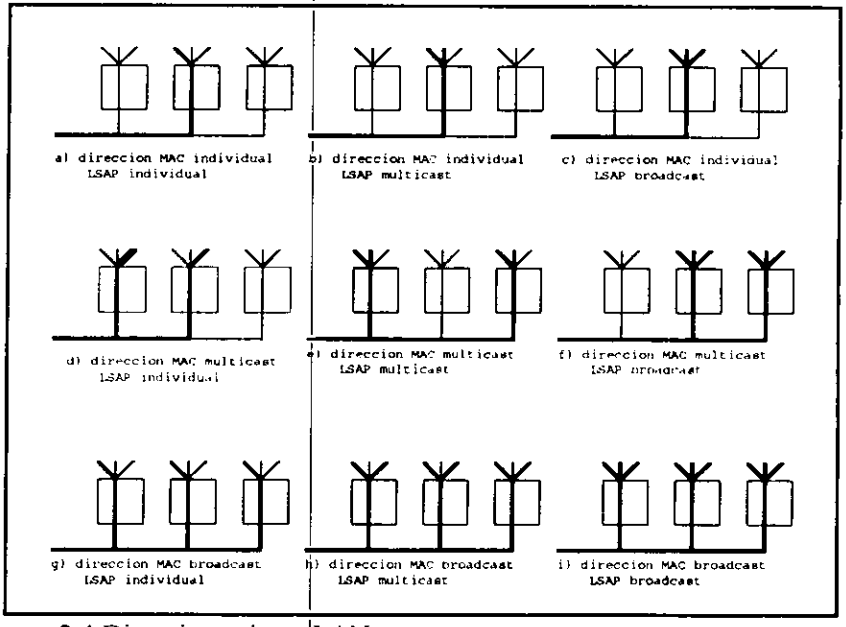


Figura 2.4 Direccionamiento LAN.

Las restantes cuatro alternativas en la figura son quizás menos fáciles de entender. Para entender su uso, necesitamos reconocer que los LSAP's son únicas solamente con una estación individual. Es solamente la entidad LLC dentro de una estación quién examina el "header" LLC y determina el usuario. De cualquier forma, es posible asignar LSAP's únicamente a través de todas las estaciones. Eso es indeseable por las siguientes razones:

1. El número total de usuarios LLC en todas las estaciones debería ser limitado por el largo del campo LSAP en el "header" LLC.
2. Un control central se requiere en la asignación de LSAP, no importa cuan larga y heterogénea sea la población de usuarios.

Por otra parte, es útil tener ciertas direcciones LSAP dedicadas que son las mismas en todas las estaciones. Por ejemplo, una entidad de control en una estación puede dársele siempre un LSAP con valor de 1, para facilitar la administración de la red. O a un grupo de entidades de control y administración dentro de una estación pueden tener la misma dirección multicast LSAP. Cuando se sigue tal convención, se vuelve posible direccionar datos a un LSAP o a un LSAP multicast en un grupo de estaciones o a todas las estaciones.

Por otro lado, todas las LAN's y MAN's consisten de una colección de dispositivos que deben compartir la capacidad de transmisión de la red. Algunos medios de controlar el acceso al medio de transmisión son necesarios para proporcionar un uso ordenado y eficiente de la capacidad. Esta es la función del protocolo de control de acceso al medio (MAC).

Los parámetros clave en cualquier técnica de control de acceso al medio son como y donde. Donde se refiere a sí el control es ejercido en tipo centralizado o distribuido. En un esquema centralizado se designa un controlador que tiene la autoridad de conceder acceso a la red. Una estación que desea transmitir debe esperar hasta que recibe permiso del controlador. En un esquema descentralizado las estaciones llevan a cabo colectivamente una función de control de acceso al medio para determinar el orden en el cual transmitirán las estaciones. Un esquema centralizado tiene ciertas ventajas, incluyendo:

- Puede proporcionar un gran control sobre el acceso indicando cosas como prioridades, overrides, y capacidad garantizada.
- Activa el uso de acceso lógico relativamente simple en cada estación.
- Evita problemas de coordinación distribuida entre entidades.

Las principales desventajas de los esquemas centralizados son:

- Crea un único punto de falla, esto es, existe un punto en la red que, si falla, causa que la red entera falle.
- Puede actuar como cuello de botella, reduciendo el desempeño.

Los pros y contras de los esquemas distribuidos son idénticos a los puntos anteriores.

El segundo parámetro, cómo es estrechado por la topología y es un tratado entre factores que compiten, incluyendo costos, desempeño, y complejidad. En general, podemos categorizar las técnicas de control de acceso como síncronas o asíncronas. Con técnicas síncronas, una capacidad específica se dedica a conexión. Este es el mismo acercamiento usado en conmutación de circuitos, multiplexaje por división de frecuencia (FDM), y multiplexaje por división de tiempo síncrono (TDM). Tales técnicas no son generalmente óptimas en LAN´s y MAN´s porque las necesidades de las estaciones son impredecibles. Es preferible que sea posible localizar capacidad en un modo asíncrono (dinámico), más o menos en respuesta de una demanda inmediata. La aproximación asíncrona puede ser subdividida dentro de tres categorías:

- **Round Robin.** Con "Round Robin", a cada estación en turno se le da la oportunidad de transmitir. Durante esa oportunidad, la estación puede declinar transmitir o puede transmitir sujeto a una especificación superior, usualmente como un monto máximo de datos transmitidos o tiempo para esta oportunidad. En cualquier caso, la estación, cuando termina, pasa su turno, y el derecho a transmitir pasa a la siguiente estación en la secuencia lógica. El control de la secuencia puede ser centralizado o distribuido. Cuando muchas estaciones tienen datos a transmitir en un extenso período de tiempo, las técnicas de "Round Robin" pueden ser muy eficientes. Si solamente unas pocas estaciones tienen datos a transmitir en un largo período de tiempo, existe un considerable exceso al pasar el turno de estación en estación, hasta que llega el momento en que las estaciones no transmiten sino simplemente pasan sus turnos. Bajo tales circunstancias deben preferirse otras técnicas, ampliamente dependientes en si el tráfico de datos tiene una cadena o característica de series. El tráfico de cadenas es caracterizado por el largo de las transmisiones; ejemplos como la comunicación de voz, telemetría y la transferencia en masa de archivos. El tráfico en ráfaga se caracteriza por transmisiones cortas y esporádicas, el tráfico interactivo entre terminal y host es un ejemplo de esta descripción.

- **Reservación.** Para el tráfico encadenado, las técnicas de reservación están bien situadas. En general, para estas técnicas, el tiempo en el medio se divide en ranuras, muy parecidas a las de TDM. Una estación que desea transmitir reserva ranuras futuras para un período extendido o incluso un período indefinido. Otra vez, la reservación puede ser hecha en modo centralizado o distribuido.

- **Contención.** Para tráfico en ráfaga, las técnicas de contención son usualmente apropiadas. Con estas técnicas, no se ejercita ningún control para determinar de quién es turno de transmitir; todas las estaciones contienden por un tiempo para transmitir que puede ser, como veremos, bastante confuso y escabroso. Estas técnicas son de necesidad distribuida por naturaleza. Su principal ventaja es que son simples de implementar y, a carga moderada eficientes. Para algunas de estas técnicas, el desempeño tiende a colapsarse bajo carga pesada. No obstante que han sido implementadas técnicas centralizadas y distribuidas de reservación en algunos productos LAN, las técnicas más comunes son la contención y el "Round Robin".

♦ Formato de trama MAC

La capa MAC recibe un bloque de datos de la capa LLC y es responsable de llevar a cabo funciones relacionadas al acceso al medio y la transmisión de datos. Como con otras capas de protocolo, MAC implementa estas funciones haciendo uso de una unidad de protocolo de datos en su capa. En este caso el PDU se refiere como trama MAC.

El formato exacto de la trama MAC difiere algo de los protocolos MAC en uso. En general, todas las tramas MAC tienen un formato similar al de la figura 2.6. Los campos de esta trama son:

- **Control MAC:** contiene toda la información de control del protocolo necesaria para el funcionamiento del protocolo. Por ejemplo, un nivel de prioridad se podría indicar.
- **Dirección destino MAC**: el punto físico de destino se une a la red por esta trama.
- **Dirección fuente MAC:** el punto físico fuente se une a la LAN por esta trama.
- **LLC:** los datos LLC de la capa anterior.

- **CRC:** el campo de chequeo de redundancia cíclica (también conocido como el campo de chequeo de secuencia (FCS). El campo CRC es una función de los contenidos del control, direccionamiento, y campos LLC. Es generado por el enviante y después por el receptor. Si el resultado en el receptor difiere del valor recibido en el campo CRC, un error en la transmisión a ocurrido.

	BUS	ANILLO	SWITCHED
Round Robin	Token bus 802.4 Polling 802.11	Token Ring FDDI 802.5	Request/priority 802.12
Reservacion	DQDB 802.6		
Contencion	CSMA/CD 802.3 CSMA 802.11		CSMA/CD 802.3

Tabla 2.5 Estándar de técnicas de control de acceso al medio.

En la mayoría de los protocolos de control de enlace de datos, la entidad de protocolo de enlace de datos es responsable no sólo de detectar errores usando el CRC, sino de recobrarlos retransmitiendo las tramas dañadas. En la arquitectura del protocolo LAN, estas dos funciones se encuentran colocadas entre la capa MAC y LLC. La capa MAC es responsable de detectar errores y descartar cualquier trama con error. Opcionalmente, la capa LLC mantiene registro de cuales tramas han sido recibidas exitosamente y retransmite tramas no exitosas. La figura 2.7 coloca la trama MAC y el PDU LLC en el contexto de la transmisión TCP/IP. Cada capa agrega campos que son necesarios para la operación del protocolo en esa capa.

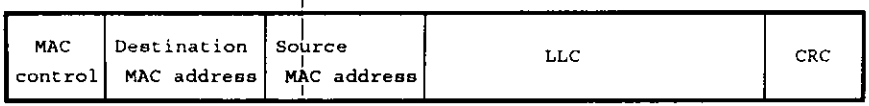


Figura 2.6 Formato de la trama MAC general.

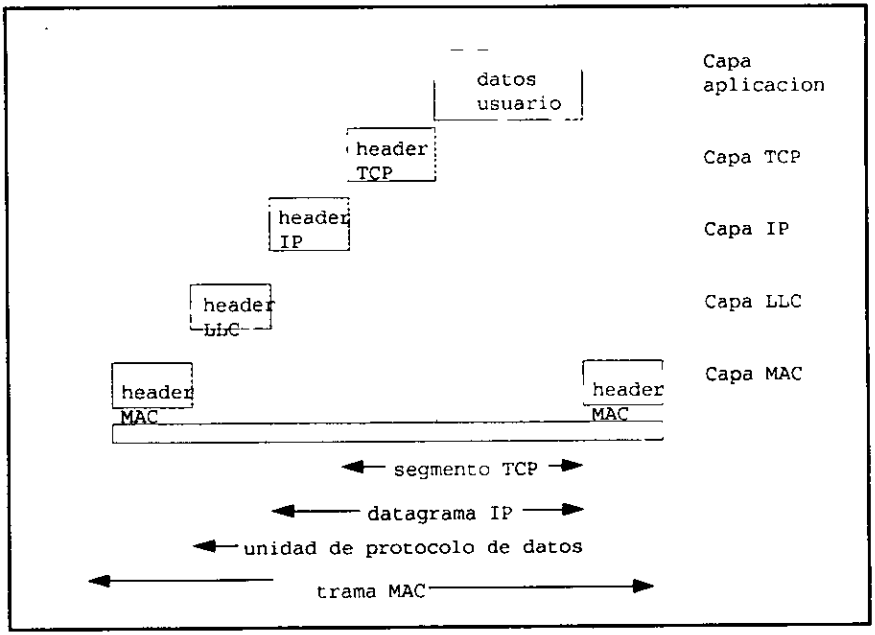


Figura 2.7 Trama MAC y PDU LLC en TCP/IP.

2.2 Ethernet

2.2.1 Topología

Topología quiere decir, la manera en como se interconectan los usuarios entre sí. Si queremos definir topología debemos hacerlo de dos maneras; una topología física y una lógica. La topología física tiene que ver con la manera en que los nodos se conectan entre ellos a través de un medio físico (cable), por ejemplo, la conexión más común es la de estrella, en la que todos los nodos están unidos a un concentrador.

La topología lógica tiene que ver en como estos nodos tienen acceso a su medio físico, tomando el ejemplo del párrafo anterior, los nodos tienen los cables conectados al concentrador, pero este internamente, tiene un arreglo particular para que estos nodos intercambien información entre ellos bajo la dirección de un servidor (software).

El método más conocido para el control de una red de área local en una estructura de bus es el método de Acceso Múltiple con Detección de Portadora (CSMA- Carrier Sense Múltiple Access). Este método está ampliamente utilizado en Ethernet.

Ethernet fue de desarrollado a través de los esfuerzos conjuntos de Xerox, Digital Equipment Corporation e Intel Corporation. Una vez concluido el trabajo de estas tres grandes compañías, esta especificación fue introducida en IEEE como 802.3

A CSMA también se le llama el método de contención, ya que las estaciones de la red compiten entre ellas por el acceso al cable. Cuando una estación en la red está preparada para enviar un paquete de información a otra estación, primero escucha la actividad en el cable para ver si otro paquete está a su vez siendo transmitido por otra estación. Si no oye otra señal en la línea, transmitirá el paquete de información. Si oyera otra señal, esperaría un tiempo aleatorio, comprobaría la línea otra vez, y enviaría el paquete de datos cuando estuviera libre.

En las redes Ethernet, los paquetes de información son transmitidos a lo largo de toda la red, pero sólo recogidos y aceptados por la estación a la que han sido direccionados.

En la práctica siempre existe la posibilidad de que dos o más estaciones intenten transmitir al mismo tiempo. Para prevenir este estado, IEEE 802.3 utiliza un método para la detección de la colisión -CD Collision Detection-. Al detectar una colisión, la estación de trabajo involucrada esperará un período de tiempo aleatorio, para reducir la probabilidad de volver a colisionar, y volverá a transmitir de nuevo.

El acceso a la red es aleatorio, no está garantizado. A causa de la contención por el acceso, el método CSMA es probabilístico, es decir, que una estación tiene cierta probabilidad de acceso a la red en un intervalo dado de tiempo, pero nunca una garantía.

En una red extremadamente ocupada por un intenso tráfico de paquetes de información, o por un malfuncionamiento de red, debido a causas de hardware o de instalación de cableado, la degradación en el funcionamiento aumenta rápidamente debido a que las colisiones entre paquetes aumentan y la red se acerca a punto de saturación.

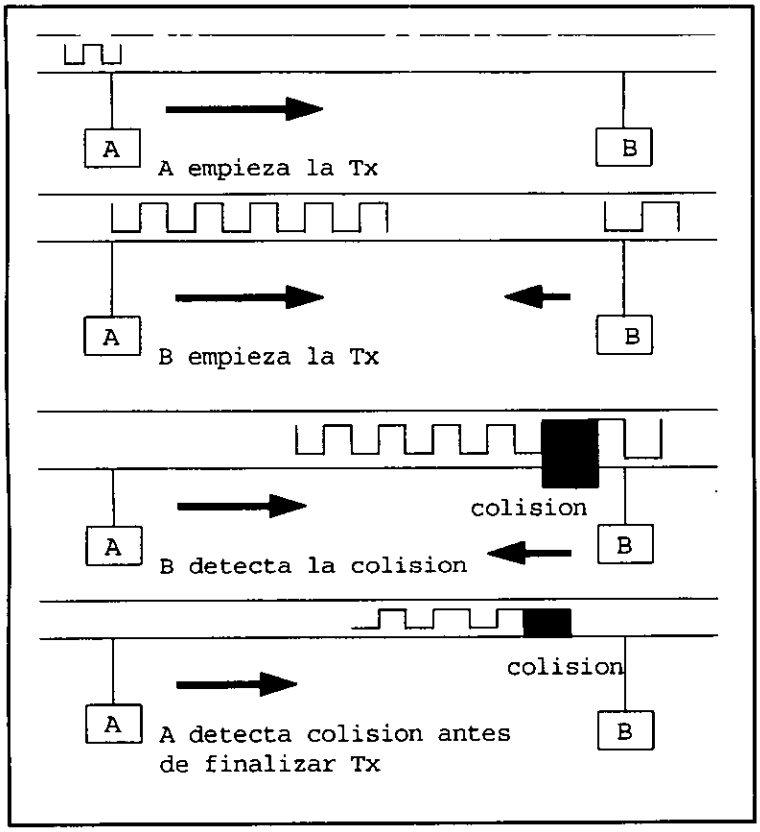


Figura 2.8 Método de colisión.

No obstante, en una red debidamente diseñada y con un adecuado funcionamiento, esta situación se produce raramente.

Ethernet es ampliamente aceptada y soportada por la industria. Cuando se necesita interconectividad en una gran red, Ethernet es siempre el estándar escogido. Además, los más importantes sistemas operativos de red están disponibles para Ethernet.

Ethernet es una de los ejemplos mejor conocidos de una LAN basada en una topología bus (ver capítulo 1), no obstante existen otras variedades, tales como árbol, malla y delta. La topología en bus esta basada en contención, típicamente

operando a una velocidad de 10Mb/s, a través del método CSMA/CD, regula como 2 o más estaciones comparten el medio de transmisión en bus.

La ventana de colisión impone un límite práctico en el largo de la red en bus. En el estándar 802.3 para contención de redes, el IEEE reconoce 2500 metros como el largo máximo en el bus, sin importar el número de repetidores, la velocidad o el tipo de cable. Un solo segmento puede alcanzar 500 metros antes de que se necesiten repetidores para extender el bus más allá de sus límites. Mientras tales dispositivos amplifican y reconstituyen señales débiles que pueden causar daño a los paquetes de datos, no compensan los retrasos en la propagación de la señal que afectan el método de acceso CSMA/CD empleado por Ethernet. De hecho, incrementan el retraso en la red, el cual puede incrementar la probabilidad de colisiones. No obstante, el uso de repetidores en LAN´s de alta velocidad esto no garantiza el desempeño de la LAN; de hecho, el desempeño se puede deteriorar con incrementos en el tráfico.

Las redes en bus típicamente cuestan menos en su implementación que otros tipos de redes. Debido a que cada dispositivo en la red es una unidad independiente, la falla de uno de ellos no afecta necesariamente a los otros. Se pueden agregar terminales o removerlas de la red sin interrumpir el servicio.

Si la red en bus, permanece estática, existe tráfico uniforme en tiempo, y los usuarios pueden tolerar algún retraso en las retransmisiones causadas por colisiones de adquisición de señales, el método de acceso CSMA/CD puede ser una elección económica para redes locales. Pero la redes tienen la tendencia a crecer conforme las necesidades de las organizaciones crecen y se vuelven sofisticadas. Conforme el número de terminales se incrementa y el volumen de tráfico crece, así como las posibilidades de colisión. Es entonces cuando CSMA/CD puede causar problemas. CSMA con anulación de colisiones (CSMA/CA) puede ayudar a evitar algunas colisiones, pero puede incrementar el retraso de las terminales al medio. Muchas aplicaciones pueden no tolerar los largos retrasos inherentes a estos métodos de acceso.

Controlando el flujo de información puede ser otro problema inherente en la arquitectura Ethernet, dependiendo del tráfico de la red. El único modo de que un dispositivo receptor pueda rechazar un mensaje es descartándolo, a menos de que exista control de flujo en la capa de transporte. Los mensajes son normalmente numerados así que cuando no hay reconocimiento pueden ser retransmitidas. Descartar mensajes no es un método efectivo de lidiar con condiciones de

sobrecarga debido a que puede existir degradación substancial en el desempeño cuando las estaciones tratan de recuperar el mensaje al solicitar frecuentes solicitudes de retransmisión.

2.2.2 Trama

El estándar 802.3 define un formato de trama específico para ser usado en los datos a través de la red. Este formato, que contiene muchos campos, difiere ligeramente del puramente Ethernet, pero las diferencias, tales como el largo 802.3 que aparece en el campo de tipo, son cruciales.

- **Preámbulo:** La trama inicia con un campo de 8 bytes llamado preámbulo, el cual consiste de 56 bits alternando entre unos y ceros. Estos son usados para la sincronización y para marcar el inicio de la trama. El mismo patrón de bits es usado por el preámbulo puramente Ethernet como en el preámbulo IEEE 802.3, que incluye el campo delimitador de inicio de trama de 1 byte.

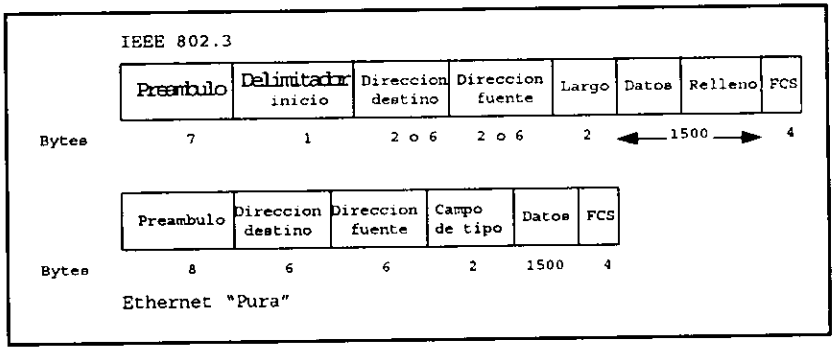


Figura 2.9 Comparación de las tramas Ethernet

- **Delimitador de inicio de trama:** El estándar especifica un campo delimitador de inicio de trama, el cual es realmente una parte del preámbulo. Se usa para indicar el inicio de la trama.

- **Campos de dirección:** El campo de dirección destino identifica las estaciones que recibirán la trama. El campo de dirección fuente identifica la estación que envía la trama. Si las direcciones son asignadas localmente, el campo de dirección puede ser tanto de 2 bytes (16 bits) como de 6 bytes (48 bits) de

largo. Una dirección destino se puede referir a una estación, un grupo de estaciones, o todas las estaciones. Ethernet especifica el uso de direcciones de 48 bits, mientras que IEEE 802.3 permite direcciones tanto de 16 o 48 bits.

- **Conteo de largo:** El campo de largo de datos que sigue es indicado por el campo de conteo de largo de 2 bytes. Este campo de especificación 802.3 determina el largo de la unidad de datos cuando se incluye en la trama un campo de relleno.

- **Campo de relleno:** Para detectar colisiones apropiadamente, la trama que es transmitida debe contener un cierto número de bytes. El estándar 802.3 especifica que si una trama que se ensambla para transmisión no cumple el mínimo de largo, se debe agregar un campo de relleno para completar largo requerido.

- **Campo de tipo:** Ethernet puro no soporta los campos de largo y relleno, como lo hace el 802.3. En vez de esto se utilizan 2 bytes que se usan para contener un campo de tipo. El valor especificado en el campo de tipo tiene solo significado para capas de la red superiores y no se define en la especificación original Ethernet.

- **Campo de datos:** Esta porción de la trama es pasada por la capa del cliente a la capa de enlace de datos en la forma de bytes de 8 bits. El tamaño mínimo de la trama es de 72 bytes, mientras que el tamaño máximo es de 1526 bytes, incluyendo el preámbulo. Si los datos a enviar usan una trama más pequeña que 72 bytes, el campo de relleno en 802.3 es usado para llenar la trama con bytes extras. Al definir un tamaño de trama mínimo, habrá pocos problemas para contener con la manipulación de colisiones. Si los datos a enviar usan una trama mas larga de 1526 bytes, es responsabilidad de las capas superiores romperla y organizarla en paquetes individuales usando un procedimiento llamado fragmentación. El máximo tamaño de trama refleja consideraciones prácticas relacionadas a los tamaños de las tarjetas buffer y la necesidad de limitar el tiempo que el medio es ocupado para transmitir una sola trama.

- **Chequeo de la secuencia de la trama**: Una trama adecuadamente formateada termina con la secuencia de chequeo de trama, el cual proporciona capacidad para chequeo de errores. Cuando una estación emisora ensambla una trama, realiza un calculo CRC sobre los bits de la trama. La estación emisora almacena el resultado de su calculo en un campo de 4 bytes de chequeo de

secuencia antes de enviar la trama. En la estación receptora, un calculo CRC idéntico se realiza y se compara con el valor original que se encuentra en el campo de chequeo de trama. Sí los dos valores no corresponden, la estación receptora asume que un error en la transmisión ha ocurrido y solicita que la trama se retransmita. En Ethernet pura, no existe corrección de errores; si los dos valores no corresponden, una notificación de que un error ha ocurrido se pasa a la capa del cliente.

2.2.3 Protocolo

El método usado para controlar el acceso al medio de transmisión, conocido como manejo de acceso al medio en términos IEEE, es llamado manejo de enlace en palabras Ethernet. El manejo de enlace es responsable de muchas funciones, comenzando con evitar las colisiones y el manejo de las mismas, los cuales son definidos por el estándar 802.3 para redes de contención.

El evitar colisiones implica monitorear la línea para conocer la presencia o ausencia de una señal (portadora). Esta es la porción de sensado de portadora de CSMA/CD. La ausencia de una señal indica que el canal no esta siendo usado y que es seguro transmitir. La detección de una señal indica que el canal esta ya en uso y que la transmisión debe esperar. Si no se detecta colisión durante el período conocido como ventana de colisión, la estación adquiere el canal y puede completar la transmisión sin arriesgarse a una colisión. Este método de evitar las colisiones limita la distancia sobre la cual puede operar Ethernet. Si el largo del cable es muy grande, una señal puede estar en el bus y no ser detectada durante la ventana de colisión debido al retraso en la propagación de la señal.

Cuando dos o más tramas son ofrecidas para la transmisión al mismo tiempo, ocurre una colisión, disparando la transmisión de una secuencia de bits llamada jam. Esto significa que todas las estaciones en la red reconocen que una colisión ha ocurrido. En este momento todas las transmisiones en progreso se suspenden.

Se intentan retransmisiones a intervalos calculados. Si existen colisiones repetidas, el manejador del enlace usa un proceso llamado *backing off* que involucra incrementar el promedio de esperas de retransmisión siguiendo colisiones sucesivas.

En el lado receptor, el manejador reconoce y filtra fragmentos de tramas que resultaron de una transmisión que fue interrumpida por una colisión. Cualquier

trama que es menor que el tamaño mínimo es supuesta como un fragmento de una colisión y no se reporta a la capa de cliente como un error.

La figura 2.10 ilustra las capas encontradas en CSMA/CD. La capa de usuario se sirve por dos capas CSMA/CD, la capa de enlace de datos y la capa física. Las dos capas más bajas consisten cada una de dos entidades separadas. La capa de enlace de datos proporcional control lógico actual a la red CSMA/CD. Es un medio independiente; consecuentemente, la banda puede ser de banda ancha o de banda base; el control de enlace de datos no importa. El estándar incluye ambas opciones banda base y banda ancha.

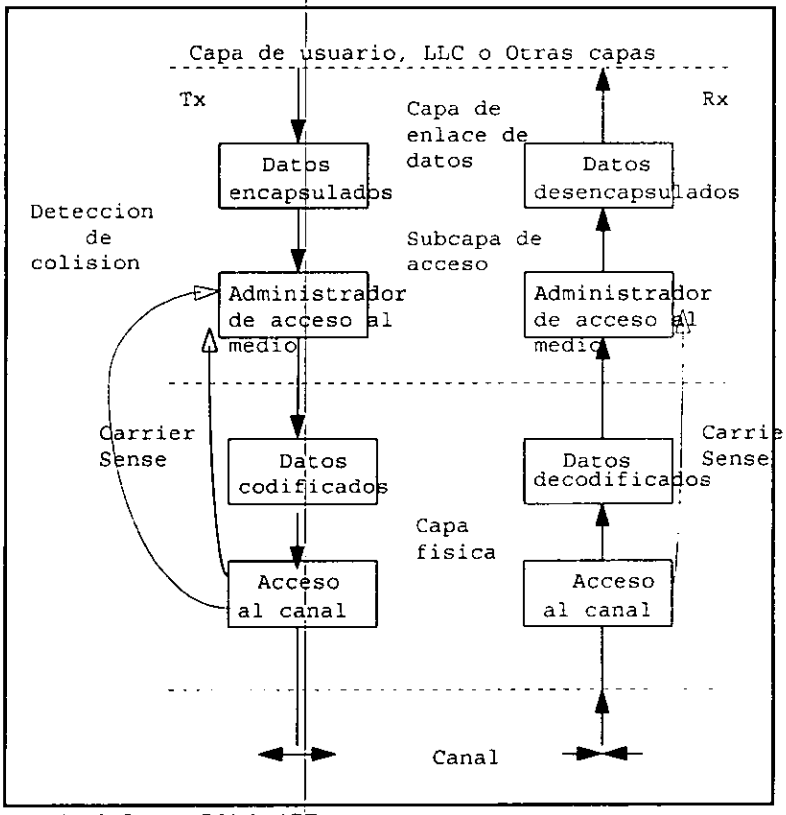


Figura 2.10 Capas CSMA/CD

Nuevos métodos están siendo descubiertos para mejorar el desempeño de Ethernet reduciendo o eliminando totalmente la oportunidad de colisión sin tener

que segmentar la LAN dentro de pequeñas subredes. Un vendedor ha descubierto un algoritmo que censa cuantas tramas están en curso de colisión. El algoritmo bloquea temporalmente una trama, mientras permite el paso a la otra. La compañía llama a este método CSMA con eliminación de colisión (CSMA/CE). CSMA/CE puede instalarse en una LAN Ethernet existente adicionando un concentrador inteligente y equipando cada microcomputadora con una tarjeta transreceptora.

La codificación se refiere al proceso de agregar bits para sincronización y convertir una señal binaria a una forma de codificación, confiable para una transmisión en Ethernet. El inverso de este proceso es la decodificación.

Además de la codificación y decodificación de datos, la capa física incluye funciones relacionadas con la unión de una estación a un medio particular de transmisión. Estas funciones son llevadas a cabo generalmente en un dispositivo separado llamado unidad de unión al medio (MAU), que se utiliza para conectar una estación de la red a un cable físico de transmisión.

Ethernet soporta tanto direcciones universales como específicas de red. Con el direccionamiento universal, a cada estación se le da una dirección que es única dentro de su red, pero puede ser la misma dirección en otra red. En este caso, cuando las redes están interconectadas, un identificador de red debe ser usado con la dirección de la estación para proporcionar una dirección única. Ethernet no especifica como deben ser usados los 48 bits de una dirección, lo que hace posible un direccionamiento específico de la red. De cualquier manera, es responsabilidad de las capas superiores de la red implementarla.

Tanto las redes universales como específicas, las direcciones pueden ser colocadas por la estación misma durante la inicialización. Cualquier trama enviada a esta dirección es recibida y procesada por la estación. Ethernet también soporta el uso de direcciones multicast y broadcast.

Una dirección consistente de todos "1" es definida como una dirección broadcast y es recibida por todas las estaciones. Una dirección multicast es asociada con un grupo particular de estaciones. Una dirección multicast es identificada por el valor "1" en el primer bit de la dirección. Cada estación puede ser activada o desactivada para multicast. Si esta activada, la estación acepta cualquier trama con direcciones multicast. Las capas altas deben entonces determinar si la estación es parte del grupo para una dirección multicast particular.

2.2.4 Medios de Transmisión

La especificación Ethernet define las características eléctricas, mecánicas y físicas para los componentes de un canal físico. La adherencia a especificaciones físicas ha permitido la manufactura de componentes de red por diferentes vendedores. Estos componentes pueden ser interconectados para formar una red única y funcional. Los requerimientos se detallan como sigue:

- Limites físicos de configuración, tales como largo del segmento de cable coaxial, número de repetidores, largo total de la ruta, y largo del cable transreceptor.
- Especificaciones de los componentes de cable coaxial, incluyendo el cable mismo, conectores y terminadores.
- Especificaciones de interface para un cable transreceptor y el transreceptor.
- Requerimientos de configuración y especificaciones ambientales.

La arquitectura Ethernet más común usa transmisión en banda base sobre cable coaxial a una velocidad de 10 Mb/s. La longitud máxima del cable es de 500 metros, lo cual se refiere como transmisión 10Base-5. Esta técnica quiere decir "velocidad 10Mb/s, señalización en banda base, con un largo por segmento de 500 metros". Las primeras instalaciones Ethernet usaban un cable coaxial de 50 ohms relativamente caro, con un diámetro de 10mm, que se conoce como "cable Ethernet grueso". Otro estándar de cable. 10Base-2, significa 10 Mb/s, señalización en banda base, 200 metros, usa cable coaxial ordinario tipo CATV, llamado "cable Ethernet delgado". Este es actualmente el tipo más común actualmente usado en Ethernet, no obstante el cableado con par torcido ha emergido como una alternativa viable. Bajo un estándar llamado 10Base-T, el cableado con par torcido ha superado al cable coaxial como el medio de transmisión preferido en Ethernet.

Esta migración de cable grueso a delgado en Ethernet, o "Cheapernet", al mismo par torcido usado en telefonía ahorra tanto en instalación como en el costo del cable. Esto ilustra la habilidad de la tecnología de redes de complacer las demandas de gran economía. Existe también un incremento en la demanda de ancho de banda en el tráfico en la red. Algunos han visto el incremento de la capacidad de Ethernet de 10Mb/s haciendo crecer los estándares; otros elevando el desempeño de las LAN's existentes a través de métodos de propietario.

2.3 Token Ring

2.3.1 Topología

La especificación IEEE 802.5 es para redes utilizando un método de acceso al medio físico por Token-Passing. Una red en anillo es un lazo cerrado en el cual los datos viajan en una dirección. Cada estación de la red está conectada por cable a la siguiente estación, formando así un anillo físico. Se recibe datos de la estación anterior y se transmiten a la estación siguiente. Para permitir una conexión y desconexión más fácil de todas las estaciones todos los cables van conectados a través de uno o más dispositivos concentradores o hubs.

En el hub, cada estación esta conectada a la estación anterior y posterior del anillo físico. Estos hubs llamados MAU´s (Multistation Access Units), y proporcionan automáticamente un by-pass de las estaciones desconectadas, manteniendo así la integridad del anillo.

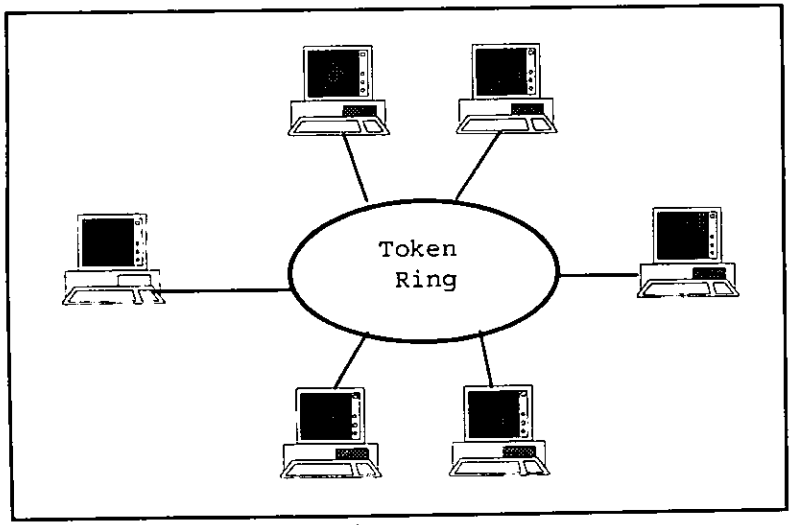


Figura 2.12 Topología Token Ring.

Un anillo usualmente trabaja con velocidades entre 4 o 16 Mb/s, además debido a que cada nodo actúa como un repetidor en donde los paquetes de datos y

el token son regenerados a su potencia original, estas redes no están limitadas por distancia o velocidad como las redes de tipo bus. En algunas configuraciones de hardware y cableado un anillo puede parecer una estrella aunque esto es solo fisicamente, porque lógicamente es un anillo. Ejemplos de estos los encontramos en la figura 2.12.

La topología en anillo ofrece múltiples ventajas tales como:

- Desde que el acceso a le red no esta determinado por un esquema de contención, una alta velocidad de envío es posible en situaciones de alto tráfico, limitada solamente por el elemento más lento -emisor, receptor o la velocidad del enlace.
- Con todos los mensajes siguiendo el mismo camino, no existen problemas de ruteo. Los direccionamientos lógicos pueden ser acomodados para permitir mensajes en broadcast a nodos elegidos.
- Se pueden agregar fácilmente terminales desconectando simplemente un conector, insertando el nuevo nodo, y volviendo a conectar de nuevo en la red. Los demás nodos son automáticamente puestos en conocimiento de la nueva dirección.
- El control es simple, y requiere solo una pequeña parte de hardware y software para implementarlo.
- El costo de la expansión de la red es proporcional al número de nodos.

Una ventaja adicional del Token Ring es que el tráfico de alta prioridad siempre va antes que el tráfico de baja prioridad. Solamente su una estación tiene tráfico igual o mayor en prioridad que el indicador colocado en el token se le permite transmitir un paquete.

2.3.2 Trama

La trama MAC para el protocolo 802.5 se muestra en la figura 2.13 y consiste de los siguientes campos:

- **Delimitador de inicio (SD):** indica el inicio de la trama. El SD consiste de patrones de señalización que se distinguen de los datos. Están codificados como sigue: JK0JK000, donde J y K son símbolos de no datos. La forma actual de un símbolo de no-datos depende de la codificación de la señal en el medio.

- **Control de acceso (AC):** tiene el formato PPPTMRRR, donde PPP y RRR son variables de 3 bits de prioridad y reservación, y M es el bit monitor; su uso lo explicaremos posteriormente. T indica tanto si es un Token o si es una trama de datos. En el caso de una trama token, el único campo restante es ED.
- **Control de trama (FC):** indica si es una trama de datos LLC. Si no, los bits en este campo controlan la operación del protocolo MAC del Token-Ring.

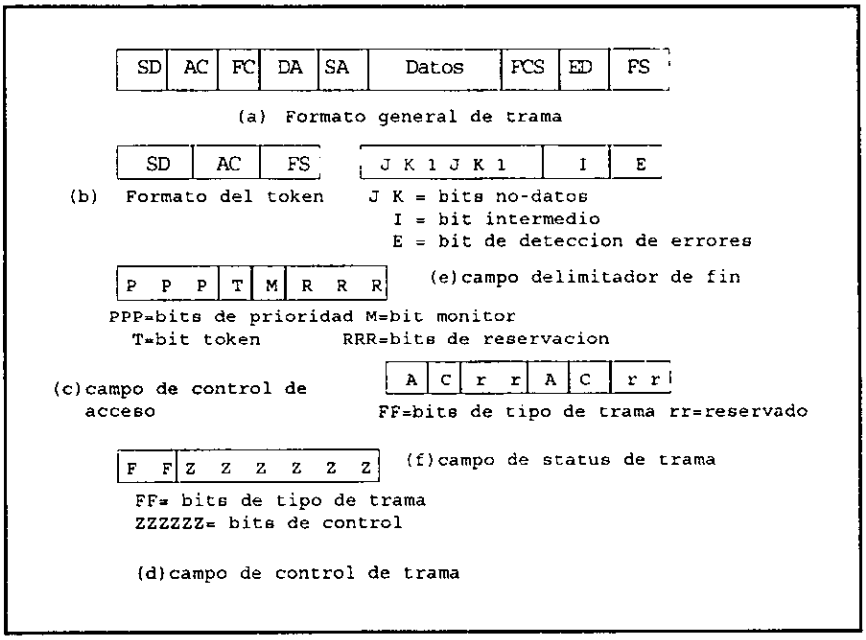


Figura 2.13 IEEE 802.5 Formato de trama

- **Dirección de destino (DA):** es igual que con 802.3
- **Dirección fuente (SA):** se usa igual que con 802.3
- **Unidad de datos:** contiene la unidad de datos LLC.
- **Trama de secuencia de chequeo (FCS):** como con 802.3.
- **Delimitador de fin (ED):** contiene el bit de detección de error (E), el cual se activa si cualquier repetidor detecta un error, y el bit intermedio (I), el cual es usado para indicar que es una trama más de una serie de varias tramas.
- **Estatus de la trama (FS):** contiene la dirección reconocida (A) y los bits copiados de trama (C), que explicaremos posteriormente. Debido a que los bits

A y C están fuera del alcance del FCS, son duplicados para proporcionar chequeo de redundancia para detectar activaciones erróneas.

Podemos ahora revisar el algoritmo Token Rin para el caso cuando se utiliza prioridad simple. En este caso, los bits de prioridad y reservación son colocados en cero. Una estación que desea transmitir espera a que un token pase por ella, con un bit token de 0 en el campo AC. La estación captura el token colocando el bit token a 1. Los campos SD y AC del token recibido ahora funcionan como los dos primeros campos de la trama de salida. La estación transmite una o más tramas, continuando hasta que termina de enviar sus tramas o hasta que el tiempo de retener el token expira. Cuando el campo AC de la ultima trama transmitida regresa, la estación coloca el bit token en 0 y añade un campo ED, resultando en la inserción de un nuevo token en el anillo.

Las estaciones en el modo de recepción escuchan el anillo, Cada estación checa las tramas que pasan tratando de descubrir un error y colocan el bit E a 1 si se detecta un error. Si una estación detecta su propia dirección MAC, coloca el bit A a 1; puede también copiar la trama, colocando el bit C a 1. Esto permite que la estación de origen diferencie tres resultados de una trama de transmisión:

- Estaciones destino no existen o no están activas (A=0, C=0).
- Estaciones destino existen pero la trama no fue copiada (A=1, C=0).
- Trama recibida (A=1, C=1).

2.3.3 Protocolo

La técnica de Token Ring esta basada en el uso de una pequeña trama llamada token, que circula cuando todas las estaciones están ociosas. Una estación que desea transmitir debe esperar hasta que detecta un token que pasa por ella. Entonces lo captura y le cambia un bit, como lo vimos anteriormente, que lo transforma de un token a una secuencia de inicio de trama para una trama de datos. La estación entonces añade y transmite los restantes campos necesarios para construir una trama.

Cuando una estación captura un token y comienza a transmitir una trama da datos, no hay token en el anillo, así que otras estaciones que deseen transmitir deben esperar. La trama circulara alrededor del anillo y de nuevo será absorbida por la estación transmisora. la estación transmisora insertará un nuevo token en el anillo cuando se cumplan las siguientes dos condiciones:

- La estación ha completado la transmisión de su trama.
- El inicio de la trama transmitida ha regresado (después de una vuelta completa en el anillo) a la estación.

Si el largo del bit del anillo es menor que el largo de la trama, la primera condición implica la segunda. Si no, una estación puede liberar un token después de que ha terminado la transmisión, pero antes de que comience a recibir su propia transmisión; la segunda condición no es estrictamente necesaria y se relaja bajo ciertas circunstancias. La ventaja de haber impuesto la segunda condición es que asegura que solo una trama de datos en cada momento puede estar en el anillo y solo una estación a la vez puede transmitir, simplificando los procedimientos de recuperación de errores.

Una vez que el nuevo token ha sido insertado en el anillo, la siguiente estación en el cable que quiera enviar datos, podrá capturar el token y transmitir.
Notese que bajo condiciones de carga ligera, hay un poco de ineficiencia con Token Ring debido a que una estación debe esperar a que el token llegue antes de poder transmitir. De cualquier modo, bajo carga pesada, que es la que importa, el anillo funciona en una forma "Round Robin", tanto eficiente como exactamente. Para observar esto considere la configuración de la figura 2.14. Después de que la estación A transmite, libera un token. La primera estación con oportunidad de transmitir es D. Si D transmite, libera entonces un token y C tiene entonces la siguiente oportunidad.

La principal ventaja del Token Ring es el control flexible que proporciona sobre el acceso. En el esquema simple descrito, el acceso es eficiente. Como veremos, se pueden utilizar esquemas para regular el acceso para proporcionar prioridad y garantizar ancho de banda. La principal desventaja del Token Ring es el requerimiento de mantener el token. La pérdida de este evita poder utilizar la red. Una duplicación del token también puede detener la operación. Una estación debe ser seleccionada como monitor para asegurar que exactamente un token este en el anillo y reinsertar uno si es necesario. El esquema de prioridad 802.5 es similar pero considerablemente más sofisticado que la descripción previa. El estándar 802.5 proporciona acceso prioritario al anillo a través del uso de los siguientes campos y registros:

- RRR Bits de reservación, permiten alta prioridad a las estaciones al solicitar el uso del siguiente token.
- PPP Bits de prioridad indican la prioridad del token, y por lo tanto cuales estaciones tienen permitido el uso del anillo.

- Rr Registro de almacenamiento para reservar un valor.
- Pr Registro de almacenamiento para el valor de prioridad.
- Sr Registro de memoria que almacena el valor de Pr
- Sx Registro de memoria que almacena el valor del token que fue transmitido
- Pm Nivel de prioridad de una trama en fila y lista para transmitir.

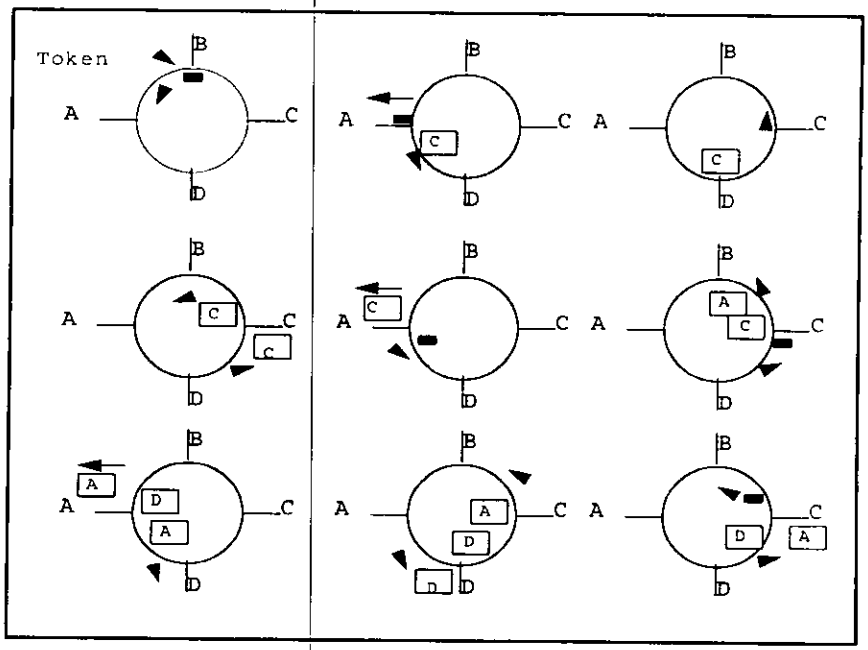


Figura 2.14 Operación Token Rin.

Los bits de prioridad (PPP) y los bits de reservación (RRR) contenidos en el token dan acceso a la trama de más alta prioridad que este lista para la transmisión en el anillo. Estos valores son almacenados en los registros Pr y Rr. El servicio de prioridad en funciones es indicado en los bits de prioridad (PPP) y el token, que esta circulando alrededor del anillo.

Los mecanismos de prioridad operan de tal manera que el mismo acceso al anillo se proporciona a todas las estaciones sin un nivel de prioridad. Esto se lleva a cabo cuando la misma estación que elevo el nivel del servicio de prioridad del anillo (estación de almacenamiento) regresa el anillo al servicio original de prioridad. Los registros Sx y Sr son usados para realizar esta función.

La operación de prioridad trabaja como sigue: cuando una estación tiene una trama de prioridad que transmitir, solicita un token de prioridad cambiando los bits de reservación (RRR) al repetir la estación el token. Si el nivel de prioridad (Pm) de la trama que esta lista para transmitirse es mayor que los bits RRR, la estación incrementa el valor del campo RRR al valor de Pm. Si el valor de los bits RRR es igual o mayor que Pm, los bits de reservación son repetidos sin cambio.

Después de que una estación ha solicitado el token, la estación transmite tramas hasta que ha completado la transmisión o hasta que la transmisión de otra trama no pudo ser completada antes de que expire el tiempo, en tal caso la estación genera un nuevo token para transmitir en el anillo.

Si la estación no tiene tramas adicionales que transmitir o si no tiene una solicitud de reservación (contenida en el registro Rr) que es más grande que el servicio de prioridad actual (contenido en el registro Pr), el token es transmitido con su prioridad presente y los bits de reservación (RRR) son más grandes que Rr o Pm, no se toma otra acción.

De cualquier modo, si la estación tiene una trama lista a transmitir o una solicitud de reservación (Rr), la cual puede ser más grande que el servicio de prioridad presente, el token es generado con la prioridad más grande de Pm o Rr y sus bits de reservación como 0. Como la estación ha hecho crecer el nivel del servicio de prioridad del anillo, la estación se vuelve una estación de almacenamiento y debe almacenar el valor anterior de servicio de prioridad como Sr y el nuevo valor como Sx. Estos valores son usados posteriormente para reducir posteriormente el valor del servicio de prioridad del anillo ciando ya no existan tramas listas para transmitir en el anillo cuya prioridad (Pm) sea igual o mayor que el almacenado en Sx.

No obstante convertirse en un almacén, la estación reclama cada token que recibe que tiene una prioridad (PPP) igual al valor más alto de prioridad almacenado (Sx). Los bits RRR del token, son examinados para elevar, mantener, o bajar el servicio de prioridad del anillo. El nuevo token es transmitido con sus bits PPP iguales al valor de los bits de reservación (RRR), pero no más bajo que el valor más alto almacenado (Sr), que es el valor original de prioridad. Este modo de operación asegura que la más alta prioridad siempre obtenga el acceso a la red.

Si el valor del nuevo servicio de prioridad (PPP igual a Rr) es más grande que Sr, los bits RRR son transmitidos como 0, el antiguo valor de prioridad contenido en Sx es reemplazado con un nuevo valor Sx igual a Rr, y la estación continua su rol como una estación de almacenamiento.

No obstante, si el valor Rr es igual o menor que el valor de prioridad más alto recibido (Sr), el nuevo token es transmitido a un valor de prioridad de Sr, tanto Sx y Sr son removidos del almacenaje, y, sin ningún otro valor de Sx y Sr son almacenados, la estación discontinua su rol como una estación de almacenaje. Esta técnica permite a las estaciones de menor valor de prioridad el uso del anillo una vez que las estaciones de alta prioridad lo hicieron.

2.3.4 Medios de Transmisión

El estándar 802.5 especifica el uso de par torcido con velocidades de transmisión entre 4 y 16 Mbps. usando codificación diferencial Manchester. Una especificación anterior de 1 Mbps. ha sido desechada en la edición mas reciente del estándar. Una adición reciente al estándar es el uso de par torcido a 4 Mbps. Tabla 2.15.

IEEE 802.5 Especificacion de medio

	Medio de Transmision	
	STP	**UTP**
Velocidad (Mbps)	4 o 16	4
Numero maximo de repetidores	250	72
Distancia maxima entre repetidores	No esp.	No esp

Tabla 2.15

2.4 FDDI

2.4.1 Topología

Cada estación lógica está compuesta de entidades lógicas conforme los estándares FDDI. El rol de una estación dada depende del número de entidades que posee. Redes con diferentes tipologías físicas pueden ser construidas, dependiendo del tipo de estaciones usadas.

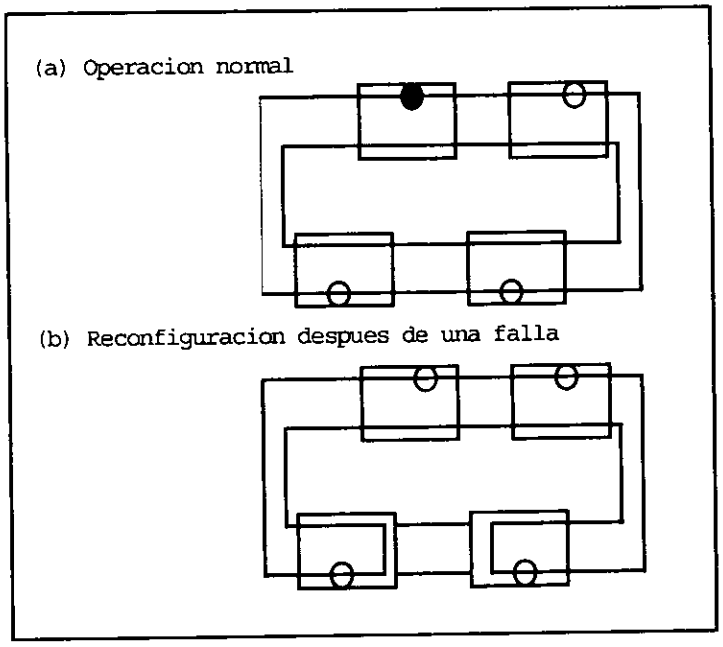


Figura 2.16 Operación del anillo dual FDDI.

Para mejorar la confiabilidad de un anillo FDDI, el estándar indica la construcción de un anillo dual, como se ilustra en la figura 2.16. Las estaciones participantes en un anillo dual están conectados a sus vecinos por dos enlaces que transmiten en direcciones opuestas. Esto crea dos anillos: un anillo primario, y un anillo secundario en el que los datos pueden circular en la dirección opuesta. Bajo condiciones normales, el anillo secundario esta ocioso. Cuando ocurre una falla en el enlace, las estaciones en ambos lados del enlace se reconfiguran como lo muestra la figura. Esto aisla la falla en el enlace y restaura el anillo. En esta figura, un punto representa una unión MAC con la estación. Así, en la dirección de

conteo, las señales pueden ser repetidas, mientras que el protocolo MAC se involucra solo en la dirección primaria. Como opción, una estación puede contener dos entidades MAC y por lo tanto ejecutar el protocolo en ambas direcciones.

Tabla 2.17 Tipos de estacion FDDI

Tipo de estacion	Definicion	Conexion para:
Dual attachment (DAS)	Tiene dis pares de entidades PHY y PMD y una o mas entidades MAC; participa en el anillo dual de linea principal	DAS, DAC
Dual attachment concentrator (DAC)	Un DAS con entidades adicionales PHY y PMD mas alla de las que se requieren para la union al anillo ; las entidades adicionales que son logicamente parte del anillo pero estan fisicamente aisladas de la linea principal del anillo	DAS, DAC, SAC SAS
Single attachment stations (SAS)	Tiene una entidad PHY, PMD y MAC, y por lo tanto no puede ser unido a la linea principal, debe ser unida por un concentrador	DAC, SAC
Single attachment concentrator (SAC)	Un SAS con entidades adicionales PHY, PMD mas alla de esos requeridos para uniones a los concentradores ; las entidades adicionales permiten la union de estaciones extra en una estructura de arbol	DAC, SAC, SAS

El tipo de estación recién descrito es solo uno de los cuatro tipos posibles definidos en el estándar FDDI (figura 2.17). El uso de cuatro tipos diferentes de estaciones permite la creación de topologías complejas y para diseños con altos niveles de desempeño.

Como se acaba de describir, la estación de enlace dual (DAS) puede ser usada para construir un anillo dual. En algunos casos este anillo dual constituirá completamente la LAN FDDI. En otros casos el anillo dual puede servir como el anillo principal para una topología más compleja. En su forma más general, la topología que puede ser realizada con FDDI es referida como un anillo dual de arboles.

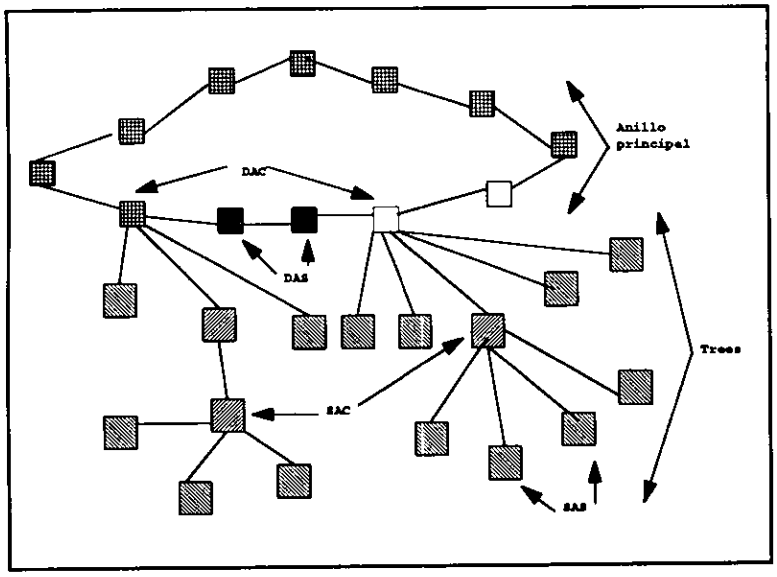


Figura 2.18 Topología general FDDI.

La figura 2.18 es un ejemplo que muestra el uso de los cuatro tipos de estación. El tronco principal en un anillo dual consistiendo solamente de estaciones que son capaces de soportar los dos anillos. Algunas de estas estaciones son DAS's, y su función es proporcionar un punto de unión para estaciones de usuario. Otras son concentradores duales de unión (DAC's), que participan en el anillo dual, y pueden soportar una estación de usuario. Además, cada DAC puede soportar estaciones que se unan a un anillo simple. Cada DAC por lo tanto sirve como la raíz de un árbol. Las estaciones simples de unión (SAS's) pueden unir a un DAC por medio de un anillo simple. La conexión SAS no proporciona una mejora a la configuración de un anillo dual disponible en el DAS. De cualquier modo, FDDI restringe la topología de forma que un SAS deba unirse aun concentrador, el concentrador puede aislar el SAS. No obstante, la mejora de un anillo dual se mantiene. Para llevar a cabo una estructura en árbol de profundidad mayor a dos, los concentradores simples de unión (SAC's) pueden ser usados. Un SAC puede unir un DAC a un SAC y puede soportar uno o más SAS's.

Es importante notar que incluso con una estructura de árbol elaborada, una configuración FDDI todavía mantiene una topología de anillo. La figura 2.19

muestra el camino de circulación para una configuración simple de un anillo dual de dos estaciones, una de las cuales es un DAC. Nótese que las seis estaciones forman una anillo único alrededor del cual un token circulará. Además, un anillo secundario esta disponible para abarcar DAS´s y DAC´s.

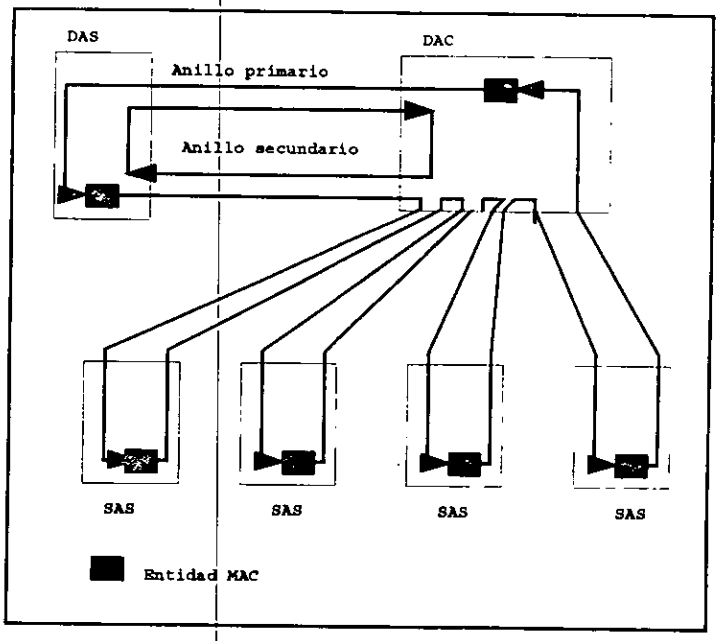


Figura 2.19 Anillo cableado como estrella

El estándar FDDI especifica reglas de conexión para asegurar que no existan topologías ilegales. Estas reglas son expresadas en términos de conexiones permitidas entre los diferentes tipos de puertos.

La definición de cuatro tipos de estaciones permite la creación de una amplia variedad de topologías. Las siguientes son de particular interés:

- **Concentrador solitario con estaciones unidas.** Este consiste de un solo concentrador y sus estaciones. Tal configuración podría ser usada para conectar múltiples dispositivos de alto desempeño en trabajo de grupo o múltiples LAN´s, con cada estación FDDI siendo un puente.
- **Anillo doble.** Este consiste de un arreglo de DAS conectados para formar un anillo dual único. Esta topología es útil cuando hay un número limitado de

usuarios. Podría también ser usada interconexión departamental de LAN's, con cada estación FDDI siendo un puente.

- **Árbol de concentradores.** Esta es una buena elección para interconectar grandes grupos de usuarios de dispositivos. Los concentradores son cableados en un arreglo de estrella jerárquica con un concentrador sirviendo como la raiz del árbol. Esta topología proporciona gran flexibilidad para agregar y remover concentradores y estaciones o cambiar su colocación sin interrumpir la LAN.

- **Anillo dual de arboles.** Esta es la topología más elaborada y flexible. Estaciones llave puede ser incorporada dentro de un anillo dual para máxima disponibilidad, y la estructura de árbol proporciona la flexibilidad descrita anteriormente.

2.4.2 Trama

La figura 2.20 describe el formato de la trama para el protocolo FDDI. El estándar define los contenidos de este formato en términos de símbolos, con cada símbolo de datos correspondiendo a un dato de 4 bits. Los símbolos son usados porque en la capa física, los datos son codificados en trozos de 4 bits. De cualquier modo, las entidades MAC, de hecho deben lidiar con bits individuales, así que la discusión que sigue algunas veces se refiere a símbolos de 4 bits y a veces a bits. Una trama diferente de un token consiste de los siguientes campos:

- **Preámbulo:** sincroniza la trama con cada reloj de estación. El originador de la trama usa un campo de 16 símbolos ociosos (64 bits); subsecuentemente las estaciones repetidoras pueden cambiar el largo del campo de acuerdo a los requerimientos del reloj. El símbolo ocioso es un patrón lleno de no-datos. La forma actual de un símbolo de no-datos dependiendo de la codificación de la señal codificada en el medio.

- **Delimitador de inicio (SD):** indica el inicio de la trama. Es codificado como JK, donde J y K son símbolos de no-datos.

- **Control de trama (FC):** tiene el formato de bit CLFFZZZZ, donde C indica si es una trama síncrona o asíncrona; L indica el uso de direcciones de 16 o 48 bits; indica si es un control LLC, MAC o trama reservada. Para un control, los cuatro bits restantes indican el tipo de trama de control.

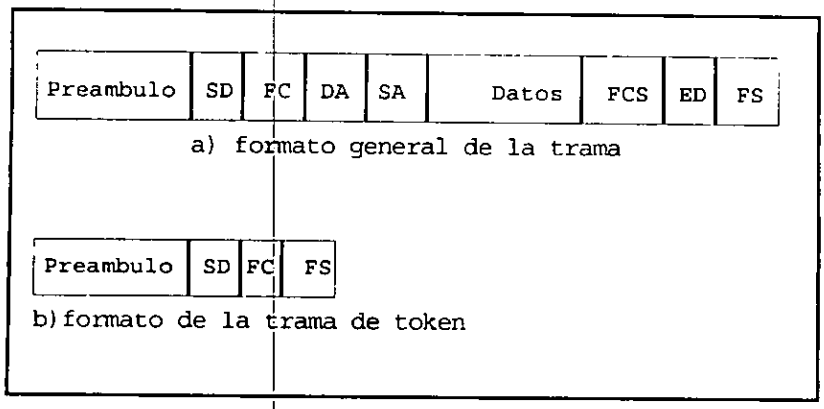


Figura 2.20 Trama FDDI.

- **Dirección destino (DA):** especifica la estación(s) para la cual la trama se encamina. Puede ser una dirección física única, una dirección multicast, o una dirección broadcast. El anillo puede contener una mezcla de longitudes de direccionamiento de 16 y 48 bits.

- **Dirección fuente (SA):** especifica la estación que envía la trama.

- **Información:** contiene unidades de datos LLC o información relacionada a la operación de control.

- **Secuencia de chequeo de trama (FCS):** un chequeo de redundancia cíclica de 32 bits, basada en los FC, DA, SA y campos de información.

- **Delimitador de fin (ED):** contiene un símbolo de no-datos (T) y marca el fin de la trama, excepto por el campo FS.

- **Estatus de la trama (FS):** contiene los indicadores de detección de error (E), reconocimiento de dirección (A), y copia de trama (F). Cada indicador es representado por un símbolo, el cual es R para "reset" o "false" y S para "set" o "true".

Una trama de token consiste de los siguientes campos:

- **Preámbulo:** como en el caso de la trama de datos.

- **Delimitador de inicio:** como en el caso de la trama de datos.
- **Control de trama (FC):** tiene el formato de bits 10000000 o 11000000 para indicar que se trata de un token.
- **Delimitador de fin (ED):** contiene un par de símbolos de no-datos (T) que terminan la trama token.

Una comparación con la trama 802.5 muestra que los dos son bastante similares. La trama FDDI incluye un preámbulo para ayudar en la sincronización, que es más demandada a altas velocidades de transmisión. Tanto las direcciones de 16 y 48 bits son permitidas en la misma red con FDDI; esta es más flexible que el esquema usado en los estándares 802. Finalmente, hay algunas diferencias en los bits de control. Por ejemplo, FDDI no incluye prioridad y reservación; la capacidad se maneja de un modo diferente.

2.4.3 Protocolo

El protocolo básico FDDI MAC es fundamentalmente el mismo que el 802.5 pero existen dos diferencias claves:

1. En FDDI, una estación esperando atrapar un token, lo puede hacer abortando la transmisión de token tan pronto como la trama de token es reconocida. Después de capturar el token este es recibido completamente, la estación no empieza a transmitir una o más tramas de datos. La técnica 802.5 de cambiar un bit para convertir un token en el inicio de una trama fue considerado impráctico debido a la alta velocidad de FDDI.
2. En FDDI, una estación que ha estado transmitiendo tramas de datos libera un nuevo token tan pronto como completa la transmisión, incluso si no ha empezado a recibir su propia transmisión. Esta es la misma técnica que comenzó a usar Token Ring. . Otra vez, debido a la alta velocidad, sería demasiado ineficiente requerir que la estación esperara a que su trama regresara.

La figura 2.21 da un ejemplo de la operación del anillo. Después de que a estación A ha atrapado el token, transmite una trama F1 e inmediatamente transmite un nuevo token. F1 es direccionado a la estación C, quién lo copia conforme circula. La trama eventualmente regresa a A, que lo absorbe. Mientras tanto, B atrapa el token liberado por A y transmite F2 seguido por un token. Esta acción podría ser repetido cualquier número de veces, así que en cualquier momento, puede haber múltiples tramas circulando en el anillo. Cada estación es

responsable de absorber sus propias tramas basadas en el campo de dirección fuente.

Podemos decir también, acerca del campo status de trama. Cada estación puede checar los bits que circulan buscando errores y puede colocar un indicador E se detecta alguno. Si una estación detecta su propia dirección, coloca el indicador A; y puede también copiar la trama, colocando el indicador C. Esto permite a la estación originante, cuando absorbió una trama que previamente transmitió, diferenciar 3 condiciones:

1. Estaciones no existentes o no activas
2. Estación activa pero no ha sido copiada la trama
3. Trama copiada

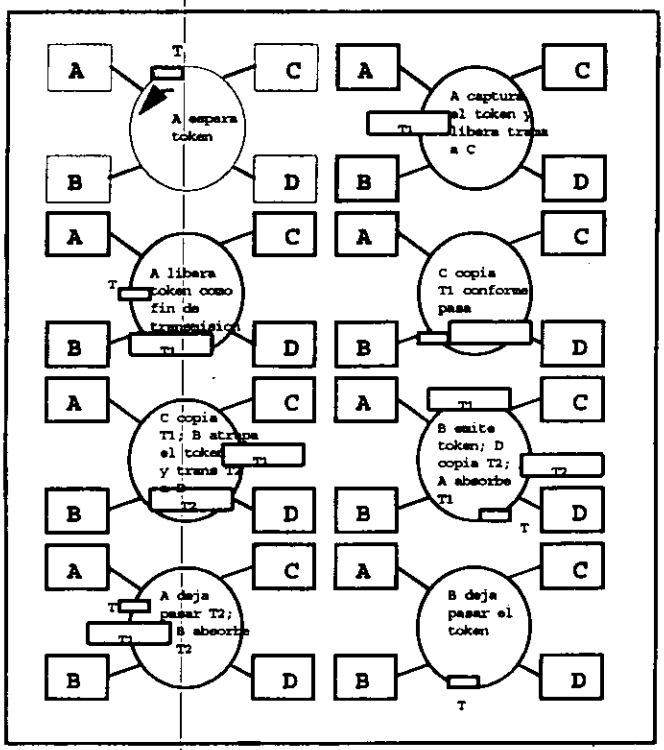


Figura 2.21 Operación del anillo FDDI.

Cuando una trama es absorbida, los indicadores de estado (E, A, C) en el campo FS pueden ser examinados para determinar el resultado de la transmisión.

De cualquier manera, si es descubierto un error o condición de falla, el protocolo MAC no trata de retransmitir la trama pero reporta la condición a LLC. Es responsabilidad de LLC o algunos protocolos de capa superior tomar la acción correctiva.

Como con IEEE 802.5 FDDI proporciona un esquema de capacidad de capacidad de distribución.

El esquema de prioridad usado en 802.5 no funciona en FDDI, debido a que una estación usualmente captura el token antes de que su propia trama regrese. Por lo que el uso de un campo de reservación no es efectivo. Además el estándar FDDI trata de proporcionar gran control sobre la capacidad de la red, más que 802.5, para lograr los requerimientos de una LAN de alta velocidad. Específicamente, el esquema de capacidad de distribución busca acomodar los siguientes requerimientos:

- Soporte para una mezcla de tráfico en ráfaga o continuo.
- Soporte para dialogo multitramas.

Con respecto al primer requerimiento, una LAN de alta capacidad se espera que pueda soportar un gran número de dispositivos o actuar como backbone para cierto número de LAN´s. En ambos casos, la LAN esperaríamos que soportara una amplia variedad de tipos de tráfico. Por ejemplo, algunas de las estaciones pueden generar tráfico en ráfagas cortas con requerimientos modestos pero la necesidad de un pequeño tiempo de retraso. Otras estaciones pueden generar largas ráfagas de tráfico que requieren gran ancho de banda, pero pueden tolerar retrasos previos al inicio de la transmisión

Con respecto al segundo requerimiento, puede ser necesario algunas veces dedicar una fracción permanente o toda la capacidad de la LAN a una aplicación única. Esto permite una larga secuencia de tramas de datos y reconocimientos a intercambiar. Un ejemplo de la utilidad de esta característica es leer o escribir en un disco de alto desempeño. Sin la habilidad de mantener un flujo constante de alta velocidad sobre la LAN, solamente un sector del disco podrá ser accesado por revolución, un desempeño inaceptable.

Para acomodar los requerimientos que soportan una mezcla de tráfico en ráfaga y continuo, FDDI define dos tipos de tráfico; síncrono y asíncrono. Cada estación se distribuye en una porción de la capacidad total (la porción puede ser cero); las tramas que se transmiten durante este tiempo se refieren como tramas

síncronas. Cualquier capacidad que no se distribuye o que no se usa esta disponible para la transmisión de tramas adicionales, referidas como tramas asíncronas.

2.4.4 Medios de transmisión

Como su nombre los sugiere la especificación original FDDI define un anillo LAN usando un medio de fibra óptica. El estándar incluye un esquema de codificación y una especificación de medio físico.

Codificación de datos. Como en el caso de la especificación IEEE 802.4 de fibra óptica, el esquema de codificación FDDI esta basado en el uso de una intensa modulación. En el caso de 802.4, los datos a transmitir son precodificados en forma Manchester antes de ser sometidos a un proceso de intensa modulación, tratando de llevar a cabo transiciones para sincronización. La desventaja de esto es que la eficiencia es de solo 50%. Esto es debido a que puede haber hasta dos transiciones por bit, seria necesaria una velocidad de señalización de 200 millones de elementos de señal por segundo (200Mbaud) para alcanzar 100 Mbps. A la alta velocidad de FDDI, esto representa un costo innecesario y carga técnica.

Para lograr una eficiencia mas grande, el estándar FDDI especifica el uso del código 4B/5B. En este esquema, se codifican 4 bits cada vez; cada 4 bits de datos son codificados en símbolos con 5 celdas, tal que cada celda contenga un elemento único de señal (presencia o ausencia de luz). En efecto cada arreglo de 4 bits es codificado como 5 bits. La eficiencia que se logra es casi el 80%: 100 Mbps. se logran con 125 Mbaud. Tal como en 100BASE-T, cada celda de 4B/5B es tratada como un valor binario y codificada usando código no retorno a cero invertido.

Debido a que codificamos 4 bits con un patrón de cinco, solamente 16 de 32 patrones son necesarios para la codificación de datos. Los códigos seleccionados para representar los 16 bloques de 4 bits tal que se encuentre presente una transición al menos dos veces para código de 5 celdas. Dándole un formato de NRZI, no se permiten mas de tres ceros por fila.

La codificación FDDI puede ser resumida como sigue:

1. Una codificación de modulación por intensidad simple se rechaza debido a que no proporciona sincronización; una cadena de unos y ceros no tendrán transiciones.
2. Los datos a transmitir primero deben ser codificados para asegurar transiciones. El código 4B/5B es preferido al Manchester porque es más eficiente.
3. El código 4B/5B es más codificable usando NRZI así que la señal diferencial resultante mejorara la recepción.
4. Los patrones específicos escogidos para la codificación de los 16 patrones de datos son escogidos para garantizar no más de tres ceros en una fila para proporcionar sincronización adecuada.

Solamente 16 de los 32 patrones posibles se requieren para representar la entrada de datos. Los patrones restantes de celdas son declarados también inválidos o asignados a un significado como símbolos de control. El estándar FI especifica un anillo de fibra óptica con una velocidad de 100Mbps, usando un esquema de codificación NRZI descrito anteriormente. La longitud de onda especificada para la transmisión de datos es 1300nm.

La especificación original especifica el uso de transmisión de fibra multimodo. No obstante que las redes de larga distancia cuentan primariamente con una fibra de monomodo, esa tecnología usualmente requiere el uso de lasers como fuentes de luz mas, que de los diodos de emisión de luz más baratos y menos poderosos (LED´s), que son adecuados para los requerimientos de FDDI. Las dimensiones del cable de fibra óptica son especificadas en términos del diámetro del corazón de la fibra y el diámetro externo de la capa que rodea el corazón. La combinación especificada en el estándar es 62.5/125 μm. El estándar lista como alternativas 50/125, 82/125, y 100/140 μm. En general diámetros mas péquenos ofrecen mas potencial en ancho de banda pero también perdidas mas altas en los conectores.

Mas recientemente, dos especificaciones de medio han sido agregadas. La especificación de fibra monomodo puede ser usada para configurar enlaces más grandes entre repetidores. La especificación de fibra de bajo costo proporcionan conexiones de fibra óptica de bajo costo para largos superiores a 500m. Los principales ahorros son realizados al relajar algunas especificaciones para los transceptores ópticos.

El estándar FDDI también especifica un anillo de par torcido con una velocidad de 100Mbps. El esquema de señalización que se usa es el MLT-3. En este esquema la señal 4B/5B NRZI se convierte de nuevo a NRZ, codificado con

un encriptador de cadenas que distribuye la energía para lograr una reducción en las emisiones radiadas, y entonces codificar usando MLT-3.

Se especifican dos medios tipos de par torcido: par torcido de 100 ohms categoría 5 sin protección. En ambos casos la distancia máxima entre repetidores es 100 metros. La especificación de par torcido proporciona una alternativa de bajo costo que puede ser usada sobre distancias cortas empleando cableado previamente preinstalado. La figura nos proporciona alternativas para FDDI.

Alternativas de medio de fibra óptica para FDDI

	Fibra multimodo	Fibra monomodo
Fuente luminosa	LED	Laser
Longitud de onda	1300nm	1300nm
Máxima distancia entre	2km	40-
Tamaño del cable	62.5/125 m	8-10/125 m

Tabla 2.22 Tipos de fibra óptica.

2.5 Interfaces en LAN

Las interfaces son los elementos que nos permiten la conexión entre los diferentes dispositivos que forman las redes LAN y las conexiones entre LAN´s y WAN´s; a continuación nos referiremos a los mas importantes.

- **AUI**

Existen ocasiones, en que, la unidad de trabajo se encuentra lejos de su conexión a la red, es decir, la MAU esta lejos de la estación de trabajo, la interface que nos permite conectar estos elementos es la AUI (Attachment Unit Interface).A continuación se muestra la AUI fisicamente

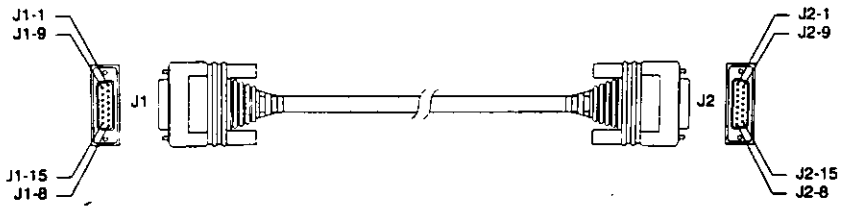


Figura 2.23 Conector AUI

Pines del conector AUI

Pin	Circuito Ethernet	Señal
3	DO-A	Circuito A Tx
10	DO-B	Circuito B Tx
11	DO-S	Circuito blindado Tx
5	DI-A	Circuito A Rx
12	DI-B	Circuito B Rx
4	DI-S	Circuito blindado Rx
2	CI-A	Control en circuito A
9	CI-B	Control en circuito B
1	CI-S	Control en el circuito blindado
6	VC	Voltaje comun
13	VP	Voltaje de alimentación
14	VS	Voltaje blindaje (L25 y M25)
Shell	PG	Tierra

Tabla 2.24 Pines del conector AUI.

- **RJ-45**

El cable UTP utiliza conectores pequeños de plástico designados como RJ-45. Son similares a los conectores telefónicos excepto que en vez de cuatro cables, la

red RJ-45 contiene 8 contactos. Para el uso de estos conectores existen además tres tipos de adaptadores:

- Adaptador DTE hembra RJ-45 a DB-9
- Adaptador DTE hembra RJ-45 a DB-25
- Adaptador DCE macho RJ-45 a DB-25 (modem).

Puerto DTE	RJ-45 a RJ-45	RJ-45 a DB-9		Consola
Señal	Pin RJ-45	Pin RJ-45	Pin DB-9	Señal
RTS	1	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	$	5	GND
RxD	6	3	3	TxD
DSR	7	3	4	DTR
CTS	8	1	7	RTS

Tabla 2.24 Señalización y cableado usando un adaptador DB-9.

Puerto DTE	RJ-45 a RJ-45	RJ-45 a DB-25 Terminal		Consola
Señal	**Pin RJ-45**	**Pin RJ-45**	**Pin DB-25**	**Señal**
RTS	1	8	5	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	7	GND
GND	5	4	7	GND
RxD	6	3	2	TxD
DSR	7	3	20	DTR
CTS	8	1	4	RTS

Tabla 2.25 Señalización y cableado usando un adaptador DB-25.

Puerto DTE	RJ-45 a RJ-45	RJ-45 a DB-25 Adaptador de modem		Consola
Señal	**Pin RJ-45**	**Pin RJ-45**	**Pin DB-25**	**Señal**
RTS	1	8	4	RTS
DTR	2	7	20	DTR
TxD	3	6	3	TxD
GND	4	5	7	GND
GND	5	4	7	GND
RxD	6	3	2	RxD
DSR	7	3	8	DCD
CTS	8	1	5	CTS

Tabla 2.26 Señalizaciçon y cableado usando un adaptador DB-25.

- **EIA-530**

El conector EIA-530 fue introducido en 1987. E intentaba operar a velocidades de 20 kbps. hasta 2 Mbps usando un conector de 25 pines a continuación mostramos su forma física y la tabla donde se indica cada pin.

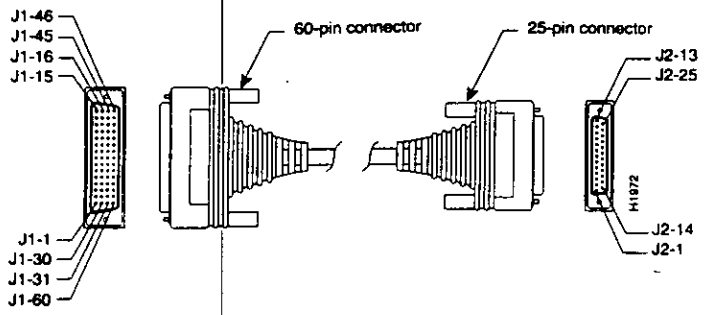


Figura 2.27 Conector EIA-530.

- **RS-232**

Los DTE´s y los DCE´s están conectados usualmente por la interfaz estándar RS-232C. La C representa la cuarta versión, que fue aprobada en 1981 (Tx asíncrona y síncrona con velocidades debajo de los 20Kbps). El CCITT tiene estándares similares llamados V.24/V.28. A continuación se muestra el uso de cada pin:

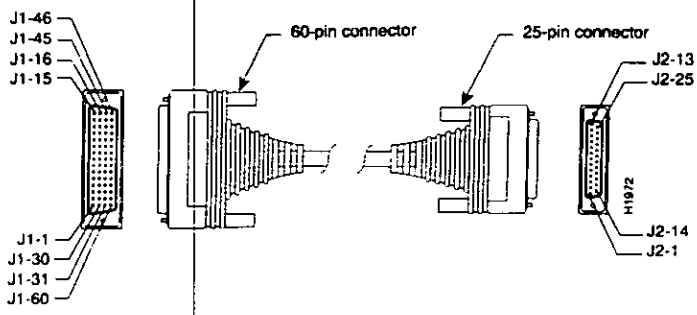


Figura 2.28 Conector RS-232C.

60 Pines	Senal	25 Pines	Señal	Dirección DTE DCE
J1-11	TxD/RxD+	J2-2	BA(A), TxD+	→
J1-12	TxD/RxD-	J2-14	BA(B), TxD-	→
J1-28	RxD/TxD+	J2-3	BB(A), RxD+	←
J1-27	RxD/TxD-	J2-16	BB(B), RxD-	←
J1-9	RTS/CTS+	J2-4	CA(A), RTS+	→
J1-10	RTS/CTS-	J2-19	CA(B), RTS-	→
J1-1	CTS/RTS+	J2-5	CB(A), CTS+	←
J1-2	CTS/RTS-	J2-13	CB(B), CTS-	←
J1-3	DSR/DTR+	J2-6	CC(A), DSR+	←
J1-4	DSR/DTR-	J2-22	CC(B), DSR-	←
J1-46	Blindado GND	J2-1	Blindado	cortado
J1-47	Modo 2	-	-	
J1-48	GND	-	-	cortado
J1-49	Modo 1	-	-	
J1-5	DCD/DCD+	J2-8	CF(A), DCD+	←
J1-6	DCD/DCD-	J2-10	CF(B), DCD-	←
J1-24	TxC/RxC+	J2-15	DB(A), TxC+	←
J1-23	TxC/RxC-	J2-12	DB(B), TxC-	←
J1-26	RxC/TxCE+	J2-17	DD(A), RxC+	←
J1-25	RxC/TxCE-	J2-9	DD(B), RxC-	←
J1-44	LL/DCD	J2-18	LL	→
J1-45	Circuit GND	J2-7	Circuit GND	
J1-7	DTR/DSR+	J2-20	CD(A), DTR+	→
J1-8	DTR/DSR-	J2-23	CD(B), DTR-	→
J1-13	TxCE/TxC+	J2-24	DA(A),	→
J1-14	TxCE/TxC-	J2-11	TxCE+	→

Tabla 2.29 Conector EIA-530 DTE (DB-60 a DB-25). Las flechas indican la dirección de la señal: → indica DTE hacia DCE, y ← indica DCE hacia DTE.

60 pin	Señal	Descripción	Dirección	25 pin	Señal
J1-50	MODE 0	cortado	–	–	–
J1-51	GND				
J1-52	MODE DCE				
J1-46	GND	único	–	J2-1	GND
J1-41	TxD/RxD	par 5	▶	J2-2	TxD
aislado	-----		–	aislado	–
J1-36	RxD/TxD	par 9	◀	J2-3	RxD
aislado	----		--	aislado	–
J1-42	RTS/CTS	par 4	▶	J2-4	RTS
aislado	----		–	aislado	–
J1-35	CTS/RTS	par 10	◀	J2-5	CTS
aislado	—		--	aislado	–
J1-34	DSR/DTR	par 11	◀	J2-6	DSR
aislado	—		--	aislado	--
J1-45	GND	par 1		J2-7	GND
aislado	–		–	aislado	–
J1-33	DCD/LL	par 12	◀	J2-8	DCD
aislado	–		–	aislado	–
J1-37	TxC/NIL	par 8	◀	J2-15	TxC
aislado	–		–	aislado	–
J1-38	RxC/TxCE	par 7	◀	J2-17	RxC
aislado	–		–	aislado	–
J1-44	LL/DCD	par 2	▶	J2-18	LTST
aislado	–		–	aislado	–
J1-43	DTR/DSR	par 3	▶	J2-20	DTR
aislado	–		--		–
J1-39	TxCE/TxC	par 6	▶	J2-24	TxCE
aislado	–		–	aislado	–

Tabla 2.30(a) Interface EIA 232, cable DTE (DB-60 a DB-25)

60 pin	Señal	Descripción	Dirección	25 pin	Señal
J1-50	MODE 0	cortado	–	–	–
J1-51	GND				
J1-46	GND	único	–	J2-1	GND
J1-41	TxD/RxD	par 5	►	J2-3	RxD
aislado	-----		–	aislado	–
J1-36	RxD/TxD	par 9	◄	J2-2	TxD
aislado	-----		–	aislado	–
J1-42	RTS/CTS	par 4	►	J2-5	CTS
aislado	----		–	aislado	–
J1-35	CTS/RTS	par 10	◄	J2-4	RTS
aislado	---		–	aislado	–
J1-34	DSR/DTR	par 11	◄	J2-20	DTR
aislado	—		–	aislado	–
J1-45	GND	par 1		J2-7	GND
aislado	–		–	aislado	–
J1-33	DCD/LL	par 12	◄	J2-18	LTST
aislado	–		–	aislado	–
J1-38	RxC/TxCE	par 8	◄	J2-24	TxCE
aislado	–		–	aislado	–
J1-44	LL/DCD	par 2	►	J2-18	LTST
aislado	–		–	aislado	–
J1-43	DTR/DSR	par 3	►	J2-6	DSR
aislado	–		–		–
J1-39	TxCE/TxC	par 7	►	J2-15	TxC
aislado	–		–	aislado	–

Tabla 2.30(b) Interface EIA-232, cable DCE (DB-60 a DB-25). Las flechas indican el sentido del flujo.

♦ **EIA-449**

Otra interface que podemos mencionar es la EIA-449, (velocidad de 2Mbps).

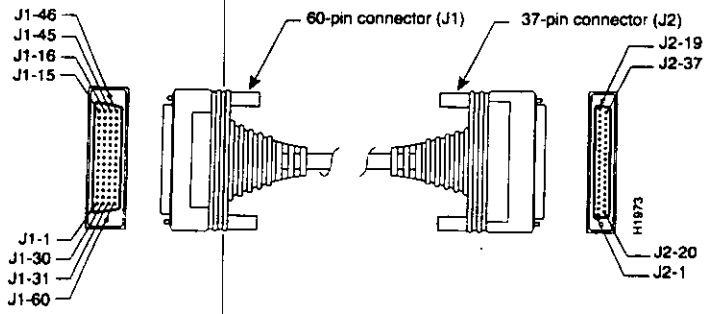


Figura 2.31 Conector EIA 449.

♦ **V.35**

La interfaz V.35 tiene su principal aplicación en la conexión de modems, puede manejar velocidades de 48, 56 y 64kbps, es síncrona y puede utilizar modulación ASK-FSK.

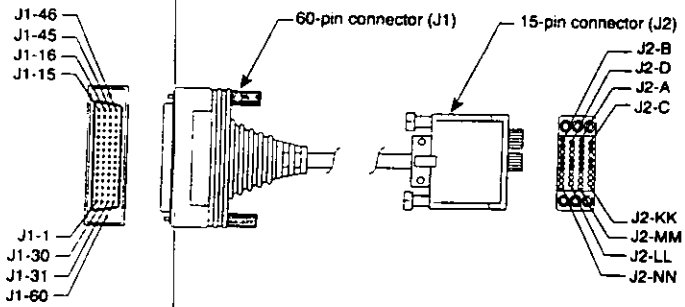


Figura 2.32 Interface (conector) V.35

60 pin	Señal	Descripción	Dirección	37 pin	Señal
J1-49	MODE 0	cortado	--	--	--
J1-48	GND				
J1-51	GND	cortado	--		
J1-52	MODE DCE				
J1-46	tierra	único		J2-1	GND
J1-11	TxD/RxD+	par 6	▶	J2-4	SD+
J1-12	TxD/RxD-		▶	J2-22	SD-
J1-24	TxC/RxC+	par 9	◀	J2-5	ST+
J1-23	TxC/RxC		◀	J2-23	ST-
J1-28	RxD/TxD+	par 11	◀	J2-6	RD+
J1-27	RxD/TxD-		◀	J2-24	RD-
J1-9	RTS/CTS+	par 5	▶	J2-7	RS+
J1-10	RTS/CTS-		▶	J2-25	RS-
J1-26	RxC/TxCE	par 10	◀	J2-8	RT+
J1-25	RxC/TxCE		◀	J2-26	RT-
J1-1	CTS/RTS+	par 1	◀	J2-9	CS+
J1-2	CTS/RTS		◀	J2-27	CS-
J1-44	LL/DCD	par 12	▶	J2-10	LL
J1-45	Circuito GND			J2-37	SC
J1-3	DSR/DTR+	par 2	◀	J2-11	DM+
J1-4	DSR/DTR-		◀	J2-29	DM-
J1-7	DTR/DSR+	par 4	▶	J2-12	TR+
J1-8	DTR/DSR-		▶	J2-30	TR-
J1-5	DCD/DCD+	par 3	◀	J2-13	RR+
J1-6	DCD/DCD-		◀	J2-31	RR-
J1-13	TxCE/TxC+	par 7	▶	J2-17	TT+
J1-14	TcCE/TxC-		▶	J2-35	TT-
J1-15	Circuit GND	par 9		J2-19	SG
J1-16	Circuit GND			J2-20	RC

Tabla 2.33(a) EIA 449, cable DTE (DB-60 a DB-25).

60 pin	Señal	Descripción	Dirección	37 pin	Señal
J1-49	MODE 1	cortado	--	--	--
J1-48	GND				
J1-46	tierra	único		J2-1	GND
J1-28	RxD/TxD+	par 11		J2-4	SD+
J1-27	RxD/TxD-			J2-22	SD-
J1-13	TxCE/TxC+	par 7	▼	J2-5	ST+
J1-14	TxCE/TxC		▼	J2-23	ST-
J1-11	TxD/RxD+	par 6	◀	J2-6	RD+
J1-12	TxD/RxD-		◀	J2-24	RD-
J1-1	CTS/RTS+	par 1	◀	J2-7	RS+
J1-2	CTS/RTS-		◀	J2-25	RS-
J1-24	TxC/RxC	par 9	▼	J2-8	RT+
J1-23	TxC/RxC		▼	J2-26	RT-
J1-9	RTS/CTS+	par 5	◀	J2-9	CS+
J1-10	RTS/CTS		◀	J2-27	CS-
J1-29	NIL/LL	par 12	◀	J2-10	LL
J1-30	Circuito GND		◀	J2-37	SC
J1-7	DTR/DSR+	par 4	▼	J2-11	DM+
J1-8	DTR/DSR-			J2-29	DM-
J1-3	DSR/DTR+	par 2	◀	J2-12	TR+
J1-4	DSR/DTR-		◀	J2-30	TR-
J1-5	DCD/DCD+	par 3	▼	J2-13	RR+
J1-6	DCD/DCD-		▼	J2-31	RR-
J1-26	RxC/TxCE+	par 10	◀	J2-17	TT+
J1-25	RxC/TxCE-		◀	J2-35	TT-
J1-15	Circuit GND	par 8	▼	J2-19	SG
J1-16	Circuit GND		▼	J2-20	RC

Tabla 2.33(b) Interface EIA-449, cable DCE (DB-60 a DB-37).

60 pin	Señal	Descripción	Dirección	34 pin	Señal
J1-49	Mode 1	cortado	--	--	--
J1-48	GND				
J1-50	Mode 0	cortado	--	--	--
J1-51	GND				
J1-52	Mode DCE				
J1-53	TxC/NIL	cortado			
J1-54	RxC_TxCE				
J1-55	RxD/TxD				
J1-56	GND				
J1-46	GND	unico	--	J2-A	GND
J1-45	Circuito GND	par 12	--	J-B	GND
aislado				aislado	
J1-42	RTS/CTS	par 9 →		J2-C	RTS
aislado				aislado	
J1-35	CTS/RTS	par 8 ←		J2-D	CTS
aislado				aislado	
J1-34	DSR/DTR	par 7 ←		J2-E	DSR
aislado				aislado	
J1-33	DCD/LL	par 6 ←		J2-F	RLSD
aislado				aislado	
J1-43	DTR/DSR	par 10 →		J2-H	DTR
aislado				aislado	
J1-44	LL/DCD	par 11 →		J2-K	LT
aislado				aislado	
J1-18	TxD/RxD+	par 1 →		J2-P	SD+
J1-17	TxD/RxD-	→		J2-S	SD-
J1-28	RxD/TxD+	par 5 ←		J2-R	RD+
J1-27	RxD/TxD-	←		J2-T	RD-
J1-20	TxCE/TxC+	par 2 →		J2-U	SCTE+
J1-19	TxCE/TxC-	→		J2-W	SCTE-
J1-26	RxC/TxCE+	par 4 ←		J2-V	SCR+
J1-25	RxC/TxCE-	←		J2-X	SCR-
J1-24	TxC/RxC+	par 3 ←		J2-Y	SCT+
J1-23	TxC/RxC-	←		J2-AA	SCT-

Tabla 2.34(a) Interface V.35, cable DTE (DB-60 a DB-34).

60 pin	Señal	Descripción	Dirección	34 pin	Señal
J1-49	Mode 1	cortado	--	--	--
J1-48	GND				
J1-50	Mode 0	cortado	--	--	--
J1-51	GND				
J1-53	TxC/NIL	cortado			
J1-54	RxC_TxCE				
J1-55	RxD/TxD				
J1-56	GND				
J1-46	GND	único	--	J2-A	GND
J1-45	Circuito GND aislado	par 12	--	J-B aislado	GND
J1-42	RTS/CTS aislado	par 9	→	J2-C aislado	CTS
J1-35	CTS/RTS aislado	par 8	←	J2-C aislado	RTS
J1-34	DSR/DTR aislado	par 7	←	J2-H aislado	DTR
J1-33	DCD/LL aislado	par 6	←	J2-K aislado	LT
J1-43	DTR/DSR aislado	par 10	→	J2-E aislado	DSR
J1-44	LL/DCD aislado	par 11	→	J2-F aislado	RLSD
J1-18	TxD/RxD+	par 1	→	J2-R	RD+
J1-17	TxD/RxD-		→	J2-T	RD-
J1-28	RxD/TxD+	par 5	←	J2-R	RD+
J1-27	RxD/TxD-		←	J2-T	RD-
J1-20	TxCE/TxC+	par 2	→	J2-U	SCR+
J1-19	TxCE/TxC-		→	J2-W	SCR-
J1-26	RxC/TxCE+	par 4	←	J2-U	SCTE+
J1-25	RxC/TxCE-		←	J2-W	SCTE-
J1-24	TxC/RxC+	par 3	←	J2-Y	SCT+
J1-23	TxC/RxC-		←	J2-AA	SCT-

Tabla 2.34(b) Interface V.35, cable DCE (DB-60 a DB-34).

♦ **X.21**

X.21 es otra interface estándar que ha sido objeto de una considerable atención en el sector, aunque no esta tan extendido como es RS-232-C. Este estándar fue publicado por primera vez en 1972. A diferencia de 232 X.21 emplea un conector de 15 contactos. Los circuitos están definidos en el documento 4903 del ISO (X.21 incluye la misma distribución de pines que RS-449).

60 pin	Señal	Descripción	Dirección	15 pin	Señal
Ji-48	GND	cortado	--	--	--
J1-47	Mode_2				
J1-51	GND	cortado	--	--	--
J1-52	Mode DCE				
J1-46	GND	único	--	J2-1	GND
J1-11	TxD/RxD	par 3	→	J2-2	Tx+
J1-12	TxD/RxD		→	J2-9	Tx-
J1-9	RTS/CTS+	par 2	→	J2-3	C+
J1-10	RTS/CTS-		→	J2-10	C-
J1-28	RxD/TxD+	par 6	←	J2-4	Rx+
J1-27	RxD/TxD-		←	J2-11	Rx-
J1-1	CTS/RTS+	par 1	←	J2-5	Ind+
J1-2	CTS/RTS-		←	J2-12	Ind-
J1-26	RxC/TxCE+	par 5	←	J2-6	T+
J1-25	RxC/TxCE-		←	J2-13	T-
J1-15 aislado	Control_GND	par 4		J2-8 aislado	Cont

Tabla 2.35(a) Interface X.21, cable DTE (DB-60 a DB-15).

60 pin	Señal	Descripción	Dirección	15 pin	Señal
Ji-48	GND	cortado	--	--	--
J1-47	Mode_2				
J1-51	GND	cortado	--	--	--
J1-46	GND	único	--	J2-1	GND
J1-11	TxD/RxD	par 3	→	J2-4	Rx+
J1-12	TxD/RxD		→	J2-11	Rx-
J1-9	RTS/CTS+	par 2	→	J2-5	ind+
J1-10	RTS/CTS-		→	J2-12	ind-
J1-28	RxD/TxD+	par 6	←	J2-2	Tx+
J1-27	RxD/TxD-		←	J2-9	Tx-
J1-1	CTS/RTS+	par 1	←	J2-3	C+
J1-2	CTS/RTS-		←	J2-10	C-
J1-24	TxC/RxC+	par 4	→	J2-6	T+
J1-25	TxC/RxC-		→	J2-13	T-
J1-15 aislado	Control_GND	par 5		J2-8 aislado	Cont

Tabla 2.35(b) Interface X.21, cable DCE (DB-60 a DB-15).

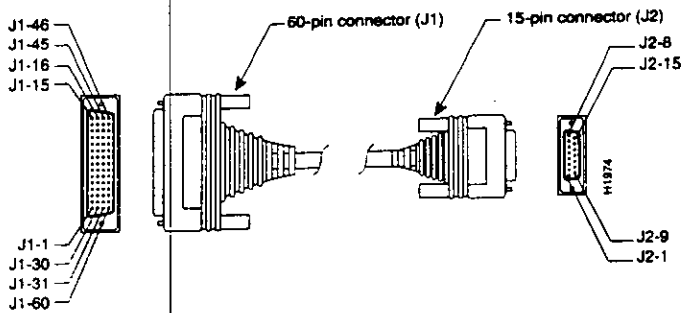


Figura 2.36 Conector para la interface X.21.

CAPITULO 3

TCP/IP

3.1 Introducción

Hasta ahora hemos visto los detalles de bajo nivel de transmisión a través de redes individuales, fundamento sobre el cual se lleva a cabo toda la comunicación por computadora.

La alternativa para proporcionar la interconexión con programas de nivel de aplicación es un sistema basado en la interconexión a nivel de red. Una interconexión a nivel de red proporciona un mecanismo que entrega los paquetes, desde su fuente original hasta su destino final. Conmutar pequeñas unidades de datos en vez de archivos o grandes mensajes tiene muchas ventajas. Primero, el esquema se proyecta directamente hacia el hardware subyacente de red, haciéndolo extremadamente eficiente. Segundo, la interconexión a nivel de red separa de los programas de aplicación las actividades de comunicación de datos, permitiendo que computadoras intermedias manejen el tráfico de red sin "entender" las aplicaciones que lo utilizan. Tercero, utilizar conexiones de red mantiene flexible a todo el sistema, haciendo posible la construcción de instalaciones de comunicación con propósitos generales. Cuarto, el esquema permite que los administradores de red agreguen nuevas tecnologías de red al modificar o agregar una pieza sencilla de software nuevo a nivel de red, mientras los programas de aplicación permanecen sin cambios.

La clave para diseñar una interconexión universal a nivel de red se encuentran en un concepto abstracto sobre sistemas de comunicación conocido como enlace de redes (internetworking). El concepto de red de redes o internet es muy poderoso. Elimina la noción sobre comunicaciones de los detalles de las tecnologías de red y oculta los detalles de bajo nivel al usuario. De manera más importante, controla todas las decisiones sobre diseño de software y explica como manejar las direcciones físicas y las rutas. Después de revisar la motivación básica para el enlace de redes, consideraremos con mayor detalle las propiedades de una red de redes.

Comenzaremos con dos observaciones fundamentales sobre el diseño de sistemas de comunicación:

- Ningún hardware de red por si mismo puede satisfacer todos los requerimientos.
- Los usuarios buscan la interconexión universal.

La primera observación es técnica. Las redes de área local, que proporcionan la mayor velocidad de comunicación, están limitadas en cuanto a su alcance geográfico; las redes de área amplia abarcan grandes distancias pero no pueden proporcionar conexiones de alta velocidad. Ninguna tecnología de red por si misma satisface todas las necesidades, así que nos vemos forzados a considerar muchas tecnologías subyacentes de hardware.

¿Cómo se interconectan las redes para formar una red de redes?. La respuesta tiene dos partes. Físicamente, dos redes sólo se pueden conectar por medio de una computadora en medio de las dos. Sin embargo, una conexión física no proporciona la interconexión que tenemos en mente, debido a que dicha conexión no garantiza que la computadora cooperara con otras máquinas que estén dispuestas a intercambiar paquetes de una red a otra. Las computadoras que interconectan dos redes y transfieren paquetes de una a otra se conocen como ruteadores de red de redes. Cuando la conexión de red de redes se vuelve más compleja, los ruteadores necesitan conocer la topología de la red de redes mas allá de las redes que interconectan. Por ejemplo en la figura 3.1 se muestran tres redes interconectadas por medio de dos ruteadores.

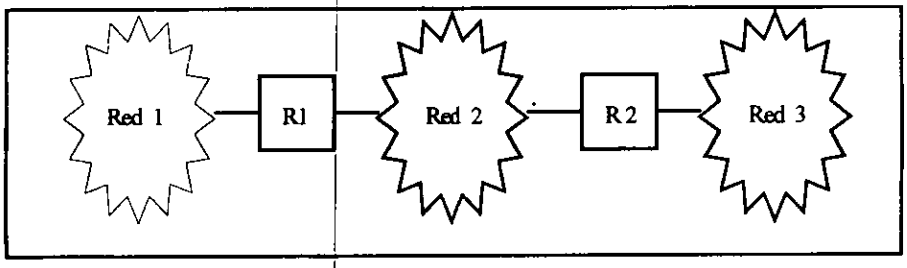


Figura3.1 Redes interconectadas por ruteadores.

En este ejemplo, el ruteador R1 debe transferir, de la red 1 a la red 2, todos los paquetes destinados a las máquinas (PC's, Hosts, Workstations, etc) de la red 2 o

de la red 3. Para una gran red de redes, la tarea de los ruteadores de tomar decisiones sobre donde enviar paquetes se vuelve más compleja.

La idea de un rutedor parece sencilla, pero es importante debido a que proporciona una forma de interconectar, no sólo. De hecho, ya hemos descubierto el principio de interconexión utilizado a través de una red de redes: en una red de redes TCP/IP, los ruteadores proporcionan todas las interconexiones entre las redes físicas.

Se puede pensar que los ruteadores, que deben saber como rutear paquetes hacia su destino, son grandes máquinas con suficiente memoria primaria o secundaria para guardar información sobre cada máquina dentro de la red de redes a la que se conectan. Sin embargo, los ruteadores utilizados en las redes de redes TCP/IP son por lo general computadoras pequeñas. A menudo tienen muy poco o nada de almacenamiento en disco y memorias principales limitadas. El truco para construir un rutedor pequeño para red de redes reside en que los ruteadores utilizan la red de destino, no el anfitrión, cuando rutean un paquete.

Si el ruteo esta basado en redes, la cantidad de información que necesita guardar un ruteador es proporcional al número de redes dentro de otra red, no en el número de computadoras.

Recuerde que el TCP/IP esta diseñado para proporcionar interconexión universal entre máquinas, independientemente de las redes en particular a las que están conectadas. Por lo tanto, queremos que un usuario vea una red de redes como una sola red virtual a la cual todas las máquinas se conectan sin importar sus conexiones físicas. En la figura 3.2 se muestra como pensar en una red de redes, en vez de pensar en redes constitutivas, simplifica los detalles y ayuda al usuario a conceptualizar la comunicación. Además de los ruteadores que interconectan redes físicas, se necesita software en cada anfitrión para permitir que los programas de aplicación utilizan la red de redes como si esta fuera una sola red física real.

La ventaja de proporcionar una interconexión a nivel de red ahora se vuelve clara. Debido a que los programas de aplicación que se comunican a través de la red de redes no conocen los detalles de las conexiones subyacentes, se pueden correr sin cambios en cualquier máquina. Como los detalles de la conexión física entre cada máquina y a la red física están ocultos en el software para red, sólo este necesita cambiar cuando aparecen nuevas conexiones físicas o cuando

desaparecen conexiones antiguas. De hecho, es posible optimizar la estructura interna de la red de redes alterando las conexiones físicas sin compilar de nuevo los programas de aplicación.

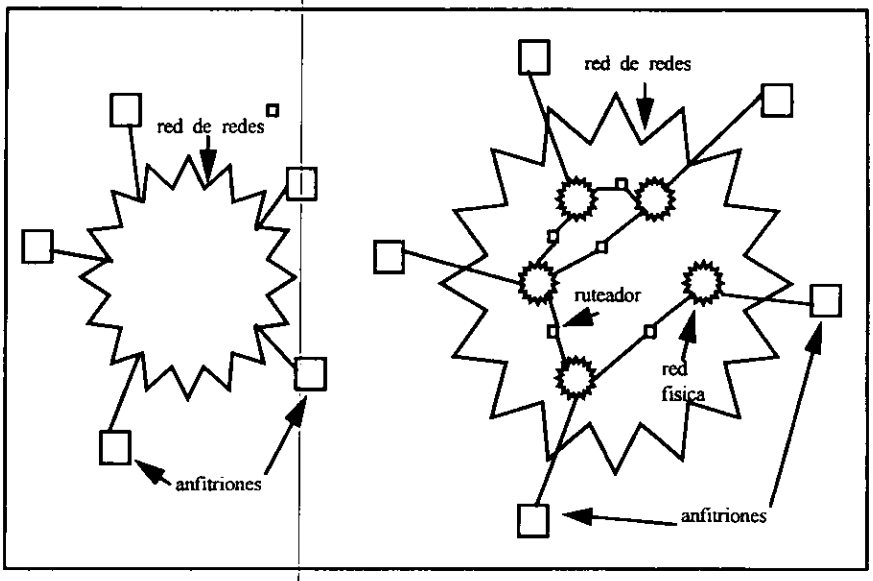


Figura 3.2 Red de redes.

Una segunda ventaja de tener la comunicación a nivel de red es menos visible: los usuarios no tienen que entender o recordar como se conectan las redes o que tipo de tráfico llevan. Se pueden crear programas de aplicación que se comuniquen independientemente de la conectividad física subyacente. De hecho, los gerentes de red están en libertad de cambiar partes interiores de la arquitectura subyacente sin tener que cambiar software de aplicación en la mayoría de las computadoras conectadas.

En la figura 3.2, podemos notar que los ruteadores no proporcionan conexiones directas entre cada par de redes. Puede ser necesario que el tráfico que viaja de una máquina a otra, pase a través de muchas redes intermedias. Por lo tanto, las redes que participan en una red de redes son análogas al sistema de carreteras interestatales de cualquier país: cada red accede a manejar el tráfico

que llegue, a cambio del derecho de enviar tráfico a través de la red de redes. Los usuarios comunes no se ven afectados ni tienen conocimiento del tráfico adicional que pasa por su red local.

3.2 Direcciones IP

Piense en una red de redes como una gran red igual a cualquier otra gran red física. La diferencia, claro esta, es que la red de redes tiene una estructura virtual, imaginada por sus diseñadores e implantada totalmente en software. Por lo tanto, los diseñadores son libres de elegir el formato y tamaño de los paquetes, las direcciones, las técnicas de entrega, y así en adelante; nada es dictado por el hardware. Para las direcciones, los diseñadores del TCP/IP eligen un esquema análogo al direccionamiento en las redes físicas, en el que cada anfitrión en la red de redes tiene asignada una dirección de número entero de 32 bits, llamada su dirección de red de redes o dirección IP. La parte inteligente del direccionamiento en una red de redes es que los números enteros son seleccionados con cuidado para hacer eficiente el ruteo. De manera especifica, una dirección IP codifica la identificación de la red a la que se conecta el anfitrión, así como la identificación de un anfitrión único en esa red.

Los detalles de una dirección IP nos ayudan a entender mejor las ideas abstractas. Cada anfitrión conectado a la red de redes tiene asignado un identificador universal de 32 bits como su dirección dentro de la red. Los bits de dirección IP de todos los anfitriones en una red comparten un prefijo común.

Conceptualmente, cada dirección es un par (net-id, host-id), en donde net-id identifica una red y host-id un anfitrión dentro de la red. En la práctica, cada dirección IP debe tener una de las primeras tres formas mostradas en la figura 3.3.

Definida una dirección IP, se puede determinar su tipo según los tres bits de orden, de los que son necesarios sólo dos bits para distinguir entre los tipos primarios. Las direcciones tipo A, que se utilizan para las pocas redes que tienen mas de 2^{16} de anfitriones (por ejemplo, 65536), asignan 7 bits al campo net-id y 24 bits al campo host-id. Las direcciones tipo B, que se utilizan para redes de tamaño mediano que tienen entre 2^{16} (por ejemplo, 256) y 2^{8} anfitriones, asignan 14 bits al campo net-id y 16 bits al host-id. Por último, las direcciones tipo C, que tienen menos de 2^{8} anfitriones, asignan 21 bits al campo net-id y sólo 8 al host-id. Nótese que las direcciones IP se han definido de tal forma que es posible extraer

rápidamente los campos host-id y net-id. Los ruteadores, que utilizan el campo net-id de una dirección para decidir a donde enviar un paquete, dependen de una extracción eficiente para lograr una velocidad alta.

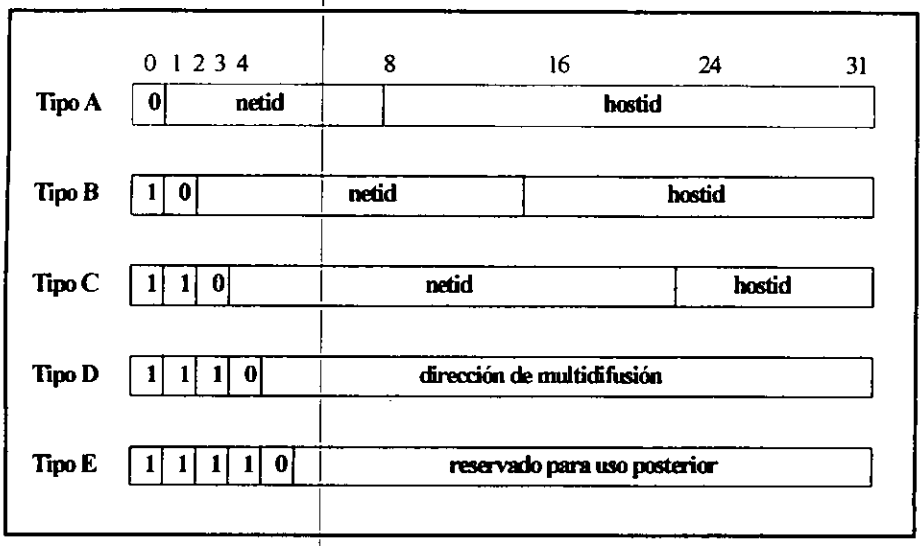


Figura 3.3 Direcciones IP.

Considere un ruteador que conecta dos redes físicas. ¿Cómo podemos asignar una sola dirección IP si dicha dirección codifica un identificador de red así como un identificador de anfitrión? De hecho, no podemos. Cuando computadoras convencionales tienen dos o más conexiones físicas se les llama anfitriones multi-homed. Los anfitriones multi-homed y los ruteadores requieren de muchas direcciones IP. Cada dirección corresponde a una de las conexiones de red de las máquinas. Por lo tanto, un ruteador que conecta cierto número de redes tiene cierto número de direcciones IP distintas, una para cada conexión de red.

La imperfección más importante del esquema de direccionamiento en una red de redes no se volverá evidente hasta que examinemos el ruteo. Sin embargo, su importancia requiere una breve introducción. Hemos sugerido que el ruteo se basara en direcciones de red de redes, con el campo net-id de la dirección utilizado para tomar direcciones de ruteo. Considere un anfitrión con dos

conexiones hacia la red de redes. Sabemos que un anfitrión así debe tener mas de una dirección IP. Lo siguiente es cierto: como el ruteo utiliza la parte de red de la dirección IP, el camino tomado por los paquetes que viajan hacia un anfitrión con muchas direcciones IP depende de la dirección utilizada.

Las implicaciones son sorprendentes. Los humanos piensan en cada anfitrión como en una sola entidad y quieren utilizar un sólo nombre. A veces se sorprenden al encontrar que deben aprender mas de un nombre, y se sorprende aun más cuando encuentran que los paquetes enviados en los que utilizan muchos nombres pueden comportarse de manera diferente.

Cuando se comunican a los usuarios, ya sea en documentos técnicos o a través de programas de aplicación, las direcciones IP se escriben como cuatro enteros decimales separados por puntos, en donde cada entero proporciona el valor de un octeto de la dirección IP. Por lo tanto, la dirección de 32 bits de una red de redes:

10000000 00001010 00000010 00011110

Se escribe:

128.10.2.30

De hecho, la mayor parte del software TCP/IP que muestra una dirección IP o que requiere que una persona la introduzca, utiliza notación decimal con puntos. Por ejemplo, el comando netstat de UNIX que muestra el ruteo actual, y los programas de aplicación como telnet y ftp utilizan la notación decimal con puntos cuando aceptan o muestran direcciones IP.

3.3 Direcciones físicas ARP

Existen dos tipos de direcciones físicas, ejemplificados por Ethernet que tiene direcciones físicas grandes y fijas, así como por proNET que tiene direcciones físicas cortas y de fácil configuración. La asociación de direcciones es difícil para

las redes de tipo Ethernet, pero resulta sencilla para redes como por prenota. Consideremos, primero, el caso más fácil.

Considere una red Token Ring tipo proNET. Recuerde que proNET utiliza números enteros pequeños para sus direcciones físicas y permite que el usuario elija una dirección de hardware cuando instala una tarjeta de interface en una computadora. La clave para facilitar la definición de direcciones con dicho hardware de red radica en observar que, mientras se tenga la libertad de escoger tanto la dirección IP como la física, se puede hacer que ambas posean las mismas partes. Normalmente, una persona asigna direcciones IP como el campo host-id igual a 1,2,3 etc., y luego, cuando instala hardware de interface de red, selecciona una dirección física que corresponda a la dirección IP. Por ejemplo, el administrador de sistema podría seleccionar la dirección física 3 para una computadora que tenga dirección IP 192.5.48.3, debido a que la dirección anterior es tipo C y tiene el campo anfitrión igual a 3.

Para las redes como proNET, computar una red física basándose en una dirección IP es trivial. El cómputo consiste en extraer el campo de anfitrión de la dirección IP. La extracción es computacionalmente eficiente pues sólo necesita unas cuantas instrucciones de máquina. La transformación es fácil de mantener porque se puede realizar sin consultar datos externos. Por último, es posible agregar nuevas máquinas a la red sin cambiar las asignaciones ya existentes ni recopilar los códigos.

Para entender por que la definición de direcciones es difícil para algunas redes, consideraremos la tecnología Ethernet. Ethernet tiene asignada una dirección física de 48 bits desde la fabricación del producto. En consecuencia, cuando el hardware falla y se necesita reemplazar una interface de Ethernet, la dirección física de la máquina cambia. Además, como la dirección Ethernet es de 48 bits, no hay posibilidad de codificarla en una dirección IP de 32 bits.

Los diseñadores de los protocolos TCP/IP encontraron una solución creativa para el problema de la asociación de direcciones en redes como Ethernet, que tienen capacidad de difusión. La solución permite agregar nuevas máquinas a la red, sin tener que recopilar el código y no requiere tener una base de datos centralizada. Para evitar la definición de una tabla de conversiones, los diseñadores utilizan un protocolo de bajo nivel para asignar direcciones en forma dinámica. Conocido como Protocolo de Resolución de Direcciones (ARP), este proporciona un mecanismo razonablemente eficaz y fácil de mantener.

La idea detrás de la asociación dinámica con ARP es muy sencilla: cuando el anfitrión A quiere definir la dirección IP, IP transmite por difusión un paquete especial que pide al anfitrión que posee la dirección IP, que responda con su dirección física, IP. Todos los anfitriones, incluyendo a B, reciben la solicitud, pero sólo el anfitrión B reconoce su propia dirección IP y envía una respuesta que contiene su dirección física. Cuando A recibe la respuesta utiliza la dirección física para enviar el paquete de red de redes directamente a B.

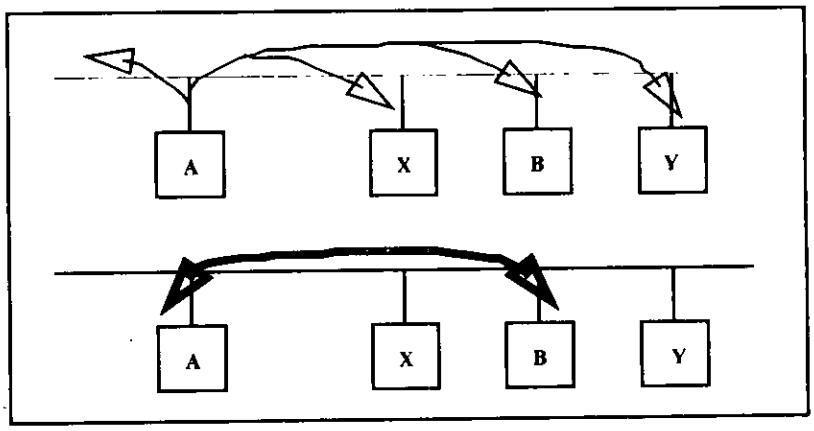


Figura 3.4 Operación de ARP.

Puede parecer extraño que para que A envíe un paquete a B, primero, tenga que transmitir una difusión que llegue a B. Podría parecer aun más extraño que A transmita por difusión la pregunta como puedo llegar hasta ti, en lugar de sólo transmitir por difusión el paquete que quiere entregar. Pero existe una razón importante para este cambio. La difusión es demasiado cara para utilizarse cada vez que una máquina necesita transmitir un paquete a otra, debido a que requiere que cada máquina en la red procese dicho paquete. Para reducir los costos de comunicación, las computadoras que utilizan ARP, mantienen una memoria intermedia de las asignaciones de dirección IP a dirección física recientemente adquiridas, para que no tengan que utilizar ARP varias veces. Siempre que una computadora recibe una respuesta ARP, esta guardada la dirección IP del transmisor, así como la dirección de hardware correspondiente, en su memoria intermedia, para utilizarla en búsquedas posteriores. Cuando transmite un paquete, una computadora siempre busca, en su memoria intermedia, una asignación antes

de enviar una solicitud ARP. Si una computadora encuentra la asignación deseada en su memoria intermedia ARP, no necesitan transmitir una difusión a la red. La experiencia nos indica que, como la mayor parte de la comunicación en red comprende mas que la sola transferencia de un paquete, hasta una memoria intermedia pequeña es muy valiosa.

ARP proporciona un mecanismo para transformar direcciones IP en direcciones físicas; ya hemos visto que algunas tecnologías de red no lo necesitan. El punto es que ARP sería totalmente innecesario si pudiéramos hacer que todo el hardware de red reconociera direcciones IP. Por lo tanto, ARP sólo impone un nuevo esquema de direccionamiento sobre cualquier mecanismo de direccionamiento de bajo nivel que el hardware utilice.

De manera funcional, ARP esta dividido en dos partes. La primera parte transforma una dirección IP en una dirección física cuando se envía un paquete y la segunda responde solicitudes de otras máquinas. La definición de direcciones para los paquetes salientes parece muy clara, pero los pequeños detalles complican la implantación. Al tener una dirección IP de destino, el software consulta su memoria intermedia ARP para encontrar la transformación de la dirección IP a la dirección física. Si la conoce, el software extrae la dirección física, pone los datos en una trama utilizando esa dirección y envía la trama. Si no conoce la transformación, el software debe transmitir una difusión que contenga la solicitud ARP y esperar una respuesta.

La segunda parte del código ARP maneja paquetes que llegan por medio de la red. Cuando llega un paquete ARP, el software extrae la dirección IP del transmisor y la dirección del hardware, luego, examina la memoria temporal local para verificar si ya existe un registro para el transmisor. Si es así, el controlador actualiza el registro al sobreescribir la dirección física con la dirección obtenida del paquete. Después, el receptor procesa el resto del paquete ARP.

El receptor debe manejar dos tipos de paquetes ARP entrantes. Si llega una solicitud ARP, la máquina receptora debe verificar si es el objetivo de la solicitud (por ejemplo, si alguna otra máquina transmitió por difusión una solicitud de la dirección física del receptor). Si es así, el software ARP formula una respuesta al proporcionar su dirección física de hardware y la envía directamente al solicitante. El receptor también agrega el par de direcciones del transmisor a su memoria temporal si estas no están presentes. Si la dirección IP mencionada en la solicitud

ARP no corresponde a la dirección IP local, el paquete solicitara la transformación de alguna otra máquina en la red aunque podría ser ignorado.

Cuando los mensajes ARP viajan de una máquina a otra, se deben transportar en tramas físicas. En la figura 3.5, se muestra como se transporta el mensaje ARP en la porción de datos de una trama.

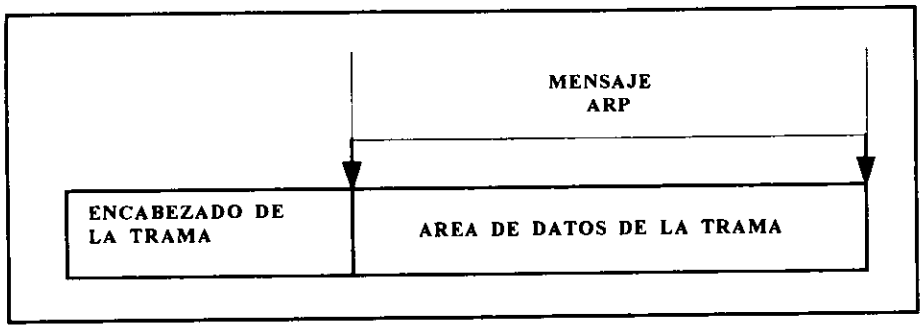


Figura3.5 Transporte de ARP en la sección de datos.

Para identificar que la trama transporta una mensaje ARP, el transmisor asigna un valor especial al campo de tipo en el encabezado de la trama y coloca el mensaje ARP en el campo de datos de la misma. Cuando llega una trama a una computadora, el software de red utiliza el campo de tipo de trama para determinar su contenido. En la mayor parte de las tecnologías, se utiliza un sólo valor para el tipo de todas las tramas que transportan un mensaje ARP -el software de red en el receptor debe examinar el mensaje ARP para distinguir entre solicitudes y respuestas.

A diferencia de la mayor parte de los protocolos, los datos en los paquetes ARP no tienen un encabezado con formato fijo. Por el contrario, para hacer que ARP sea útil para varias tecnologías de red, la longitud de los campos que contienen direcciones depende del tipo de red. Sin embargo, para hacer posible la interpretación de un mensaje ARP arbitrario, el encabezado incluye campos fijos cerca del comienzo, que especifican la longitud de las direcciones que se encuentran en los campos siguientes. De hecho, el formato de un mensaje ARP es los suficientemente general como para permitir que sea utilizado con direcciones físicas arbitrarias y direcciones arbitrarias de protocolos. En el ejemplo de la

figura 3.6 se muestra el formato de 28 octetos de un mensaje ARP que se utiliza en el hardware Ethernet (en que las direcciones físicas tienen una longitud de 4 octetos).

En la figura, se muestra un mensaje ARP con 4 octetos por línea, formato estándar a través de todo este texto. Por desgracia, a diferencia de la mayor parte de los otros protocolos, los campos de longitud variable en los paquetes ARP no se alinean firmemente en fronteras de 32 bits, lo cual causa que el diagrama sea difícil de leer. Por ejemplo, la dirección de hardware del transmisor, etiquetada como SENDER HA, ocupa 6 octetos contiguos, por lo que abarca dos líneas en el diagrama.

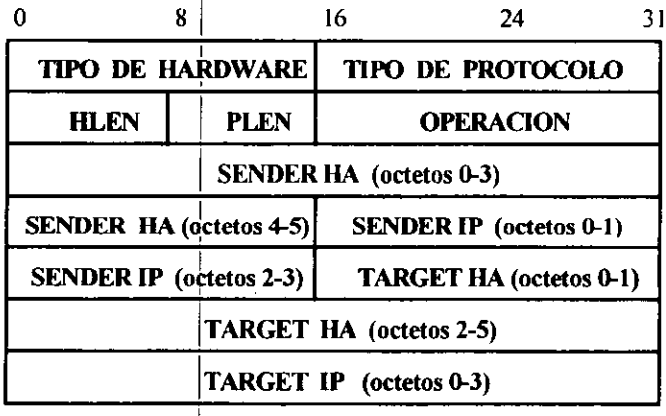


Figura 3.6 Estructura del mensaje ARP.

El campo HARDWARE TYPE especifica un tipo de interface de hardware para el que el transmisor busca una respuesta; contiene el valor 1 para Ethernet. De forma similar, el campo PROTOCOL TYPE especifica el tipo de dirección de protocolo de alto nivel que proporciono el transmisor: contiene 0800 para la dirección IP. El campo OPERATION especifica una solicitud ARP (1), una respuesta ARP (2), una solicitud RARP (3) 0 una respuesta RARP (4). Los campos HLEN y PLEN permiten que ARP se utilice con redes arbitrarias ya que estas especifican la longitud de la dirección de hardware y la longitud de la dirección del protocolo de alto nivel. El transmisor proporciona sus direcciones IP y de hardware, si las conoce, en los campos SENDER HA y SENDER IP. Cuando realiza una solicitud, el transmisor también proporciona la dirección IP

del objetivo (ARP) o la dirección de hardware del objetivo (RARP), utilizando los campos TARGET HA y TARGET IP. Antes de que la máquina objetivo responda, completa las direcciones faltantes, voltea los pares de objetivo y transmisor, y cambia la operación a respuesta. Por lo tanto, una respuesta transporta las direcciones tanto de hardware como de IP del solicitante original, lo mismo que las direcciones de hardware e IP de la máquina para la que realizo asignación.

3.4 Protocolo RARP

Los diseñadores de los protocolos TCP/IP se dieron cuenta de que ya existe otra pieza disponible para la identificación exclusiva, a saber, la dirección física de red de la máquina. Utilizar la dirección física como identificación única tiene dos ventajas. Debido a que un anfitrión obtiene sus direcciones físicas del hardware de interface de red, dichas direcciones siempre están disponibles y no tienen que limitarse al código de iniciación. Como la información de identificación depende de la red y no del modelo o la marca del CPU, todas las máquinas en red proporcionarán identificadores únicos y uniformes. Por lo tanto, el problema se convierte en el inverso de la asociación de direcciones; una vez dada una dirección física de red, invente un esquema que permita que un servidor la transforme en una dirección de red de redes.

Una máquina sin disco utiliza un protocolo TCP/IP para las redes llamado RARP (Protocolo inverso de asociación de direcciones) a fin de obtener su dirección IP desde un servidor. RARP es una adaptación al protocolo ARP y utiliza el mismo formato de mensajes. En la práctica, el mensaje RARP enviado para solicitar una dirección de red de redes es un poco más general: permite que una máquina solicite la dirección IP de una tercera máquina tan fácilmente como si solicitara la suya. También lo permite cuando se trata de muchos tipos de redes físicas.

Al igual que un mensaje ARP, un mensaje RARP se envía de una máquina a otra, encapsulado en la porción de datos de una trama de red. Por ejemplo, una trama Ethernet que transporta una solicitud RARP tiene el preámbulo usual, las direcciones Ethernet tanto fuente como destino y campos de tipo paquete al comienzo de la trama. El tipo de trama contiene el valor 8035 para identificar que el contenido de la trama contiene un mensaje RARP. La porción de datos de la trama contiene el mensaje RARP de 28 octetos.

En la figura 3.7, se ilustra la manera en que un anfitrión utiliza RARP. El que envía transmite por difusión una solicitud RARP especificada como máquina transmisora y receptora, y proporciona su dirección física de red en el campo de dirección de hardware objetivo. Todas las máquinas en la red reciben la solicitud, pero sólo las autorizadas para proporcionar el servicio RARP la procesan y envían la respuesta; dichas máquinas se conocen de manera informal como servidores RARP. Para que RARP funcione correctamente, la red debe contener por lo menos un servidor RARP.

Una vez llamado el campo de dirección de protocolo objetivo, los servidores contestan las solicitudes, cambian el tipo de mensaje de solicitud a respuesta y envían esta de vuelta directamente a la máquina que la solicito. La máquina original recibe respuesta de todos los servidores RARP, aunque sólo necesite una contestación.

Debemos tener en mente que toda la comunicación entre la máquina que busca su dirección IP y el servidor que la proporciona, se debe llevar a cabo utilizando sólo una red física. Además, el protocolo permite que un anfitrión pregunte sobre un objetivo arbitrario. Por lo tanto, el transmisor proporciona su dirección de hardware separada de la dirección de hardware del objetivo y el servidor tiene cuidado de enviar la respuesta a la dirección de hardware del transmisor. En una Ethernet, tener un campo para la dirección de hardware del transmisor podría parecer redundante ya que la información también esta contenida en el encabezado de la trama Ethernet. Sin embargo, no todo el hardware Ethernet proporciona al sistema operativo acceso al encabezado de la trama física.

Como cualquier comunicación en una red de entrega con el mejor esfuerzo, las solicitudes RARP son susceptibles de perdida o corrupción. Ya que RARP utiliza directamente la red física, ningún otro software de protocolos cronometrará la respuesta ni retransmitirá la solicitud; es el software RARP el que debe manejar estas tareas. En general, RARP se utiliza sólo en redes de área local, como Ethernet, en las que la probabilidad de falla es muy baja. Sin embargo, si una red tiene sólo un servidor RARP, dicha máquina quizá no sea capaz de manejar la carga y, por tanto, los paquetes se pierdan.

Algunas estaciones de trabajo que dependen de RARP para realizar su proceso de iniciación reintentan este una y otra vez hasta que reciben una respuesta. Otras implementaciones, al cabo de un par de intentos, lo suspenden indicando que hay

fallas y evitan con ello inundar la red con tráfico innecesario de difusión (por ejemplo, en el caso de que el servidor no esta disponible). En una Ethernet, la falla de red no sucede solamente por la sobrecarga del servidor. Hacer que el software RARP retransmita rápidamente puede causar un efecto indeseable: inundar con mas tráfico un servidor congestionado. Valerse de un retraso largo garantiza que los servidores tengan tiempo suficiente para satisfacer la solicitud y generar una respuesta.

3.5 Protocolo y datagrama de Internet

Hemos analizado una arquitectura de red de redes en la que los ruteadores conectan múltiples redes físicas. Considerar esto exclusivamente como una arquitectura puede ser engañoso, debido a que el enfoque se daría hacia la interface que proporciona la red de redes al usuario, sin considerar la tecnología de interconexión.

Conceptualmente, como se muestra en la figura 3.7 una red de redes TCP/IP proporciona tres conjuntos de servicios; su distribución en la figura sugiere una dependencia entre ellos. En el nivel inferior, un servicio de entrega sin conexión proporciona el fundamento sobre el cual se apoya el resto. En el siguiente nivel, un servicio de transporte confiable proporciona una plataforma de alto nivel de la cual dependen las aplicaciones. Exploraremos cada uno de estos servicios, entendiendo que es lo que proporciona cada uno y considerando los protocolos asociados a ellos.

El servicio más importante de la red de redes consiste en un sistema de entrega de paquetes. Técnicamente, el servicio se define como un sistema de entrega de paquetes sin conexión y con el mejor esfuerzo, análogo al servicio proporcionado por el hardware de red que opera con un paradigma de entrega con el mejor esfuerzo. El servicio se conoce como no confiable porque la entrega no esta garantizada. Los paquetes se pueden perder, duplicar, retrasar o entregar sin orden, pero el servicio no detectara estas condiciones ni informara al emisor o al receptor. El servicio es llamado sin conexión dado que cada paquete es tratado de manera independiente de todos los demás. Una secuencia de paquetes que se envían de una computadora a otra puede viajar por diferentes rutas, algunos de ellos pueden perderse mientras otros se entregan. Por último, se dice que el servicio trabaja con base en una entrega con el menor esfuerzo porque el software de red de redes hace un serio intento por entregar los paquetes. Esto es,

la red de redes no descarta paquetes caprichosamente; la no confiabilidad aparece sólo cuando los recursos están agotados o la red subyacente falla.

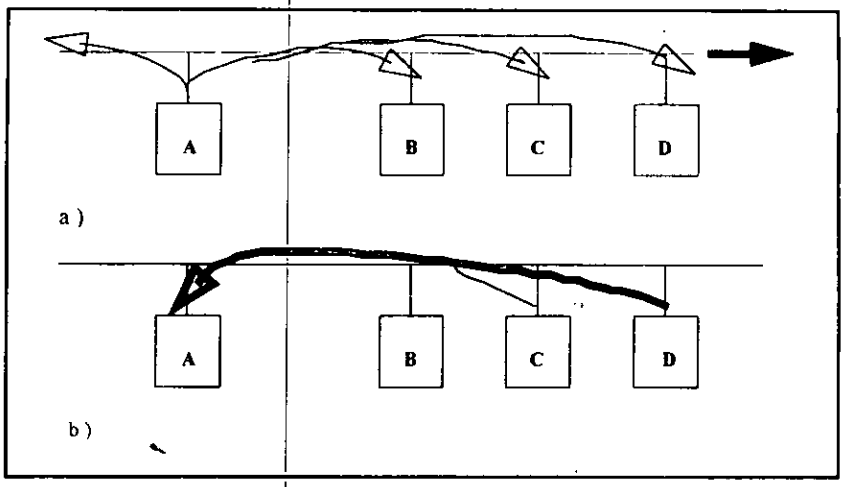


Figura 3.7 Servicios TCP/IP

El protocolo que define el mecanismo de entrega sin conexión y no confiable es conocido como Protocolo Internet y, por lo general se le identifica por sus iniciales, IP. El protocolo IP proporciona tres definiciones importantes. Primero, define la unidad básica para la transferencia de datos utilizada a través de una red de redes TCP/IP. Es decir, especifica el formato exacto de todos los datos que pasaran a través de una red de redes TCP/IP. Segundo, el software IP realiza la función de ruteo, seleccionando la ruta por la que los datos son enviados. Tercero, además de aportar especificaciones formales para el formato de los datos y el rateo, el IP incluye un conjunto de reglas que le dan forma a la idea de entrega de paquetes no confiable. Las reglas caracterizan la forma en que los anfitriones y ruteadores deben procesar los paquetes, como y cuando deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados. El IP es una parte fundamental del diseño de la red de redes TCP/IP, que a veces se conoce como tecnología basada en el IP.

La red de redes llama a esta unidad de transferencia básica datagrama Internet, a veces datagrama IP o simplemente datagrama. Como una trama común de red

física, un datagrama se divide en áreas de encabezado y datos. También, como una trama, el encabezado del datagrama contiene la dirección de la fuente y del destino, contiene también un campo de tipo que identifica el contenido del datagrama. La diferencia, por supuesto, es que el encabezado del datagrama contiene direcciones IP en tanto que el encabezado de la trama contiene direcciones físicas.

Ahora que hemos descrito la disposición general de un datagrama IP, podemos observar su contenido con mayor detalle. Debido a que el proceso de los datagramas se da en el software, el contenido y el formato no esta condicionado por ningún tipo de hardware. Por ejemplo, el primer campo de 4 bits en un datagrama (VERS) contiene la versión del protocolo IP que se utilizó para crear el datagrama. Esto se utiliza para verificar que el emisor, el receptor y cualquier ruteador entre ellos proceda de acuerdo con el formato del datagrama. Todo software IP debe verificar el campo de versión antes de procesar un datagrama para asegurarse de que el formato corresponde el tipo de formato que espera el software. Si hay un cambio en el estándar, las máquinas rechazarán los datagramas son versiones de protocolo que difieren del estándar, evitando con ello que el contenido de los datagramas sea mal interpretado debido a un formato obsoleto.

El campo de longitud encabezado (HLEN), también de 4 bits, proporciona el encabezado del datagrama con una longitud medida en palabras de 32 bits. Como podemos ver, todos los campos del encabezado tienen longitudes físicas excepto para el campo OPTIONS de IP y su correspondiente como PADDING. El encabezado más común, que no contiene opciones ni rellenos, mide 20 octetos y tiene un campo de longitud de encabezado igual a 5.

El campo TOTAL LENGTH proporciona la longitud del datagrama IP medido en octetos, incluyendo los octetos del encabezado y los datos. El tamaño del área de datos se puede calcular restando la longitud del encabezado (HLEN) de TOTAL LENGTH. Dado que el campo TOTAL LENGTH tiene una longitud de 16 bits, el tamaño máximo posible de un datagrama IP es de 2^{16}, una consideración importante en el futuro, si las redes de alta velocidad llegan a transportar paquetes de datos superiores a los 65535 octetos.

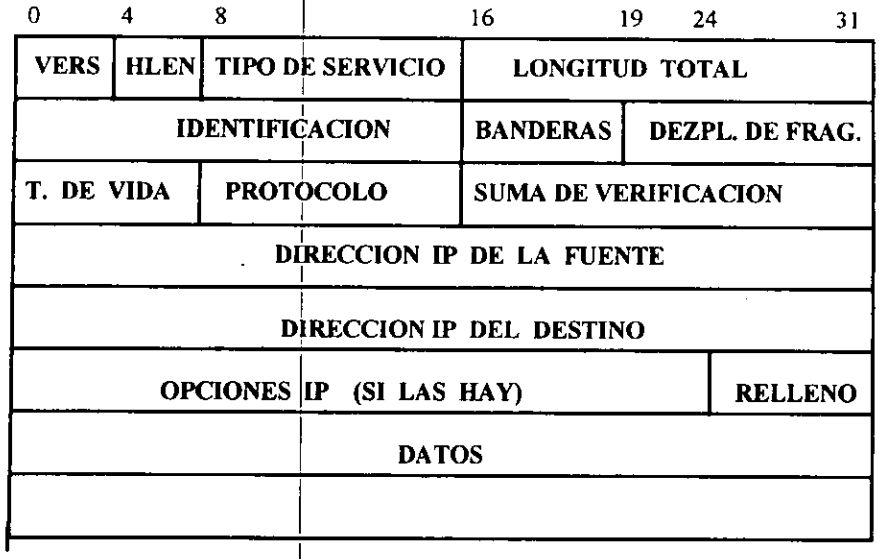


Figura. 3.8 Datagrama IP

Conocido informalmente como Type of Service (TOS), el campo de 8 bits SERVICE TYPE especifica como debe manejarse el datagrama; el campo esta subdividido en 5 subcampos, como se muestra en la figura 3.8:

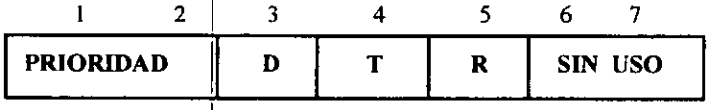


Figura. 3.9 Campo SERVICE TYPE

Tres bits PRECEDENCE especifican la prioridad del datagrama, con valores que abarcan de 0 (prioridad normal) a 7 (control, de red), permitiendo con ello indicar al emisor la importancia de cada datagrama. Aun cuando la mayor parte del software de los anfitriones y los ruteadores ignora el tipo de servicio, este es un concepto importante dado que proporciona un mecanismo que permite controlar la información que tendrá prioridad en los datos.

Los bits D, T y R especifican el tipo de transporte deseado para el datagrama. Cuando esta activado, el bit D solicita procesamiento con retardos cortos, el bit T solicita un alto desempeño y el bit R solicita alta contabilidad.

También es importante para la realización del proceso que los algoritmos de ruteo seleccionen de entre las tecnologías de red física subyacente, las características de retardo, desempeño y confiabilidad. Con frecuencia, una tecnología dada intercambiará una característica por otra (por ejemplo, un alto desempeño implicara un mayor retardo). Así, la idea es proporcionar un algoritmo de ruteo como si se tratara de una indicación de que es lo más importante; rara vez es necesario especificar los tres tipos de servicio juntos. Hemos visto la especificación del tipo de transporte como una indicación para el algoritmo de ruteo que ayuda en la selección de una ruta entre varias hacia un destino, con base en el conocimiento de las tecnologías de hardware disponibles en esas rutas. Una red de redes no garantiza la realización del tipo de transporte solicitado.

A diferencia de las tramas de las redes físicas que pueden ser reconocidas por el hardware, los datagramas son manejados por el software. Estos pueden tener cualquier longitud seleccionada por el diseño de protocolo. Las limitaciones más importantes en el tamaño de un datagrama se dan en la práctica misma.

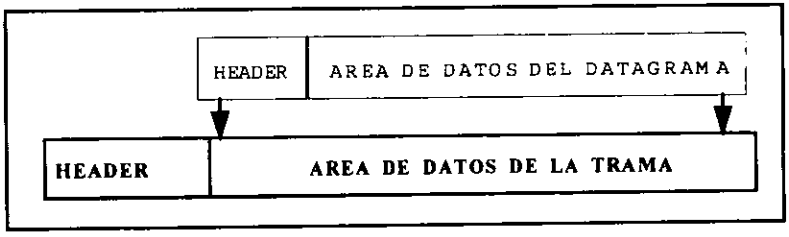


Figura. 3.10 Datagrama en el área de datos de una trama

La idea de transportar un datagrama dentro de una trama de red es conocida como encapsulamiento. Para la red subyacente un datagrama es como cualquier

otro mensaje que se envía de una máquina a otra. El hardware no reconoce el formato del datagrama ni entiende las direcciones destino IP.

En un caso ideal, el datagrama IP completo se ajusta dentro de una trama física haciendo que la transmisión a través de la red física sea eficiente. Para alcanzar esta eficiencia, los diseñadores de IP tendrían que seleccionar un tamaño máximo de datagrama, de manera que el datagrama siempre se ajuste dentro de una trama. ¿Pero que tamaño de trama deberían seleccionar?.

Cada tecnología de conmutación de paquetes establece un limite superior fijo para la cantidad de datos que pueden transferirse en una trama física. Por ejemplo, Ethernet limita la transferencia de datos a 1500 octetos, mientras que FDDI permite aproximadamente 4470 octetos por trama. Nos referiremos a estos límites como la unidad de transferencia máxima de una red (Maximum Transfer Unit, o MTU por sus siglas en inglés). El tamaño de MTU puede ser muy pequeño: algunas tecnologías de hardware limitan la transferencia a 128 octetos o menos. La LIMITACION de los datagramas para que se ajusten a la MTU más pequeña posible en una red de redes hace que la transferencia sea ineficiente cuando estos datagramas pasan a través de una red que puede transportar tramas de tamaño mayor. Sin embargo, permitir que los datagramas sean más grandes que la MTU mínima de una red, en una red de redes, puede significar que un datagrama no siempre se ajuste dentro de una sola trama de red.

La selección debería ser obvia: el punto a considerar en el diseño de una red de redes es ocultar la tecnología de red subyacente y hacer la comunicación conveniente para el usuario. Así, en lugar de diseñar datagramas que se ajusten a las restricciones de la red física, el software TCP/IP selecciona un tamaño de datagrama más conveniente desde el principio y establece una forma para dividir datagramas en péqueños fragmentos cuando el datagrama necesita viajar a través de una red que tiene una MTU pequeña. Las pequeñas piezas dentro de un datagrama dividido se conocen con el nombre de fragmentos y el proceso de división de un datagrama se conoce como fragmentación.

El tamaño de cada fragmento se selecciona, de manera que cada uno de estos pueda transportarse a través de la red subyacente en una sola trama. Además, dado que el IP representa el desplazamiento de datos en múltiplos de 8 octetos, el tamaño del fragmento debe seleccionarse de modo que sea un múltiplo de 8. Por supuesto, al seleccionar el múltiplo de 8 octetos más cercano a la MTU de la red no es usual dividir el datagrama en fragmentos de tamaños iguales; los últimos

fragmentos por lo general son mas cortos que los otros. Los fragmentos se deben reensamblar para producir una copia completa del datagrama original, antes de que pueda procesarse en su lugar de destino.

En una red de redes TCP/IP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas separados hacia su destino final donde serán reensamblados. Preservar los fragmentos en todo el trayecto hasta su destino final tiene dos desventajas. Primero, dado que los datagramas no son reensamblados inmediatamente después de pasar a través de una red con una MTU pequeña, los fragmentos péqueños deben transportarse en esa forma desde el punto de fragmentaron hasta el destino final. Reensamblar los datagramas en el destino final puede implicar que el proceso se realice con cierta ineficiencia: aun cuando se encuentre en una red física con una capacidad de MTU grande después del punto de fragmentaron, esta será atravesada por fragmentos pequeños. Segundo, si se pierde cualquier fragmento, el datagrama no podrá reensamblarse. La máquina de recepción hace que arranquen un temporizador de reensamblado cuando recibe un fragmento inicial. Si el temporizador termina antes de que todos los fragmentos lleguen, la máquina de recepción descartara los fragmentos sin procesar el datagrama. Así la probabilidad de perder un datagrama se incrementa con la fragmentaron ya que la perdida de un sólo fragmento provoca la pérdida del datagrama completo.

Aun considerando desventajas menores, la realización del reensamblado en el destino final trabaja bien. Esto permite que cada fragmento se pueda rutear de manera independiente sin necesidad de que ruteadores intermedios almacenen o reensamblen fragmentos.

Tres campos en el encabezado del datagrama, IDENTIFICATION, FLAGS y FRAGMENT OFFSET, controlan la fragmentación y el reensamblado de los datagramas. El campo IDENTIFICATION contiene un entero único que identifica al datagrama. Recordemos que cuando un ruteador fragmenta un datagrama, este copia la mayor parte de los campos del encabezado del datagrama dentro de cada fragmento. El campo IDENTIFICATION debe copiarse. Su propósito principal es permitir que el destino tenga información acerca de que fragmentos pertenecen a que datagramas. Conforme llega cada fragmento, el destino utiliza el campo IDENTIFICACIÓN junto con la dirección de la fuente del datagrama para identificar el datagrama. Las computadoras que envían datagramas IP deben generar un valor único para el campo IDENTIFICATION por cada datagrama. Hay una técnica utilizada por el software IP que establece un contador global en

memoria, lo incrementa cada vez que se crea un datagrama nuevo y asigna el resultado al campo del datagrama IDENTIFICATION.

Recordemos que cada fragmento tiene exactamente el mismo formato que un datagrama completo. Para un fragmento, el campo FRAGMENT OFFSET especifica el desplazamiento en el datagrama original de los datos que se están acarreando en el fragmento, medido en unidades de 8 octetos, comenzando con un desplazamiento igual a cero. Para reensamblar el datagrama, el destino debe obtener todos los fragmentos comenzando con el fragmento que tiene asignado un desplazamiento igual a 0 hasta el fragmento con el desplazamiento de mayor valor. Los fragmentos no necesariamente llegaran en orden, además no hay comunicación entre el ruteador que fragmento el datagrama y el destino que trata de reensamblarlo.

Los 2 bits de orden menor del campo de 3 bits FLAGS controlan la fragmentación. Por lo general, el software de aplicación que utiliza TCP/IP no se ocupa de la fragmentación debido a que tanto la fragmentación como el reensamblado son procedimientos automáticos que se dan a bajo nivel en el sistema operativo, invisible para el usuario final.

El campo TIME TO LIVE especifica la duración, en segundos, del tiempo que el datagrama tiene permitido permanecer en el sistema de red de redes. La idea es sencilla e importante: cada vez que una máquina introduce un datagrama dentro de la red de redes, se establece un tiempo máximo durante el cual el datagrama puede permanecer ahí. Los ruteadores y los anfitriones que procesan los datagramas deben decrementar el campo TIME TO LIVE cada vez que pasa un datagrama y eliminarlo de la red de redes cuando su tiempo ha concluido.

Cada ruteador, a lo largo de un trayecto, desde una fuente hasta un destino, es configurado para decrementar por 1 el campo TIME TO LIVE cuando se procesa el encabezado del datagrama. Sin embargo, para manejar casos de ruteadores sobrecargados que introducen largos retardos, cada ruteador registra el tiempo local cuando llega un datagrama, y decrementa el TIME TO LIVE por el número de segundos que el datagrama permanece dentro del ruteador esperando que se le despache.

Cada vez que un campo TIME TO LIVE llega a cero, el ruteador descarta el datagrama y envía un mensaje de error a la fuente. La idea de establecer un temporizador para los datagramas es interesante ya que garantiza que los

datagramas no viajarán a través de la red de redes indefinidamente, aun cuando si una tabla de ruteo se corrompa y los ruteadores direccionen datagramas en un ciclo.

Hablando de otros campos de encabezado de datagrama; el campo PROTOCOL es análogo al campo tipo en una trama de red. PROTOCOL especifica que protocolo de alto nivel se utilizo para crear el mensaje que se esta transportando en el área DATA de un datagrama. En esencia, el valor de PROTOCOL especifica el formato del área DATA. La transformación entre un protocolo de alto nivel y el valor entero utilizado en el campo PROTOCOL debe administrarlo por una autoridad central para garantizar el acuerdo entre los enteros utilizados en Internet.

El campo HEADER CHECKSUM asegura la integridad de los valores del encabezado. La suma de verificación IP se forma considerando al encabezado como una secuencia de enteros de 16 bits (en el orden de los octetos de la red), sumándolos juntos mediante el complemento aritmético uno a uno, y después tomando el complemento a uno del resultado. Para propósitos de calculo de la suma de verificación, el campo HEADER CHECKSUM se asume como igual a cero.

Los campos SOURCE IP ADDRESS y DESTINATION IP ADDRESS contienen direcciones IP de 32 bits de los datagramas del emisor y del receptor involucrado. Aun cuando los datagramas sean dirigidos a través de muchos ruteadores inmediatos, los campos de fuente y destino nunca cambian; estos especifican la dirección IP de la fuente original y del destino final.

El campo marcado con el nombre DATA en la figura 3.8 muestra el comienzo del área de datos de un datagrama. Su longitud depende, por supuesto, de que es lo que se esta enviando en el datagrama. El campo OPTIONS de IP que se analiza a continuación tiene una longitud variable. El campo señalado como PADDING depende de las opciones seleccionadas. Este representa un grupo de bits puestos en cero que podrían ser necesarios para asegurar que la extensión del encabezado sea múltiplo exacto de 32 bits (recordemos que el campo de longitud del encabezado se especifica en unidades formadas en palabras de 32 bits).

3.6 Ruteo de datagramas IP

En un sistema de conmutación de paquetes, el ruteo es el proceso de selección de un camino sobre el que se mandarán paquetes y el ruteador es la computadora que hace la selección.

El ruteo en una red de redes puede ser difícil, en especial entre computadoras que tienen muchas conexiones físicas de red. De forma ideal, el software de ruteo examinara aspectos como la carga de la red, la longitud del datagrama o el tipo de servicio que se especifica en el encabezado del datagrama, para seleccionar el mejor camino. Sin embargo, la mayor parte del software de ruteo en red de redes es mucho menos sofisticado y selecciona rutas basándose en suposiciones sobre los caminos más cortos.

Los ruteadores toman decisiones de ruteo IP (ese es su principal propósito y la razón de llamarlos ruteadores). Cualquier computadora con muchas conexiones de red puede actuar como ruteador y, como veremos, los anfitriones multi-homed que ejecutan el TCP/IP tienen todo el software necesario para el ruteo. Además, los sitios que no pueden adquirir ruteadores por separado a veces utilizan máquinas de tiempo compartido y propósito general como anfitriones y ruteadores. Sin embargo, los estándares TCP/IP hacen una gran diferenciación entre las funciones de un anfitrión y las de un ruteador, además los sitios que intentan mezclar funciones de anfitrión con funciones de ruteador en una sola máquina, a veces, encuentran que sus anfitriones multi-homed llevan a cabo interacciones inesperadas. Por ahora, distinguiremos los anfitriones de los ruteadores y asumiremos que los primeros no realizan la función, exclusiva de los ruteadores, de transferir paquetes de una red a otra.

Hablando sin formalismos, podemos dividir el ruteo en dos partes: entrega directa y entrega indirecta. La entrega directa, que es la transmisión de un datagrama desde una máquina a través de una sola red física hasta otra, es la base de toda la comunicación en una red de redes. Dos máquinas solamente pueden llevar a cabo la entrega directa si ambas se conectan directamente al mismo sistema subyacente de transmisión física (por ejemplo, una sola Ethernet). La entrega indirecta ocurre cuando el destino no es una red conectada directamente, lo que obliga al transmisor a pasar el datagrama a un ruteador para su entrega. ¿Cómo sabe el transmisor si el destino reside en una red directamente conectada? La respuesta es la siguiente: sabemos que las direcciones IP se dividen en un

destino reside en una de las redes directamente conectadas, el transmisor extrae la porción de red de la dirección IP de destino y la compara con la porción de red de su propia dirección IP. Si corresponden, significa que el datagrama se puede enviar de manera directa. Aquí vemos una de las ventajas del esquema de direccionamiento de Internet.

Desde la perspectiva de una red de redes, la forma más fácil de pensar en la entrega directa es como el paso final de cualquier transmisión de datagramas, aun si el datagrama atraviesa muchas redes y ruteadores intermedios. El último ruteador del camino entre la fuente del datagrama y su destino siempre se conectará directamente a la misma red física que la máquina de destino. Por lo tanto, el último ruteador entregará el datagrama utilizando la entrega directa. Podemos pensar en la entrega directa entre la fuente y el destino como un caso especial de ruteo de propósito general -en una ruta directa, el datagrama nunca pasa a través de ningún ruteador intermedio.

La entrega indirecta es más fácil que la directa porque el transmisor debe identificar un ruteador para enviar el datagrama. Luego, el rutedor debe encaminar el datagrama hacia la red de destino.

Para visualizar como trabaja el ruteo indirecto, imagínese una gran red con muchas redes interconectadas por medio de ruteadores, pero sólo con dos anfitriones en sus extremos más distantes. Cuando un anfitrión quiere enviar un datagrama a otro, lo encapsula y lo envía hacia el ruteador más cercano. Sabemos que se puede alcanzar un ruteador debido a que todas las redes físicas están interconectadas, así que debe existir un ruteador conectado a cada una. Por lo tanto, el anfitrión de origen puede alcanzar un ruteador utilizando una sola red física. Una vez que la trama llega al ruteador, el software extrae el datagrama encapsulado, y el software IP selecciona el siguiente ruteador a lo largo del camino hacia el destino. De nuevo, se coloca el datagrama en una trama y se envía a través de la siguiente red física hacia un segundo ruteador, y así sucesivamente, hasta que se pueda entregar de forma directa.

¿Cómo sabe un ruteador a donde enviar cada datagrama? ¿Cómo puede saber un anfitrión que ruteador utilizar para llegar a un destino determinado? Las dos preguntas están relacionadas ya que comprenden el ruteo IP.

El algoritmo usual de ruteo IP emplea una tabla de ruteo Internet (a veces, conocida como tabla de ruteo IP) en cada máquina que almacena información

El algoritmo usual de ruteo IP emplea una tabla de ruteo Internet (a veces, conocida como tabla de ruteo IP) en cada máquina que almacena información sobre posibles destinos y sobre como alcanzarlos. Debido a que tanto los ruteadores como los anfitriones rutean datagramas, ambos tienen tablas de ruteo IP. Siempre que el software de ruteo IP en un anfitrión necesita transmitir un datagrama, consulta la tabla de ruteo para decidir a donde enviarlo.

¿Que información se debe guardar en las tablas de ruteo? Si cada tabla de ruteo contuviera información sobre cada posible dirección de destino, seria imposible mantener actualizadas las tablas. Además, como el número de destinos posibles es muy grande, las máquinas no tendrían suficiente espacio para almacenar la información.

De manera conceptual, nos gustaría utilizar el principio de ocultación de información y permitir a las máquinas tomar decisiones de ruteo con una información mínima. Por ejemplo, nos gustaría aislar la información sobre anfitriones específicos del ambiente local en el que existen y hacer que las máquinas que están lejos ruteen paquetes hacia ellos sin saber dichos detalles. Por fortuna, el esquema de direccionamiento IP nos ayuda a lograr este objetivo. Recordemos que las direcciones IP se asignan de tal manera que todas las máquinas conectadas a una red física compartan un prefijo común (la porción de red de la dirección). Ya hemos visto que una asignación de este tipo hace que la comprobación para la entrega directa sea eficiente. También significa que las tablas de ruteo sólo necesitan contener prefijos de red y no direcciones IP completas.

Utilizar la porción de red de una dirección de destino tal vez de toda la dirección de anfitrión hace que el ruteo sea eficiente y mantiene reducidas las tablas de ruteo. También es importante, porque ayuda a ocultar información al mantener los detalles de los anfitriones específicos confinados al ambiente local en el que operan. Por lo común, una tabla de ruteo contiene pares (N, R), donde N es la dirección IP de una red de destino y R la dirección IP del "siguiente" ruteador en el camino hacia la red N. El rutedor R es conocido como el salto al siguiente y la idea de utilizar una tabla de ruteo para almacenar un salto siguiente para cada destino es conocida como ruteo con salto al siguiente. Por lo tanto, la tabla de ruteo en el ruteador R sólo especifica un paso a lo largo del camino de R a su red de destino -el ruteador no conoce el camino completo hacia el destino.

el ruteador R. Ya que R se conecta de manera directa a las redes 20.0.0.0 y 30.0.0.0, puede utilizar la entrega directa para llevar a cabo un envío a un anfitrión en cualquiera de esas redes (posiblemente utilizando ARP para encontrar las direcciones físicas). Teniendo un datagrama destinado para un anfitrión en la red 40.0.0.0, R lo rutea a la dirección 30.0.0.7, que es la dirección del ruteador S. Luego, S entregara el datagrama en forma directa. R puede alcanzar la dirección 30.0.0.7 debido a que tanto R como S se conectan directamente con la red 30.0.0.0.

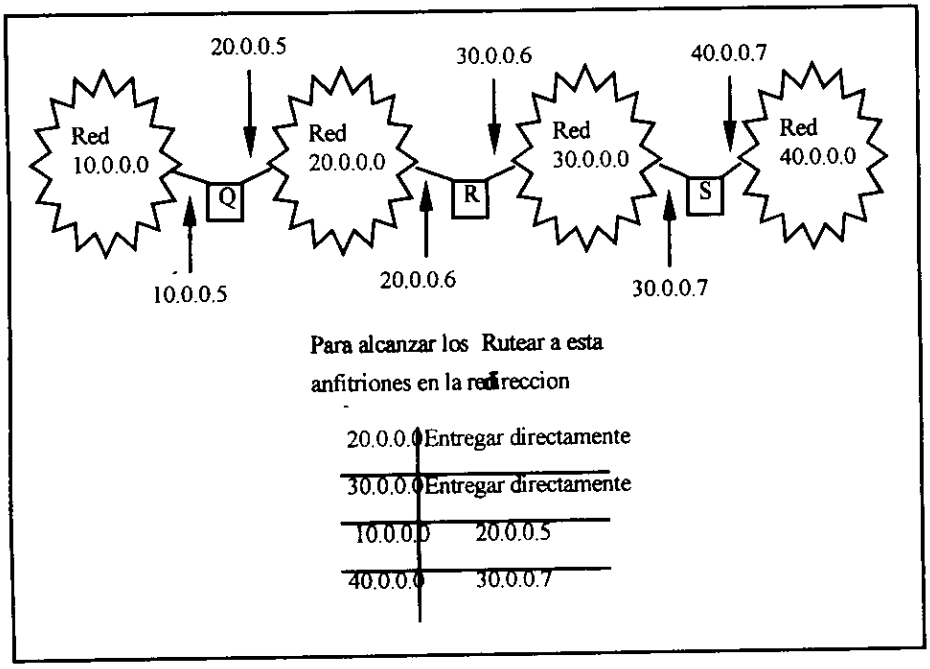


Figura 3.10 Tabla de ruteo

Como se demuestra en la figura 3.10, el tamaño de la tabla de ruteo depende del número de redes en la red; solamente crece cuando se agregan nuevas redes. Sin embargo, el tamaño y contenido de la tabla son independientes del número de anfitriones individuales conectados a las redes.

Sin embargo, el tamaño y contenido de la tabla son independientes del número de anfitriones individuales conectados a las redes.

Escoger rutas basándose tan sólo en la identificación de la red de destino tiene muchas consecuencias. Primero, en la mayor parte de las implantaciones, significa que todo el tráfico destinado a una cierta red toma el mismo camino. Como resultado, aun cuando existen muchos caminos, quizá no se utilicen constantemente. De igual manera, todos los tipos de tráfico siguen el mismo camino sin importar el retraso o la generación de salida de las redes físicas. Segundo, debido a que sólo el último ruteador del camino intenta comunicarse con el anfitrión final, solamente este ruteador puede determinar si el anfitrión existe o esta en operación. Por lo tanto, necesitamos encontrar una forma para que el ruteador envíe reportes sobre problemas de entrega, de vuelta a la fuente original. Tercero, debido a que cada ruteador rutea el tráfico de forma independiente, los datagramas que viajan del anfitrión A al B pueden seguir un camino totalmente distinto al que siguen los datagramas que viajan del anfitrión B al A. Necesitamos asegurarnos de que los ruteadores cooperen para garantizar que siempre sea posible la comunicación bidireccional.

Otra técnica utilizada para ocultar información y mantener reducido el tamaño de las tablas de ruteo, es asociar muchos registros a un ruteador asignado por omisión. La idea es hacer que el software de ruteo IP busque primero la tabla de ruteo para encontrar la red de destino. Si no aparece una ruta en la tabla, las rutinas de ruteo envían el datagrama a un ruteador asignado por omisión. El ruteo asignado por omisión es de gran ayuda cuando un sitio tiene pocas direcciones locales y sólo una conexión con el resto de la red de redes.

Aunque hemos dicho que todo el ruteo esta basado en redes y no en anfitriones individuales, la mayor parte del software de ruteo IP permite que se especifiquen rutas por anfitrión como caso especial. Tener rutas por anfitrión le da al administrador de red local un mayor control sobre el uso de la red, le permite hacer comprobaciones y también se puede utilizar para controlar el acceso por razones de seguridad. Cuando se depuran conexiones de red o tablas de ruteo, la capacidad para especificar una ruta especial hacia una máquina individual resulta ser especialmente útil.

CAPITULO 4

SWITCHES Y RUTEO

4.1 Ruteo

Un ruteador es un dispositivo que permite que sean enviados mensajes entre dos o más redes. Es un nodo direccionable que podría ser como una pequeña caja que se sitúa en el "Communications Closet" cerca del concentrador, o una computadora con NIC's (tarjetas de interface de red) y software especial.

Los ruteadores trabajan en una manera similar a los puentes, no obstante, los ruteadores operan con los protocolos de la capa de red (capa 3) del modelo OSI, mientras que los puentes operan en la capa física (capa 1)o con los protocolos de la capa de enlace de datos (capa 2). Como un puente, un ruteador tiene su propio microprocesador y sabe donde se encuentran localizadas las estaciones de trabajo, pero, un ruteador tiene un software más inteligente que un puente y es más adecuado para ambientes con redes mixtas.

La operación de un ruteador depende del uso de un protocolo de trabajo interredes. La figura 4.1 muestra un ejemplo del uso típico de IP, en el cual dos LAN's están interconectadas por una WAN de conmutación de paquetes X.25. La figura muestra la operación de un protocolo internet para el intercambio de datos entre el host A y una LAN (subred 1) y un host B en otra LAN (subred 2) a través de la WAN. La figura muestra el formato de la unidad de datos en cada etapa. Las terminales y los ruteadores deben compartir un protocolo internet común. Además, las terminales deben compartir los protocolos superiores a IP (capas 4 a 7). Los ruteadores intermedios necesitan solo de IP.

El IP en "A" recibe bloques de datos para ser enviados a "B" de las capas superiores de software en "A". IP une un encabezado especificando, entre otras cosas, la dirección internet global de "B". Esa dirección tiene dos partes lógicas: identificador de red e identificador de terminal. El resultado es llamado una unidad de datos de protocolo internet, o simplemente un datagrama. El datagrama entonces se encapsula con el protocolo LAN y se envía al ruteador, que separa los campos LAN para leer el encabezado IP. Después, el ruteador encapsula el

datagrama con los campos de protocolo X.25 y los transmite a través de la WAN a otro ruteador. Este ruteador extrae los campos X.25 y recupera el datagrama, le coloca los campos LAN apropiados a la LAN 2 y lo envía a B.

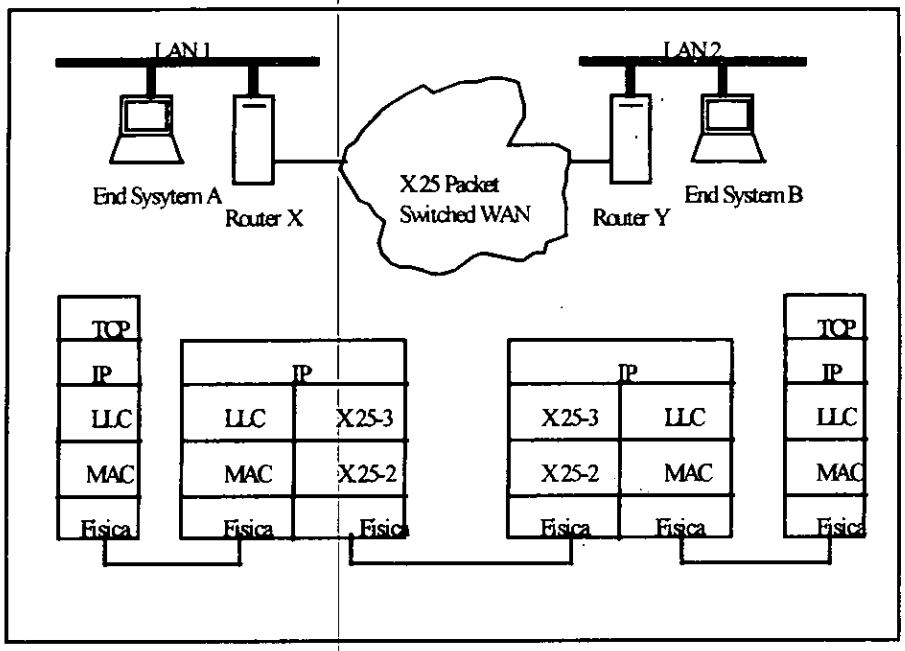


Figura 4.1 LAN's interconectadas por una WAN.

Veamos ahora este proceso con más detalle. La terminal A tiene un datagrama para transmitir a la terminal B; el datagrama incluye la dirección internet de B. El módulo IP en A reconoce que el destino (B) esta en otra subred. Así que el primer paso es enviar los datos a un ruteador, en este caso ruteador X. Para lograr esto, IP pasa el datagrama hacia abajo a la siguiente capa (en este caso LLC) con instrucciones de enviarlo al ruteador X. LLC en cambio pasa esta información hacia la capa MAC, que inserta el nivel de dirección MAC del ruteador X en el encabezado MAC. De tal manera que el bloque de datos transmitido hacia la LAN 1 incluye datos de una capa o capas superiores TCP, más un encabezado TCP, un encabezado IP, un encabezado LLC y un encabezado y una cola ("trailer").

Enseguida, el paquete viaja a través de la subred 1 al ruteador X. El ruteador remueve los campos MAC y LLC y analiza el "header" IP para determinar el destino final de los datos, en este caso B. El ruteador debe hacer ahora una decisión de ruteo. Existen 3 posibilidades:

- La estación de destino Y es conectada directamente a una de las subredes a la que el ruteador esta unido. En este caso el ruteador envía el datagrama directamente al destino.
- Para llegar a su destino, uno o más ruteadores adicionales deben ser atravesados. En este caso una decisión de ruteo debe realizarse: ¿a que ruteador debe ser enviado el datagrama? En ambos casos el módulo IP en el ruteador envía el datagrama hacia la siguiente capa inferior con la dirección de destino de subred. Nótese que estamos hablando de dirección de capa inferior que se refieren a esta red.
- El ruteador no sabe la dirección de destino. En este caso el ruteador regresa un mensaje de error a la fuente del datagrama.

En este ejemplo los datos deben pasar a través de un ruteador Y antes de que alcancen su destino. Así, el ruteador X envía un nuevo paquete al agregar un encabezado X.25, conteniendo la dirección del ruteador Y, a la unidad de datos IP. Cuando este paquete llega al ruteador Y, el encabezado del paquete se extrae. El ruteador determina que esta unidad de datos IP esta destinada a B, que esta conectada directamente a la red en la cual el ruteador trabaja. Por lo tanto el ruteador, crea una trama con una dirección de destino de B y la envía dentro de la LAN 2. Los datos finalmente llegan a B, donde los encabezados IP y LAN pueden ser extraídos.

En cada ruteador, antes de que los datos sean enviados, puede ser necesario segmentar los datos para acomodarlos al tamaño máximo de trama permisible en esa trama en particular. La unidad de datos es dividida en dos o más segmentos, cada uno de los cuales se convierte en una unidad de datos IP independiente. Cada nueva unidad de datos es colocada en un paquete de capa inferior y se pone en fila para ser transmitida. El ruteador podría también limitar el largo de la fila para cada red a la cual esta unido para evitar tener una red lenta penalizando a una rápida. Una vez que se alcanza el límite, las unidades de datos adicionales son simplemente desechadas.

El proceso descrito anteriormente continua a través de tantos ruteadores como sea necesario atravesar para que el paquete llegue a su destino. Como los ruteadores, las terminales recuperan la unidad de datos IP de su red. Si ha

ocurrido segmentación, el modulo IP en la terminal pone en un buffer los datos entrantes hasta que el mensaje completo pueda ser reensamblado. Después este bloque de datos es pasado a una capa superior de la terminal.

Este servicio ofrecido por el protocolo internet es no confiable. Esto es, el protocolo internet no garantiza que todos los datos serán entregados o que los datos que son entregados llegarán en el orden apropiado. Es responsabilidad de la siguiente capa superior (por ejemplo TCP) el recuperar cualquier error que ocurra.

Con el acceso del protocolo internet, cada unidad de datos es pasada de un ruteador a otro en un intento de que la fuente alcance al destino. Debido a que la entrega no esta garantizada, no existe un requerimiento particular de formalidad en ninguna de las subredes. De tal forma que el protocolo funcionará con cualquier combinación de tipos de subredes. Debido a que la secuencia de entrega no esta garantizada, unidades sucesivas de datos pueden seguir diferentes vías a través de internet. Esto permite al protocolo reaccionar a la congestión y falla en la red simplemente cambiando rutas.

Con este breve esquema de la operación de internet controlada por IP, podemos examinar algunos tópicos de disueno, como serian: direccionamiento, ruteo, vida de datagrama, segmentación y reensamblado. Además mantener correctamente tablas de ruteo en todos los ruteadores en una gran red internet es una tarea compleja. En la mayor parte de los casos, las tablas de ruteo son mantenidas dinámicamente para reflejar la topología actual de los sistemas internet y permitir el ruteo alrededor de enlaces con fallas. Un ruteador normalmente completa esto al participar en un protocolo de ruteo con otros ruteadores. Algunos de los protocolos de ruteo más populares en el ambiente TCP/IP son:

- Routing Information Protocol (RIP).
- Open Shortest Path First Protocol (OSPF).
- Exterior Gateway Protocol (EGP).
- Border Gateway Protocol (BGP).

Para poder proceder en nuestra discusión de protocolos ruteador a ruteador, necesitamos introducir el concepto de sistema autónomo. Un sistema autónomo es una red conectada por ruteadores homogéneos; generalmente los ruteadores están bajo el control administrativo de una entidad única. Un protocolo de ruteo interior (IRP) pasa información de ruteo entre los ruteadores dentro de un sistema autónomo. El protocolo usado dentro del sistema autónomo no necesita ser

implementado fuera del sistema. Esta flexibilidad permite a los que los IRP's sean configurados para requerimientos y aplicaciones especificas.

Puede ocurrir, de cualquier modo, que una internet esté constituida de más de un sistema autónomo. Por ejemplo, todas las LAN en un sitio, tal como un complejo de oficinas o campus, podrían ser enlazadas por ruteadores para formar un sistema autónomo. Este sistema podría ser enlazado a través de una red WAN a otros sistemas autónomos. Esta situación es ilustrada en la figura. En este caso los algoritmos y las tablas de ruteo usadas por los ruteadores en diferentes sistemas autónomos pueden diferir. No obstante, los ruteadores en un sistema autónomo necesitan al menos, un mínimo de información concerniente a las redes fuera de su sistema. El protocolo usado para pasar la información de ruteo en diferentes sistemas autónomos es llamado protocolo de ruteo exterior (EGP).

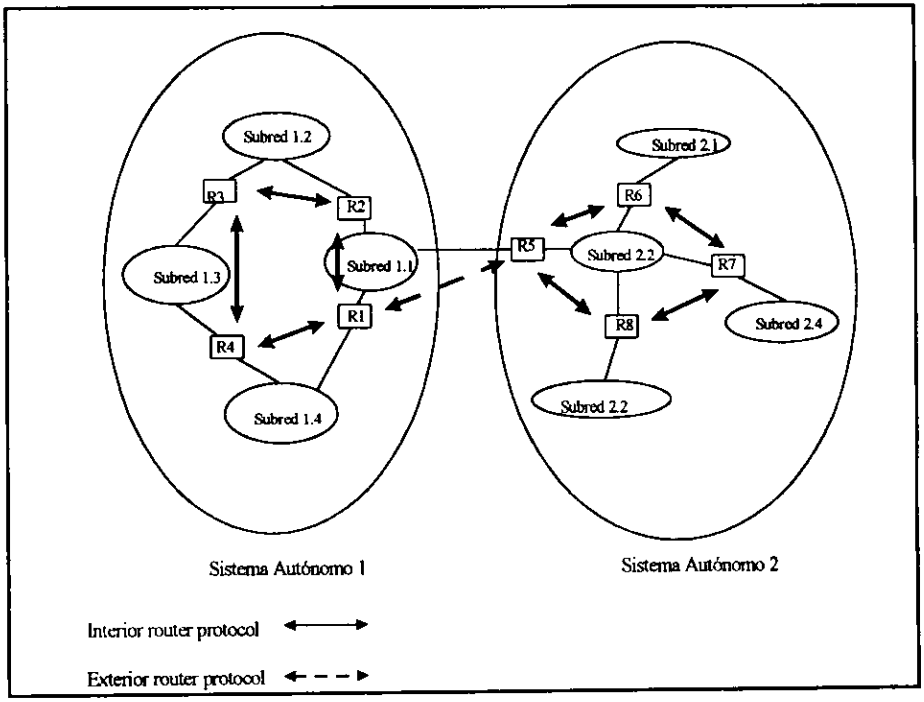


Figura 4.2 Sistemas autónomos

Podemos esperar que un ERP necesitara menor información y ser más simple que un IRP, por la siguiente razón. Si un datagrama será transmitido de un host en

un sistema autónomo a un host en otro sistema autónomo, un ruteador en el primer sistema necesita solamente determinar el sistema autónomo de destino y encontrar un ruteador para entrar al sistema de destino. Una vez que el datagrama entra al sistema autónomo destino, los ruteadores internos de ese sistema pueden cooperar para finalmente entregar el datagrama.

4.1.1 Exterior Gateway Protocol (EGP)

A dos ruteadores que intercambian información de ruteo se les llama vecinos exteriores, si pertenecen a dos sistemas autónomos diferentes, y vecinos interiores si pertenecen al mismo sistema autónomo. El protocolo que emplea vecinos exteriores para difundir la información de accesibilidad a otros sistemas autónomos se le conoce como Protocolo de Pasarela Exterior (Exterior Gateway Protocol) o EGP, y los ruteadores que se utilizan se conocen como ruteadores exteriores. En la conexión de Internet, el EGP es especialmente importante ya que los sistemas autónomos lo emplean para difundir información de accesibilidad hacia el sistema de núcleo.

La figura 4.3 muestra dos vecinos exteriores que utilizan el EGP. El ruteador R1 recoge información acerca de las redes en el sistema autónomo 1 y reporta esta información al ruteador R2 mediante el EGP, mientras el ruteador R2 reporta información desde el sistema autónomo 2.

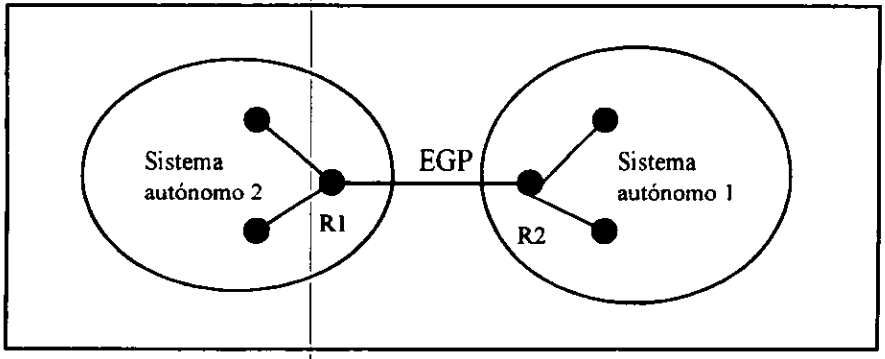


Figura 4.3 Vecinos exteriores que utilizan EGP.

El EGP tiene tres características principales. Primero, soporta un mecanismo de adquisición de vecino que permite a un ruteador solicitar a otro un acuerdo para que los dos comuniquen información de accesibilidad. Decimos que un

ruteador consigue un par EGP (EGP peer), o un vecino EGP. Los pares EGP son vecinos solo en el sentido en que estos intercambiaran información de ruteo, con lo cual no se hace alusión a su proximidad geográfica. Segundo un ruteador prueba continuamente si su vecino EGP esta respondiendo. Tercero, los vecinos EGP intercambian información de accesibilidad de red de manera periódica, transfiriendo un mensaje de actualización de ruteo. Para implementar las tres funciones básicas, el EGP define nueve tipos de mensajes:

- **Acquisition Request**
  Solicitud para que un ruteador se defina como vecino (par).
- **Acquisition Confirm**
  Respuesta positiva a la solicitud de adquisición.
- **Acquisition Refuse**
  Respuesta negativa a la solicitud de adquisición.
- **Cease Request**
  Solicitud para terminar la relación con un vecino.
- **Cease Confirm**
  Respuesta de afirmación para suspender la solicitud.
- **Hello**
  Solicitud a un vecino para que responda si esta activo.
- **I Heard you**
  Respuesta al mensaje Hello.
- **Poll Request**
  Solicitud de actualización de ruteo de red.
- **Routing Update**
  Información de accesibilidad de red.
- **Error**
  Respuesta a un mensaje incorrecto.

Todos los mensajes EGP comienzan con un encabezado fijo que identifica el tipo de mensaje. Figura 4.4.

El EGP restringe a los ruteadores permitiéndoles anunciar solo los destinos de red completamente accesibles dentro del sistema autónomo del ruteador. Sin embargo, hay una limitación más importante impuesta por el EGP. El EGP no interpreta ninguna de las métricas de distancia que aparecen en los mensajes de actualización de ruteo.

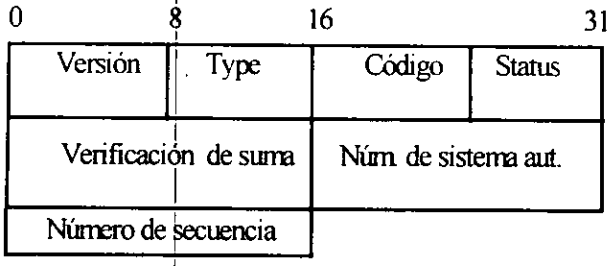


Figura 4.4 Encabezado EGP.

La regla especifica que un valor de 255 significa que la red es inaccesible, pero otros valores son también comparables si estos se refieren a ruteadores en el mismo sistema autónomo. En esencia el EGP utiliza el campo de distancia para especificar si una trayectoria existe; el valor no puede usarse para calcular la proximidad de dos rutas a menos que ambas se encuentren dentro de un solo sistema autónomo. Debido a que el EGP solo difunde información de accesibilidad, restringe la topología de cualquier red de redes que utilice el EGP, a una estructura de árbol en la que un sistema de núcleo forma la raíz; no hay ciclos entre otros sistemas autónomos conectados.

4.1.2 Border Gateway Protocol (BGP)

El BGP fue desarrollado para su uso en conjunción con internets que emplean el protocolo TCP/IP, no obstante los conceptos son aplicables a cualquier internet. BGP se ha convertido en el estándar de protocolo de ruteo exterior para Internet.

BGP fue diseñado para permitir a los ruteadores, llamados compuertas en el estándar, cooperar en el intercambio de información de ruteo en diferentes sistemas autónomos. El protocolo opera en términos de mensajes, que son enviados sobre conexiones TCP. El repertorio de mensajes es resumido en la tabla 4.5:

- Adquisición de vecinos.
- Accesibilidad del vecino.
- Accesibilidad de la red.

Mensaje	Definición
Open	Usado para abrir una relación de vecino con otro ruteador
Update	Usado para (1) transmitir información acerca de una ruta en particular y/o (2) listar multiples rutas accesibles
Keepalive	Usado para (1) reconocer un mensaje Open y (2) periódicamente confirmar la relación de vecino
Notification	Se envia cuando se detecta una condición de error

Tabla 4.5 Mensajes BGP

Dos ruteadores son considerados vecinos si están unidos a la misma subred. Si dos ruteadores están en diferentes sistemas autónomos, podrían querer intercambiar información de ruteo. Para este propósito es necesario primeramente realizar una adquisición de vecino. El término vecino se refiere a dos ruteadores que comparten la misma subred. En esencia, la adquisición de vecino ocurre cuando dos ruteadores vecinos en diferentes sistemas autónomos acuerdan intercambiar información de ruteo. Un procedimiento de adquisición formal es necesario desde que uno de los ruteadores puede no querer participar. Por ejemplo, el ruteador puede estar sobrecargado y no querer responsabilizarse del tráfico proveniente de un sistema externo. En el proceso de adquisición de vecino, un ruteador envía un mensaje de solicitud a otro, el cual puede aceptarlo o rechazarlo. El protocolo no direcciona la manera en como un ruteador reconoce una dirección o incluso la existencia de otro ruteador, tampoco como decide que necesita intercambiar información de ruteo con ruteador en particular. Estos procesos tienen que ver con la configuración o la intervención activa de un administrador de red.

Para realizar la adquisición de vecino, un ruteador envía un mensaje abierto a otro. Si el ruteador de destino acepta la solicitud, envía de regreso un mensaje de "keepalive" en respuesta.

Una vez que la relación entre vecinos es establecida, el procedimiento de accesibilidad de vecino se utiliza para mantener la relación. Cada parte necesita asegurar a la otra que todavía existe y todavía esta conectado en al relación de

vecinos. Para este propósito, los dos ruteadores periódicamente generan mensajes de "keepalive" uno a otro.

El procedimiento final especificado por BGP es la accesibilidad de red. Cada ruteador mantiene una base de datos de las subredes que pueden alcanzarse y la ruta preferida para alcanzar cada subred. En el momento que se realiza un cambio a la base de datos, el ruteador genera un mensaje de actualización que es difundido a todos los otros ruteadores que tienen implementado BGP. Debido al envío de esta información de actualización los ruteadores BGP pueden mantener la información de ruteo.

La figura 4.7 ilustra los formatos de todos los mensajes BGP y la tabla 4.6 define los campos. Cada mensaje comienza con un encabezado conteniendo tres campos, como lo indica la porción sombreada de cada mensaje en la figura. Para tomar un vecino, un ruteador primero abre una conexión TCP al ruteador vecino de su interés. Entonces envía un mensaje de apertura. Este mensaje identifica el sistema autónomo al cual pertenece el emisor y proporciona la dirección IP del ruteador. También incluye el parámetro "tiempo de espera", el cual indica el número de segundos que el emisor propone para el valor del tiempo de espera. Si el receptor esta preparado para establecer una relación de vecino calcula un valor de tiempo de espera que es el mínimo de su tiempo de espera y el "tiempo de espera" en el mensaje de apertura. Este valor calculado es el máximo número de segundos que pueden transcurrir entre la recepción de keepalives sucesivos y los mensajes de actualización del emisor.

El mensaje de keepalive consiste simplemente del encabezado. Cada ruteador genera este mensaje a cada uno de sus colegas a menudo lo suficiente como para prevenir la expiración del tiempo de espera.

CAMPO	DESCRIPCIÓN
	ENCABEZADO
Marker	Reservado para autentificación. El emisor puede insertar un valor en este campo que podría ser usado como parte de un mecanismo que habilite el recibo para verificar la identidad del emisor.

Length	Largo del mensaje en octetos.
Type	Tipo del mensaje: Open, Update, Notification, Keepalive.

OPEN MESSAGE	
Version	Versión del protocolo BGP.
My AS	Identificador del sistema autónomo del emisor.
Hold Time	Valor propuesto del Hold Timer.
BGP Identifier	Dirección IP identificando al emisor BGP.
Length Optional Parameter	Largo en octetos del campo optional parameters.
Optional Parameters	Lista de los parámetros opcionales.

UPDATE MESSAGE	
Unfeasible Routes Length	Largo del campo de rutas disponibles en octetos.
Withdrawn routes	Lista de los prefijos de direcciones IP siendo retiradas de servicio.
Total Path Attribute Length	Largo en octetos del campo de los atributos de ruta.
Path Attributes	Secuencia de los atributos de ruta.
Capa de red	Lista de los prefijos de direcciones IP.

	NOTIFICATION
Error code	Indica el tipo de notificación.
Error subcode	Proporciona información adicional acerca de los reportes de error.
Data	Contiene información de diagnostico relacionada a la notificación.

Figura 4.6 Descripción de campos BGP.

El mensaje de actualización comunica dos tipos de información:

- Información acerca de una sola ruta a través de internet. Esta información esta disponible para agregarse a la base de datos de cualquier ruteador que la reciba.
- Una lista de rutas previamente anunciada por este ruteador que están siendo actualizadas.

Un mensaje de actualización puede contener uno o ambos tipos de información. Consideremos primero el primer tipo de información. Información acerca de una ruta única a través de la red involucra tres campos: el campo de información de accesibilidad de la capa de red (NLRI), el campo de atributos de ruta total y el campo de atributos de ruta. El campo NLRI consiste de una lista de identificadores de subredes que pueden ser alcanzadas por esta ruta. Cada subred es identificada por su dirección IP, que es una porción de una dirección IP completa. Recordemos que una dirección IP es una cantidad de 32-bits de la forma (red, terminal). La otra parte o porción del prefijo de esta cantidad identifica una red en particular.

El campo de atributos de ruta contiene una lista de atributos que aplican a esta ruta en particular. Los siguientes son los atributos definidos:

- **Origin:** indica tanto si esta información fue generada por un protocolo de ruteo interior (OSPF) o un protocolo de ruteo exterior (BGP).
- **AS Path**: una lista de los SA atravesados por esta ruta.

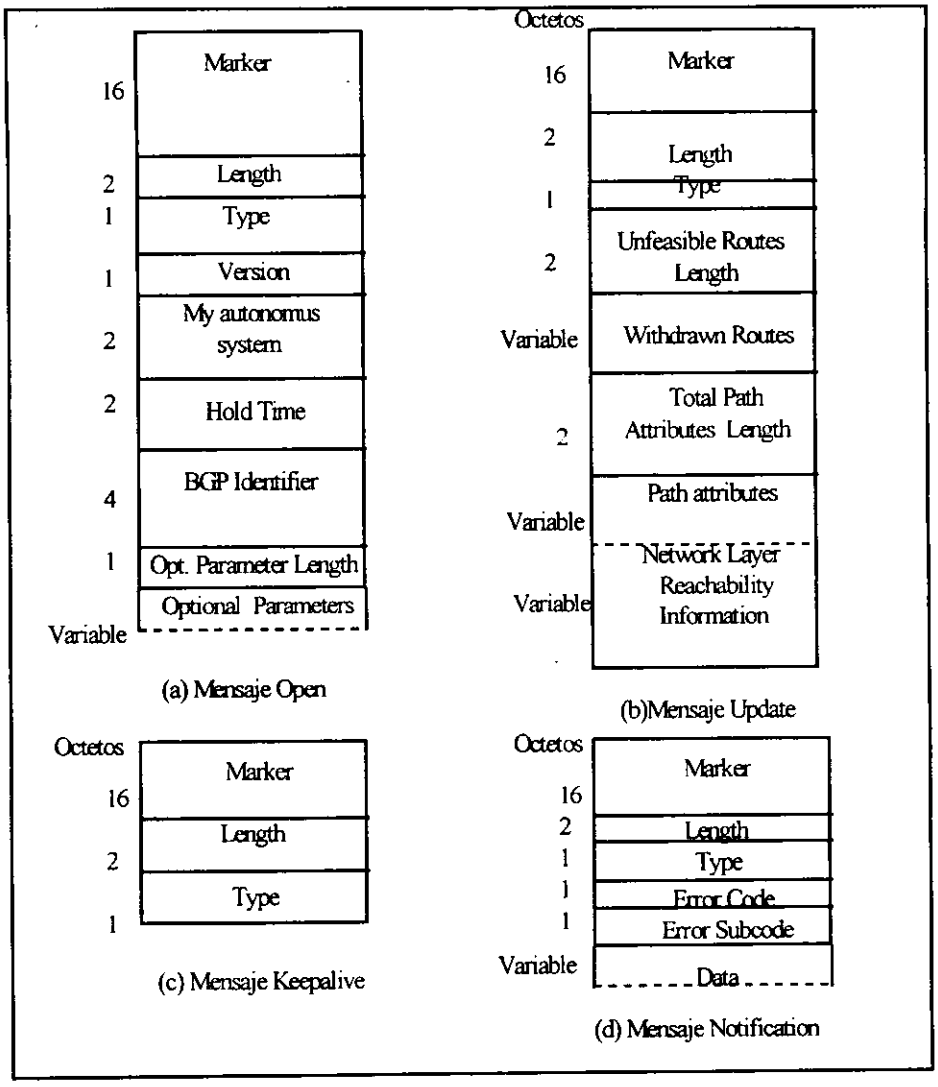


Fig.4.7 Formatos de mensajes BGP.

- **Next Hop:** la dirección IP del ruteador extremo que debe ser usado como el siguiente salto para los destinos listados en el campo NLRI.

- **Multi Exit Disc:** usados para comunicar alguna información acerca de las rutas internas en un AS.

- **Local Pref:** usado por un ruteador para informar otras rutas dentro del mismo sistema autónomo y su grado de preferencia para una ruta en particular. No tiene significado para otras rutas en otros AS´s.

- **Atomic Aggregate, Aggregator:** implementa el concepto de agregación de ruta. En esencia, una internet y su espacio correspondiente de dirección puede ser organizado jerárquicamente, o como árbol. En este caso, las direcciones de subred son estructuradas en dos o más partes. Todas las subredes de un subárbol dado comparten una dirección común parcial. Usando esta dirección común parcial, la cantidad de información que debe ser comunicada en NLRI puede ser reducida significativamente.

El atributo AS Path actualmente sirve a dos propósitos. Debido a que lista los AS´s que un datagrama debe atravesar si sigue esa ruta, esta información AS Path permite al ruteador realizar una política de ruteo. Esto es, un ruteador puede decidir evitar una ruta en particular, para evitar pasar por un AS en particular. Por ejemplo, información que es confidencial puede ser limitada a ciertas clases de AS´s. O un ruteador puede tener información acerca del desempeño o la calidad de la porción de internet que esta incluida en un AS que conduce al ruteador a evitar ese AS. Ejemplos de rendimiento o medidas de calidad incluyen, velocidad del enlace, capacidad, tendencia a congestionarse, y calidad general de operación. Otro criterio que puede ser usado es minimizar el número de AS´s transitados.

Podríamos sorprendernos acerca del propósito del atributo Next Hop. El ruteador solicitante necesariamente querrá saber que redes son accesibles vía el ruteador que responde, pero ¿porque proporcionar información acerca de otros ruteadores? Esto es mejor explicado si nos referimos a la figura 4.2. En este ejemplo, el ruteador R1 en el sistema autónomo 1 y el ruteador 5 en el sistema autónomo implementan BGP y adquieren una relación de vecinos. R1 genera un mensaje de actualización a R5 indicando cuales redes pueden ser alcanzadas y las distancias involucradas (saltos de red). R1 también proporciona la misma información en la parte de R2. Esto es, R1 le indica a R5 que redes son alcanzables vía R2. En este ejemplo, R2 no implementa BGP. Típicamente, la mayoría de los ruteadores en un sistema autónomo no implementará BGP. Solamente a unos cuantos ruteadores se les asignara la responsabilidad para comunicarse con los ruteadores en otros sistemas autónomos. Un punto final: R1

esta en posesión de la información necesaria acerca de R2, debido a que R1 a R2 comparten un protocolo de ruteo interior (IRP).

El segundo tipo de información de actualización es el de anunciar uno o más nuevos ruteadores. En cada caso la ruta es identificada por la dirección IP de la red de destino. Finalmente, el mensaje de notificación es enviado cuando una condición de error se detecta.

La esencia de BGP es el intercambio de información de ruteo entre ruteadores participantes en múltiples sistemas autónomos. Este procedimiento puede ser bastante complejo.

Consideremos un ruteador R1 en el sistema autónomo A (AS1 Figura 4.2). Para empezar un ruteador que implementa BGP también implementara un protocolo interno de ruteo como OSPF. Usando OSPF, R1 puede intercambiar información de ruteo con otros ruteadores dentro de AS1 y construir una imagen de la topología de la subred y los ruteadores AS1 y construye una tabla de ruteo. Enseguida, R1 puede generar un mensaje de actualización a R5 en AS2. El mensaje de actualización puede incluir lo siguiente:

- **AS Path:** la identidad de AS1.
- **Next Hop:** la dirección IP de R1.
- **NLRI:** una lista de todas las subredes en AS1.

Este mensaje informa a R5 que todas las subredes listadas en NLRI son alcanzables vía R1 y que el único sistema autónomo atravesado es AS1.

Supongamos ahora que R5 también tiene una relación de vecino con otro ruteador en otro sistema autónomo, digamos R9 en AS3. R5 transmitirá la información recién recibida de R1 a R9 en un nuevo mensaje de actualización. Este mensaje incluye lo siguiente:

- **AS Path:** la lista de identificadores (AS2, AS1).
- **Next Hop:** la dirección IP de R5.
- **NLRI:** una lista de todas las subredes en AS1.

Este mensaje informa a R9 que todas las subredes listadas en NLRI son alcanzables vía R5 y que los sistemas autónomos atravesados son AS2 y AS1. R9 debe decidir si esta ruta es la mejor ruta a la subred listada. Puede tener reconocimiento de una ruta alterna a alguna o todas estas subredes que prefiere por razones de desempeño o algunas otras política de métrica. Si R9 decide que la

ruta proporcionada en el mensaje de actualización de R5 es preferible, R9 incorpora esa información de ruteo dentro de su base de datos de ruteo y envía esta nueva información a otros vecinos. Este nuevo mensaje incluirá un campo AS Path de (AS1, AS2, AS3).

De esta manera, la información de actualización de ruteo es propagada a través de la red en general, consistiendo de una red interconectada de sistemas autónomos. El campo AS Path es usado para asegurar que dicho mensaje no circulara indefinidamente: Si un mensaje de actualización es recibido por un ruteador en un sistema autónomo que esta incluido en el campo AS Path, el ruteador no compartirá la información actualización con otros ruteadores, previniendo el que el mensaje entre en un loop.

La discusión anterior deja fuera muchos detalles que se resumen brevemente. Los ruteadores dentro del mismo AS, llamados vecinos internos, puede intercambiar información BGP. En este caso el ruteador emisor no agrega el identificador del AS común al campo AS Path. Cuando el ruteador ha seleccionado una ruta preferida a un destino externo, transmite esta ruta a todos sus vecinos internos. Cada uno de estos ruteadores decide entonces si la nueva ruta es preferida, en tal caso se agrega la nueva ruta a la base de datos y un nuevo mensaje de actualización es emitido.

Cuando existen múltiples puntos de entrada hacia un AS que esta disponible a un ruteador de frontera en otro AS, el atributo Multi Exit Disc puede ser usado para escoger entre ellos. Este atributo contiene un número que refleja algunas métricas internas para alcanzar destinos dentro de un AS. Por ejemplo, suponga en la figura 4.8 que ambos R1 y R2 implementan BGP y ambos tienen una relación de vecinos con R5. Cada uno proporciona un mensaje de actualización a R5 para la subred 1.3 que incluye una ruta métrica usada internamente a AS1, tal como una métrica de ruteo asociada con el protocolo de ruteo interno OSPF. R5 puede entonces usar estas dos métricas como la base de escoger entre 2 rutas.

4.1.3 Routing Information Protocol (RIP)

Uno de los IGP (Interior Gateway Protocol) más ampliamente utilizado es el Protocolo de Información de Ruteo (RIP, Routing Information Protocol), también conocido con el nombre de un programa que lo implementa, routed. Este se apoya

en la difusión de la red física para realizar el intercambio de ruteo rápidamente. No fue diseñado para usarse en redes de área amplia (aunque ahora sí se hace).

Al margen de mejoras menores con respecto a sus predecesores, la popularidad de RIP, como un IGP, no reside en sus méritos técnicos. Por el contrario, es el resultado de que Berkeley distribuyó el software routed junto con su popular sistema 4BSD de UNIX. Así muchas localidades TCP/IP adoptaron e instalaron routed y comenzaron a utilizar RIP sin considerar sus méritos o limitaciones técnicas. Una vez instalado y corriendo, se convirtió en la base del ruteo local y varios grupos de investigadores lo adoptaron para redes amplias.

El protocolo subyacente RIP es consecuencia directa de la implantación del ruteo de vector-distancia para redes locales. En principio, divide las máquinas participantes en activas y pasivas (silenciosas). Los ruteadores activos anuncian sus rutas a los otros; las máquinas pasivas listan y actualizan sus rutas con base en estos anuncios, pero no anuncian. Sólo un ruteador puede correr RIP de modo activo; un anfitrión debe utilizar el modo pasivo.

Un ruteador que corre RIP de modo activo difunde un mensaje cada 30 segundos. El mensaje contiene información tomada de la base de datos de ruteo actualizada. Cada mensaje consiste de pares, donde cada par contiene una dirección de red IP y un entero que representa la distancia hacia un destino. En la métrica RIP, un ruteador define un salto desde la red conectada directamente, dos saltos desde la red que esta al alcance a través de otro ruteador, y así sucesivamente. De esta manera, el número de saltos (number of hops) o el contador de saltos (hop count) a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de ruteadores que un datagrama encontrará a lo largo de la trayectoria. Debe ser obvio que utilizar el conteo de saltos para calcular la trayectoria más corta no siempre produce resultados óptimos. Por ejemplo, una trayectoria con un conteo de saltos igual a 3 que cruza tres redes Ethernet puede ser notablemente más rápido que una trayectoria con un contador de saltos igual 2 que atraviesa dos líneas seriales lentas. Para compensar las diferencias tecnológicas, muchas implantaciones RIP permiten que los administradores configuren artificialmente los contadores de saltos con valores altos cuando deban anunciar conexiones hacia redes lentas.

Tanto los participantes RIP activos como los pasivos "escuchan" todos los mensajes difundidos y actualizan sus tablas de acuerdo al algoritmo vector-distancia descrito anteriormente. Por ejemplo, en la red de redes de la figura 4.8,

el ruteador R1 difundirá un mensaje en la red 2 que contiene el par (1, 1), dando a entender que puede alcanzar la red 1 al costo 1. Los ruteadores R2 y R5 recibirán la difusión e instalarán una ruta hacia la red 1 a través de R1 (al costo 2). Después, los ruteadores R2 y R5 incluirán el par (1, 2) cuando difundan sus mensajes RIP en la red 3. Finalmente, todos los ruteadores y anfitriones instalarán una ruta hacia la red 1.

RIP especifica unas cuantas reglas para mejorar el desempeño y la confiabilidad. Por ejemplo, una vez que un ruteador aprende una ruta desde otro ruteador, debe conservar esta ruta hasta que aprenda otra mejor. En nuestro ejemplo, si los ruteadores R2 y R5 anuncian la red 1 al costo 2, los ruteadores R3 y R4 instalarán una ruta a través del que logre anunciarlo primero. Así pues, podemos resumir lo siguiente: Para prevenir que los ruteadores oscilen entre dos o más trayectorias de costos iguales, RIP especifica que se deben conservar las rutas existentes hasta que aparezca una ruta nueva con un costo estrictamente menor.

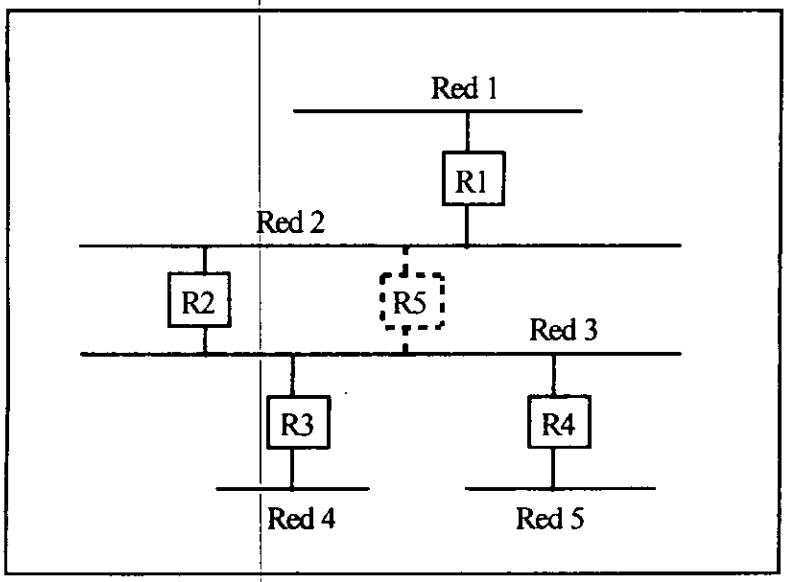


Figura 4.8 Red de redes con ruteadores.

¿Qué sucede si falla el primer ruteador que anuncia en la ruta (es decir, sí queda fuera de funcionamiento)? RIP especifica que todos los escuchas deben asociar un tiempo límite a las rutas que aprenden por medio de RIP. Cuando un ruteador instala una ruta en su tabla, inicia un temporizador para tal ruta. Este tiempo debe iniciarse cada vez que el ruteador recibe otro mensaje RIP anunciando la ruta. La ruta queda inválida si transcurren 180 segundos sin que el ruteador haya recibido un anuncio nuevamente.

RIP debe manejar tres tipos de errores ocasionados por los algoritmos subyacentes. En primer lugar, dado que el algoritmo no especifica detección de ciclos de ruteo, RIP debe asumir que los participantes son confiables o deberá tomar precauciones para prevenir los ciclos. En segundo lugar, para prevenir inestabilidades, RIP debe utilizar un valor bajo para la distancia máxima posible (RIP utiliza 16). Así, para una red de redes en la que es válido un contador de saltos de cerca de 16, los administradores deben dividir la red de redes en secciones o utilizar un protocolo alternativo. Tercero, el algoritmo vector-distancia empleado por RIP crea un problema de convergencia lenta (slow convergence) o conteo al infinito (count to infinity), problema en el cual aparecerán inconsistencias, debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red. Seleccionando un infinito pequeño (16) se ayuda a limitar la convergencia lenta, pero no se elimina.

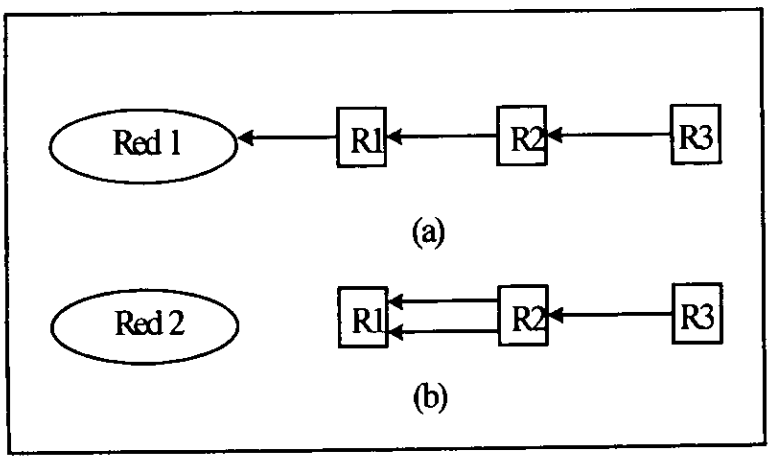


Figura 4.9 Comunicación de ruteadores con una red.

La inconsistencia en la tabla de ruteo no es exclusiva de RIP. Este es un problema fundamental que se presenta cuando cualquier protocolo vector-distancia en el que los mensajes de actualización transportan únicamente pares de redes de destino y distancias hacia estas redes. Para comprender el problema consideremos el conjunto de ruteadores mostrados en la figura 4.9. La figura describe rutas hacia la red 1 para la red de redes mostrada en al figura 4.8.

Los mensajes RIP pueden ser clasificados, a grandes rasgos, en dos tipos: mensajes de información de ruteo y mensajes utilizados para solicitar información. Ambos se valen del mismo formato, consistente en un encabezado fijo seguido por una lista opcional de pares de redes y distancias. La figura 4.10(b) muestra en formato de los mensajes:

Comando	Significado
1	Solicitud para información parcial
2	Respuesta con distancias de red de pares desde la tabla de ruteo del emisor
3	Activar el modo de trazado (obsoleto)
4	Desactivar el modo de trazado (obsoleto)
5	Reservado para uso interno de Sun Microsystems

Figura 4.10(a) Comandos RIP

En la figura 4.10(b), el comando COMMAND especifica una operación de acuerdo a la tabla que se encuentra en la parte superior de la figura. Un ruteador o anfitrión puede solicitar información de ruteo a otro para enviar un comando request. El ruteador responde a la solicitud mediante el comando response. Sin embargo, en la mayoría de los casos, los ruteadores difunden mensajes de respuestas no solicitados periódicamente. El campo VERSION contiene el número de la versión del protocolo (actualmente 1) y lo utiliza el receptor para verificar que interpretará el mensaje de manera correcta.

Los mensajes RIP no contienen un campo de longitud explícito. De hecho, RIP asume que los mecanismos de entrega subyacentes dirán al receptor la longitud de un mensaje entrante. En particular, cuando se utilizan con el TCP/IP, los mensajes RIP dependen del UDP para informar al receptor la longitud del mensaje. RIP opera el puerto 520 en UDP. Aun cuando una solicitud RIP puede

originar otro puerto UDP, el puerto de destino UDP para solicitudes es siempre 520, que es el puerto de origen desde el cual en principio RIP difunde los mensajes.

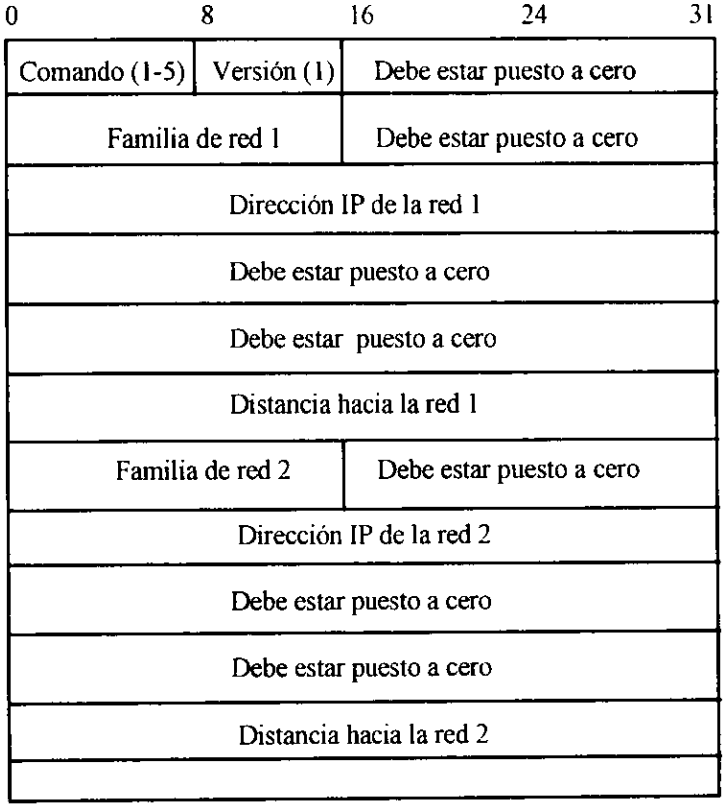


Figura 4.10(b) Formato de los mensajes RIP.

El uso de RIP como protocolo de ruteo interior limita el ruteo a una métrica basada en contadores de saltos. Casi siempre los contadores de saltos proporcionan sólo una medición general de la respuesta de red o de la capacidad que no produce rutas óptimas. Además, calcular rutas con base en el conteo mínimo de saltos tiene la severa desventaja de que hace el ruteo relativamente estática, dado que las rutas no pueden responder a los cambios en las cargas de la red.

4.1.4 Protocolo HELLO

El protocolo HELLO proporciona un ejemplo de un IGP que utiliza una métrica de ruteo basada en retardos en la red en lugar de contadores de saltos. A pesar de que ahora HELLO es obsoleto, es importante en la historia de Internet porque fue el IGP empleado entre los primeros ruteadores "fuzzball" de la columna vertebral NSF net. HELLO es importante para nosotros porque proporciona un ejemplo de un algoritmo vector-distancia que no utiliza contadores de saltos.

HELLO proporciona dos funciones: sincroniza los relojes entre un conjunto de máquinas y permite que cada máquina calcule las rutas de trayecto más corto hacia su destino. Así, los mensajes HELLO transportan información de sello de hora así como información de ruteo. La idea básica oculta o subyacente en HELLO es sencilla: cada máquina participante en el intercambio HELLO mantiene una tabla de sus mejores estimaciones de los relojes de las máquinas vecinas. Antes de transmitir un paquete, una máquina añade su sello de hora copiando el valor de reloj actual dentro del paquete. Cuando un paquete llega, el receptor calcula el retardo actual en el enlace. Para hacerlo, el receptor sustrae el sello de hora en el paquete entrante de su valor estimado para el reloj actual en el vecino. De manera periódica, las máquinas sondean a sus vecinos a fin de restablecer sus estimaciones para los relojes.

Los mensajes HELLO también permiten a las máquinas participantes calcular nuevas rutas. El algoritmo trabaja en forma parecida a RIP, pero utiliza retardos en lugar de contadores de salto. Cada máquina envía periódicamente a su vecino una tabla de los retardos estimados para todas las otras máquinas. Supongamos que la máquina A envía a la máquina B una tabla de ruteo que especifica destinos y retardos. B examina cada entrada de información en la tabla. Si los retardos actuales de B para alcanzar un destino dado, D son mayores que el retardo desde B hasta A, B cambia su ruta y envía el tráfico hacia D vía A. Esto es, B rutea el tráfico hacia A y toma la trayectoria de retraso más corto.

Como en cualquier algoritmo de ruteo, HELLO no puede cambiar rutas rápidamente o se volvería inestable. La inestabilidad en un algoritmo de ruteo produce un efecto de oscilación dos estados en el cual el tráfico conmuta "de ida y de regreso" entre rutas alternas. En el primer estado, la máquina encuentra una trayectoria ligeramente cargada y de manera abrupta conmuta el tráfico hacia ésta,

sólo para encontrar que comienza a estar completamente sobrecargada. En el segundo estado, la máquina conmuta el tráfico de regreso de la ruta sobrecargada, sólo para encontrar que la trayectoria comienza a sobrecargarse, y el ciclo continúa. Estas oscilaciones pueden presentarse. Para evitarlas, las implementaciones de HELLO seleccionan cambiar rutas sólo cuando la diferencia en el retardo es grande.

La figura 4.11 muestra el formato de mensaje HELLO. El protocolo es más complejo que el formato de mensaje indicado puesto que distingue las conexiones de redes locales de los saltos múltiples hacia afuera, los límites de tiempo caducan en entradas de información en las tablas de ruteo y utiliza identificadores locales para los anfitriones en lugar de direcciones IP completas.

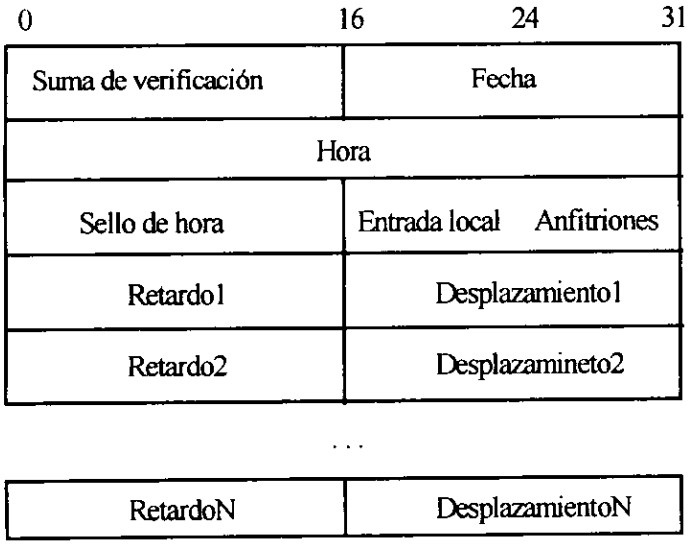


Figura 4.11 Formato del mensaje HELLO

4.1.5 Protocolo de SPF abierto (OSPF)

El algoritmo de propagación de rutas SPF escala mejor que los algoritmos vector-distancia. Un grupo de trabajo de la Fuerza de Tarea de Ingeniería de Internet ha diseñado un IGP que utiliza el algoritmo SPF. Llamado Open SPF (OSPF), el nuevo protocolo se propone varios objetivos.

La especificación está disponible en la información pública, lo que la hace un estándar abierto y que cualquiera puede implantar sin pagar licencias de uso. Los diseñadores esperan que muchos vendedores soporten OSPF y lo conviertan en un reemplazo popular para protocolos propietarios.

El OSPF incluye un ruteo de servicio de tipo. Los administradores pueden instalar múltiples rutas hacia un destino dado, uno para cada tipo de servicio (por ejemplo, retardo bajo o rendimiento alto). Cuando se rutea un datagrama, un ruteador que corre OSPF utiliza la dirección de destino y el campo de servicio de tipo en un encabezado IP para seleccionar una ruta. El OSPF está entre los primeros protocolos TCP/IP que ofrecen un ruteo de servicio de tipo. El OSPF proporciona balance de carga. Si un administrador especifica múltiples rutas hacia un destino dado con el mismo costo, el OSPF se encuentra entre los primeros IGP abiertos en ofrecer balance de carga; los protocolos como RIP calculan una sola ruta para cada destino.

Para permitir el crecimiento y hacer las redes de una localidad fáciles de manejar, el OSPF permite que una localidad dividida sus redes y ruteadores en subconjuntos llamados áreas. Cada área es autónoma; el conocimiento de la topología de un área se mantiene oculto para las otras áreas. Así, varios grupos dentro de una localidad dada pueden cooperar en el uso del OSPF para rutear, lo que permite que cada grupo conserve la capacidad de cambiar su topología de red interna de manera independiente.

El protocolo OSPF especifica que todos los intercambios entre ruteadores deben ser autentificados. El OSPF permite una variedad de esquemas de autenticación y también permite seleccionar un esquema para una área diferente al esquema de otra área. La idea detrás de la autenticación es garantizar que sólo ruteadores confiables difundan información de ruteo. Para entender por qué éste podría ser un problema considere que puede suceder cuando se usa RIP, el cual no tiene la capacidad de autenticación. Si una persona maliciosa utiliza una computadora personal para propagar mensajes RIP anunciando rutas de bajo costo, otros ruteadores y anfitriones que estén corriendo RIP cambiarán sus rutas y comenzarán a enviar datagramas hacia la computadora personal.

El OSPF soporta rutas específicas para anfitriones y rutas de subred, así como rutas específicas de red. Todos estos tipos pueden ser necesarios en una red de redes extensas.

Para adaptar redes de accesos múltiples como Ethernet, el OSPF amplia el algoritmo SPF. Describimos el algoritmo utilizando un grafo de punto a punto y diciendo que cada ruteador corre SPF difundiendo periódicamente mensajes de estado de enlace sobre cada vecino accesible. Si se tienen K ruteadores conectados a una red Ethernet, éstos difundirán K mensajes de accesibilidad. El OSPF minimiza la difusión permitiendo una topología de grafo complejo en el que cada nodo representa un ruteador o una red. Consecuentemente, el OSPF permite a todas las redes de accesos múltiples tener un ruteador designado (llamada compuerta designada, designated gateway, en el estándar) que envía mensajes de estado de enlace en nombre de todos los enlaces de la red a los ruteadores conectados a la red. El OSPF también se vale de capacidades de difusión de hardware, si existen, para entregar mensajes de estado de enlace. Para permitir una flexibilidad máxima, el OSPF permite que los administradores describan una topología de red virtual que haga abstracción de los detalles de conexiones físicas. Por ejemplo, un administrador puede configurar un enlace virtual entre dos ruteadores en el grafo de ruteo, aunque la conexión física entre los dos ruteadores requiera de comunicaciones a través de una red de tránsito.

El OSPF permite a los ruteadores intercambiar información de ruteo aprendida desde otras localidades (externas). Básicamente, uno o más ruteadores con conexiones hacia otras localidades reciben información sobre otras localidades y la incluyen cuando envían mensajes de actualización. El formato de mensaje distingue entre información adquirida de fuentes externas e información adquirida de ruteadores en el interior de la localidad, para evitar ambigüedad acerca de la fuente o de la confiabilidad de las rutas.

Cada mensaje OSPF comienza con un encabezado fijo de 24 octetos como se muestra en la figura 4.12.

El campo VERSION especifica la versión del protocolo actual. El campo TYPE (TIPO) identifica el tipo de mensajes según lo siguiente:

TYPE	**Significado**
1	Hello (se utiliza para prueba de accesibilidad)
2	Descripción de base de datos (topología)
3	Solicitud de estado de enlace
4	Actualización de estado de enlace
5	Acuso de recibo de estado de enlace

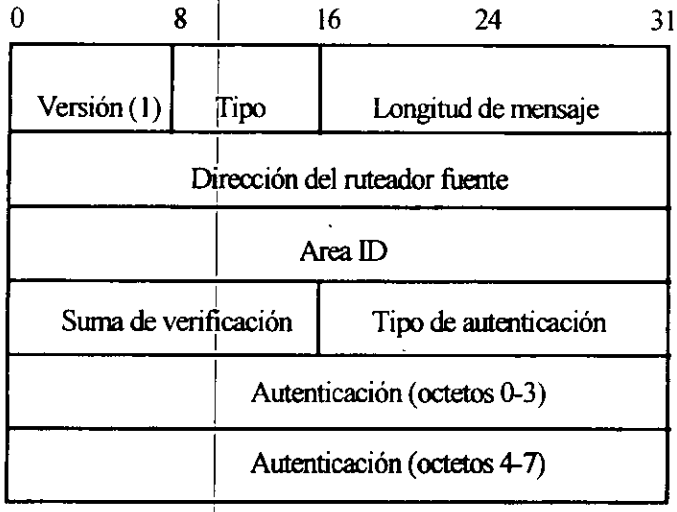


Figura 4.12 Encabezado OSPF.

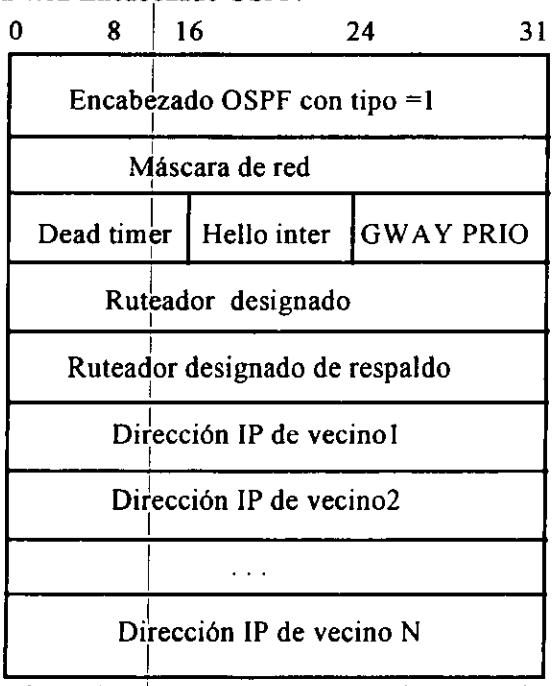


Figura 4.13 Formato de los mensajes HELLO.

El OSPF envía mensajes hello en cada enlace periódicamente para establecer y probar la accesibilidad del vecino. La figura 4.13 muestra el formato.

La Figura 4.14 muestra el formato del mensaje descripción de la base de datos OSPF.

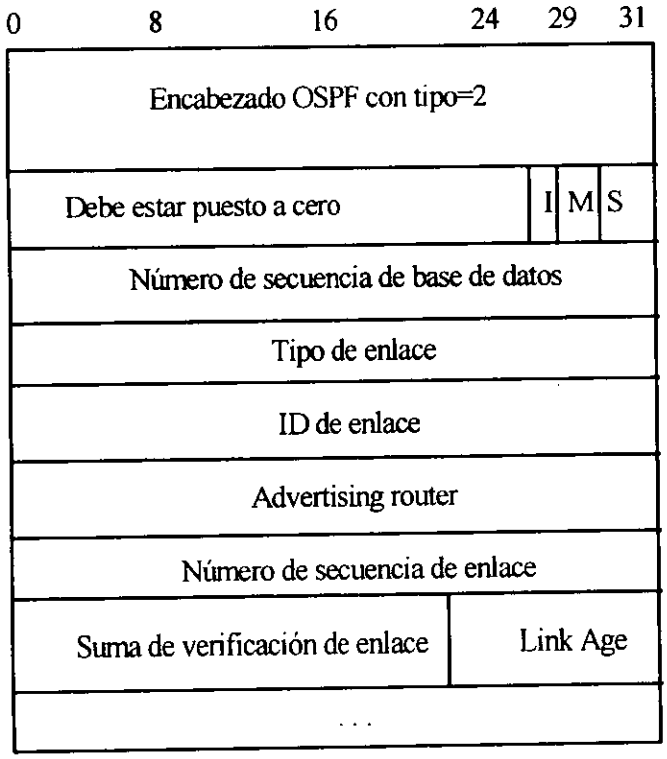


Figura 4.14 Mensaje OSPF de base de datos.

Luego de intercambiar mensajes de descripción de bases de datos con un vecino, un ruteador puede descubrir que algunas partes de su base de datos están fuera de fecha. Para solicitar que el vecino proporcione información actualizada, el ruteador envía un mensaje de solicitud de estado de enlace (Link Status Request). El mensaje lista enlaces específicos como se muestra en la figura 4.15. El vecino responde con la información más actualizada que tiene en relación a estos enlaces. Los tres campos que se muestran se repiten para cada enlace del

que se solicitó el status. Si la lista de solicitud es larga, puede ser necesario más de un mensaje de solicitud.

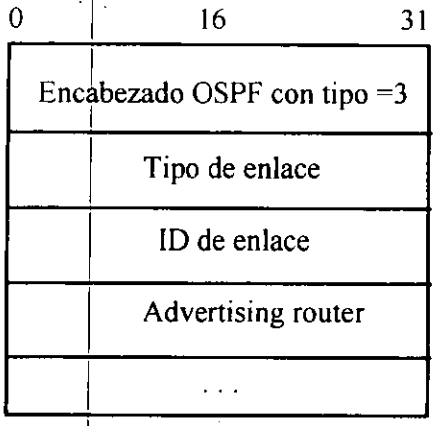


Figura 4.15 Mensaje de enlaces.

Los ruteadores difunden el estado de enlace con un mensaje de actualización de estado de enlace (link status update). Cada actualización consiste en una lista de anuncios, como se muestra en la Figura 4.16. Cada anuncio de estado de enlace tiene un formato de encabezado como se muestra en la figura 4.17. El valor utilizado en cada campo es el mismo que en el mensaje de descripción de base de datos.

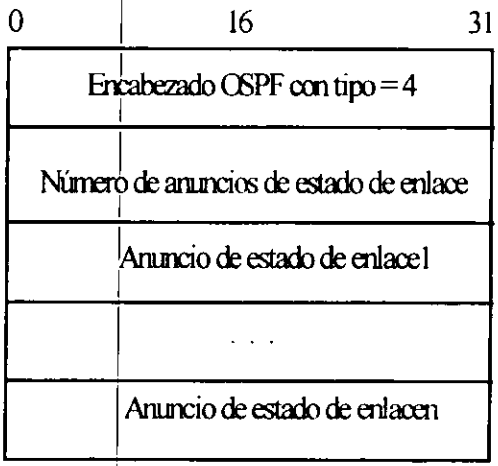


Figura 4.16 Lista de anuncios.

Los anfitriones pueden rutear con información parcial pues dependen de los ruteadores. Debe ser claro ahora que no todos los ruteadores tienen información completa. La mayor parte de los sistemas autónomos tienen un solo ruteador que forma un puente al conectar el sistema autónomo con otros

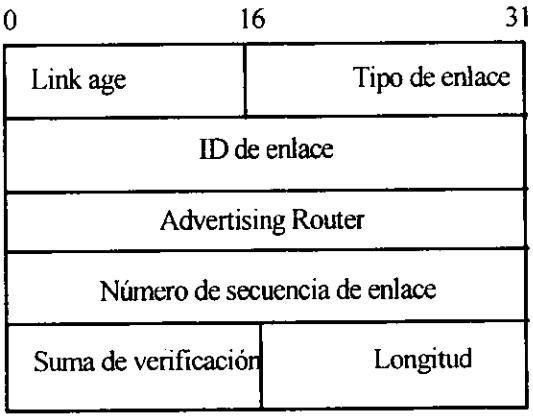


Figura 4.17 Anuncio de estado de enlace.

Sistemas autónomos. Si la localidad está conectada con Internet, el último ruteador debe tener una conexión que se dirija desde la localidad hacia una columna vertebral de una red nacional. Los ruteadores dentro del sistema autónomo tienen conocimiento sobre los destinos dentro de este sistema autónomo, pero éstos rutearán todo el tráfico restante hacia el puente.

Hacer el ruteo con información parcial comienza a ser obvio si examinamos la tabla de ruteo de un ruteador. Los ruteadores en un sistema núcleo tienen un conjunto completo de rutas hacia todos los destinos posibles; éstos no utilizan el ruteo por omisión. De hecho, si una dirección de red de destino no aparece en las tablas del núcleo, sólo existen dos posibilidades: la dirección no es una dirección IP de destino válida o la dirección es válida pero actualmente inaccesible (por ejemplo si el único ruteador que conducía hacia esa dirección ha fallado). Los ruteadores no-núcleo usualmente no tienen un conjunto completo de rutas; éstos dependen de una ruta por omisión para manejar direcciones de redes que no entienden.

Utilizar rutas por omisión para la mayor parte de los ruteadores no-núcleo tiene dos consecuencias. Primero, significa que los errores de ruteo locales podrían no detectarse. Por ejemplo, si una máquina en un sistema autónomo rutea incorrectamente un paquete hacia un sistema autónomo externo en lugar de hacerlo hacia un ruteador local, el sistema externo lo ruteará de regreso (posiblemente enviando un mensaje de redireccionamiento ICMP hacia la fuente original). Así, la conectividad podría parecer que se preserva incluso si el ruteo es incorrecto. El problema podría no ser severo para sistemas autónomos pequeños que tienen redes de área local de alta velocidad, pero en una red de área amplia con líneas de velocidad relativamente bajas, las rutas incorrectas pueden ser desastrosas. En segundo lugar, por el lado positivo, tener rutas por omisión significa que el mensaje de actualización de ruteo IGP será mucho más pequeño que las actualizaciones de ruteo utilizadas en un sistema núcleo.

4.3 Conmutación

Las redes locales actuales (LAN's) se están saturando de tráfico y han sido sobrepasadas en su capacidad. Además de un incremento siempre creciente de usuarios, muchos otros factores se están combinando para saturar las capacidades de las LAN's tradicionales:

- **CPU's más rápidos.** En la mitad de lo 80's, la workstation más común era una PC. En este momento, la mayoría de las PC pueden ejecutar 1 millón de instrucciones por segundo (MIPS). Actualmente, workstations con poder de procesar de 50 a 75 MIPS son muy comunes, por lo que las velocidades I/O se han incrementado también. Dos workstations modernas en la misma LAN pueden saturarla fácilmente.

- **Sistemas operativos más rápidos.** Hasta recientemente, el diseño de sistemas operativos ha mejorado el acceso a red. De los tres sistemas operativos más comunes (DOS/Windows, sistema operativo UNIX, el OS MAC), solo el sistema operativo UNIX puede ser multifunciones. El multifuncionamiento permite a los usuarios iniciar transacciones simultaneas en la red. Con la llegada de Windows 95, que refleja un rediseño de DOS/Windows que incluye multifunciones, los usuarios estarán en posibilidad de incrementar sus demandas para la red.

- **Red de aplicaciones intensivas.** Uso de aplicaciones cliente servidor, tales como Network File System (NFS), LAN Manager, NetWare, y World Wide

Web se están incrementando ampliamente. Las aplicaciones cliente-servidor permite centralizar información a los administradores, siendo además muy fácil de mantener y proteger. Las aplicaciones de cliente servidor liberan a los usuarios del pesado trabajo de mantener la información y el costo de proporcionar suficiente disco duro para almacenarlos. Dando el costo-beneficio de aplicaciones cliente-servidor, tales aplicaciones son parece que se volverán aún más ampliamente usadas.

La "conmutación" LAN es una tecnología que alivia la congestión en redes Ethernet, Token Ring, y FDDI al reducir el tráfico e incrementar el ancho de banda. Tales switches, conocidos como LAN switches, son designados para trabajar con la infraestructura de cable existente de tal forma que puedan ser instalados con mínima interrupción de las redes existentes. A menudo, ellos reemplazan hubs compartidos.

El término "Switching" fue originalmente usado para describir tecnologías tales como Link Access Procedure, Balanced (LAPB), Frame Relay, Switched Multimegabit Data Service (SMDS), y X.25. Hoy el conmutación se refiere a una tecnología que es similar a un puente en muchas maneras. Un LAN switch es un dispositivo que retransmite paquetes entre diferentes usuarios basados en algún tipo de tabla de guía. La función de "switching" es por lo tanto análoga a reenviar paquetes (forwarding packets). La tabla de conmutación puede ser creada en diferentes maneras. El método más común es crear una lista de direcciones capa MAC asociada con un puerto en particular a través de un filtro inteligente que monitoreo el tráfico de la red y aprende que puertos están asociados con que usuarios en la red.

En efecto, un LAN switch es un controlador de tráfico que determina que paquetes tienen permitido pasar entre diferentes usuarios en puertos diferentes. Un LAN Switch puede proporcionar un servicio de no-bloqueo, esto quiere decir, que el tráfico puede pasar entre diferentes pares de sitios fuente/destino sin impactar el tráfico de otros usuarios. De una manera muy similar como un PBX que permite múltiples llamadas ocurriendo simultáneamente, un LAN switch permite múltiples conexiones entre usuarios que ocurran simultáneamente.

Esta funcionalidad es muy similar a un bridge o un router, en que los tres dispositivos proporcionan los medios de filtrar y llevar paquetes LAN entre usuarios en la red. Adicionalmente, como un bridge, todos los puertos conectados a un LAN switch son considerados parte de la misma LAN fisica (similarmente a

lo que realiza un ruteador en que los puertos son asociados con diferentes LAN's lógicas). Los puertos LAN switch no ofrecen ninguna segmentación lógica de la red.

Mucha de la tecnología de LAN switching básica es derivada directamente de la tecnología de "bridging". Los bridges y los LAN switches operan en la capa de enlace OSI (nivel 2), que nos indica que utilizan una tabla de ruteo basada en direcciones de capa MAC. Aprovechando que las direcciones MAC Ethernet o Token Ring son únicas para cada tarjeta de interface de red Ethernet o Token Ring.

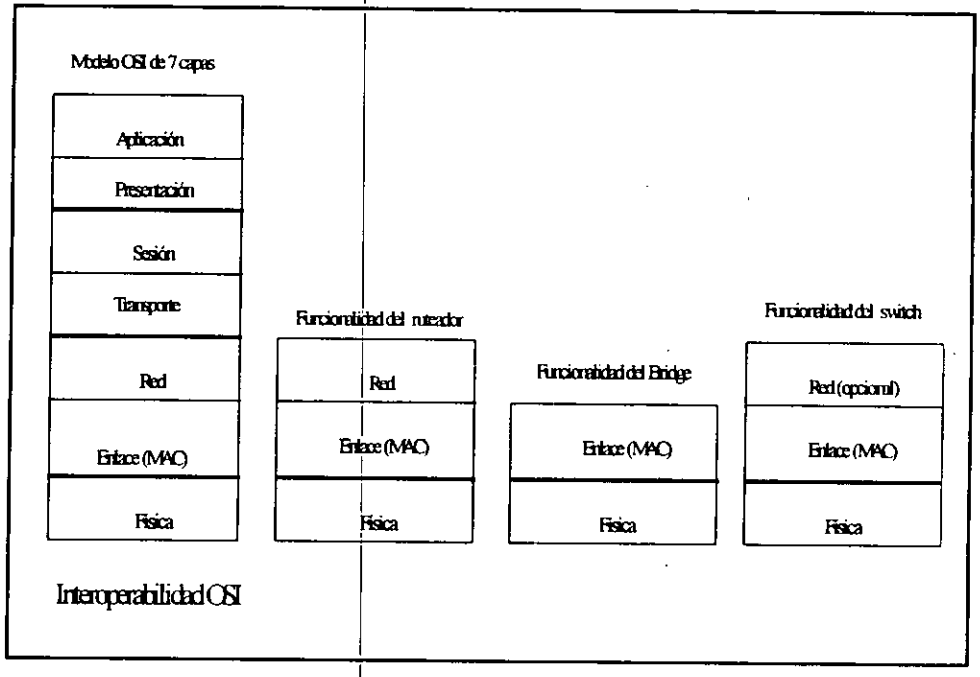


Figura 4.18 Switch comparado con otros dispositivos

No obstante, existen diferencias entre switches y bridges. La mayoría de los switches ignoran totalmente lo referente a conectividad remota, mientras muchos bridges ofrecen algún tipo de funcionalidad de red de área amplia (WAN). Adicionalmente, mientras la mayoría de los bridges están limitadas a un pequeño

número de puertos (usualmente menos de seis), la mayoría de LAN switches contienen cuando menos 8 puertos, hasta a docenas de puertos por switch (cada puerto equivalente a un puerto de bridge). En ese sentido, los LAN switches pueden verse como bridges LAN multipuerto. Y mientras los bridges y ruteadores son generalmente instalados tanto en el medio de la red (backbone) o en el extremo de la red (oficinas remotas), la mayoría de los LAN switches son empleados a nivel de grupo de trabajo, tanto entre workstations o grupos de trabajo LAN.

Un punto interesante en la evolución de los LAN bridges es que la mayoría de los productos bridge desarrollados a finales de los 80's surgieron eventualmente marginados por la tecnología de ruteo como resultado de un mercado masivamente tendiendo a los ruteadores como los dispositivos estándar para la interconexión de redes LAN. Antes de la aparición de los switches, los usuarios que deseaban comprar grandes bridges multipuerto fueron forzados a comprar ruteadores. De cualquier manera, conforme la tecnología de redes ha empezado a madurar, encontramos que los requerimientos de ruteadores en cada interconexión de redes no es tan alta como originalmente se pensó.

Un importante diferenciador entre productos bridge/router y LAN switches básicos, es que los LAN switches necesariamente no operan más allá de la capa MAC. No necesitan realizar filtrado de ruteo de capa 3, como tampoco necesitan utilizar protocolos de ruteo tradicionales tales como RIP o OSPF, debido a que no están intercambiando información de "vías de ruteo" entre dispositivos de la red. La mayoría de las implementaciones de LAN switches son complementarias a las de ruteadores, con ambos dispositivos trabajando como equipo. Es importante notar que muchos sistemas de switching futuros incorporarán funciones de ruteo de capa de red (capa 3), pero esto no es un requerimiento para los LAN switches.

Al mismo tiempo que los switches pueden verse como simples bridges multipuertos, estamos observando una alta tendencia a desarrollar funciones sofisticadas por software para los LAN switches. Por ejemplo, LAN's virtuales les permiten a los administradores de red crear múltiples redes lógicas (grupos broadcast, workgroups, subredes de capa 3 lógica) entre grupos de puertos LAN físicos, dependientes de la localización de los puertos LAN. Esto contrasta a la mayoría de las implementaciones con routers que requieren de una red lógica (TCP/IP subred) que este asociada con un puerto físico único en un ruteador.

Existen dos tipos diferentes de tecnologías de conmutación usadas en los LAN switches actuales: Cut-Through y Store and Forward. La tecnología cut-

through (también llamada "on the fly") es una tecnología extremadamente rápida que permite a un switch empezar el filtrado y proceso de reenvío (determinando por que puerto de salida el paquete debe ser enviado, y enviándolo a este) antes de que el paquete completo haya sido recibido por el LAN switch . Realiza esto al no realizar el proceso de almacenamiento usualmente asociado con la mayoría de tecnologías de bridge y router (referidas como Store and Forward). En la mayoría de los sistemas Cut-Through, esto se traduce en una inhabilidad de realizar procesamiento de valor agregado en los paquetes, incluyendo detección de errores. De cualquier modo , esto no es un tópico de importancia debido a que:

- La mayoría de los LAN switches no son usados para proporcionar funcionalidad de valor agregado.
- La mayoría de las LAN's proporcionan un ambiente muy limpio y libre de errores, donde checar errores en cada paquete no es usualmente requerido.

Como se mencionó anteriormente, la tecnología Store and Forward es una tecnología basada en almacenamiento, donde cada trama entrante a un switch es almacenada totalmente en un buffer. Ya en el buffer se realizan actividades como corrección de errores y filtrado en las tablas de ruteo. Teniendo el paquete completo puede facilitar la realización de procesamiento complicado de paquetes y utilizado por muchos administradores de red como llave para soportar funciones de ruteo (no obstante los méritos de ambas tecnologías están altamente debatidas entre los vendedores, usuarios y analistas). La tecnología store and forward es también clave para soportar adaptación a velocidades (10Mbps a 100Mbps) y conversiones de protocolo.

El medio más común es el tradicional Ethernet, que tiene como máximo ancho de banda de 10Mbps. Ethernet es una tecnología half-duplex. Cada host Ethernet checa la red para ver si existen datos viajando a través de los cables para evitar colisiones entre tramas. Un LAN switch Ethernet mejora el ancho de banda al separar los dominios de colisión y enrutar selectivamente el tráfico hacia los segmentos apropiados. La figura 4.19 muestra la topología de una red Ethernet típica en la cual un LAN switch ha sido instalado.

En la figura cada segmento Ethernet esta conectado a un puerto en un LAN switch. Si el servidor A en el puerto 1 necesita transmitir al cliente B en el puerto 2, el LAN switch envía tramas Ethernet del puerto 1 al 2, liberando a los puertos 3 y 4 de las tramas destinadas a B. Si el servidor C necesita enviar datos al cliente D al mismo tiempo que el servidor A envía datos al cliente B, puede hacer esto porque el LAN switch puede enviar tramas del puerto 3 al puerto 4 al mismo

tiempo que envía tramas del puerto 1 al puerto 2. Si el servidor A necesita enviar datos al cliente E, que también reside en el puerto 1, el LAN switch no necesita enviar ninguna trama.

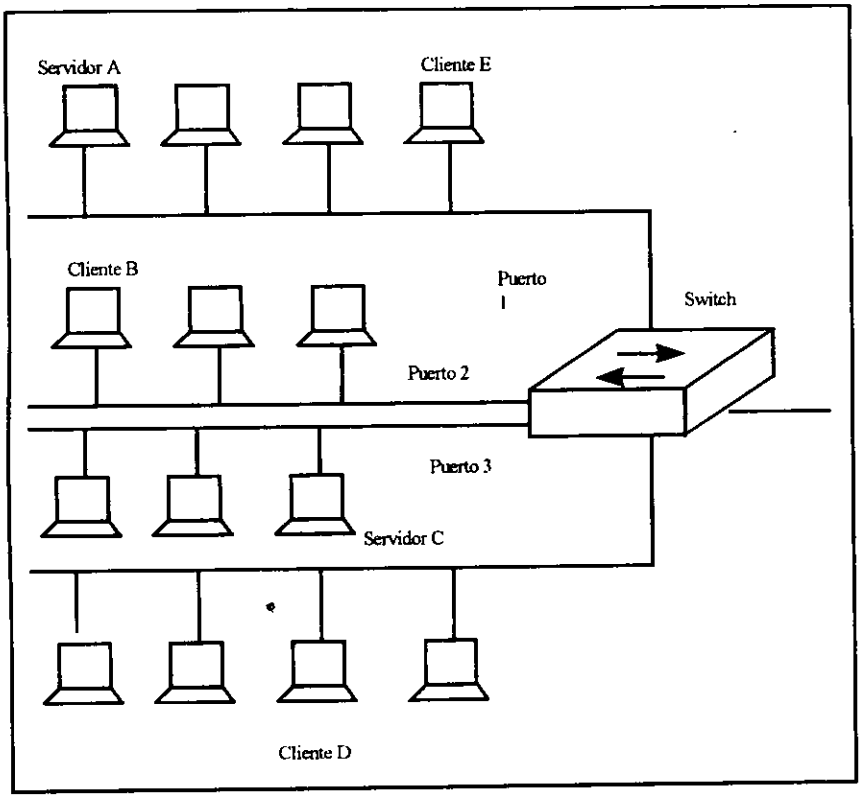


Figura 4.19 Ethernet con LAN switch instalado

El desempeño de mejora en las LAN's donde se instalan LAN switches debido a que los LAN switches crean dominios aislados de colisiones. Al repartir a los usuarios sobre muchos dominios de colisión, las colisiones son evitadas y se mejora el desempeño. La instalación de LAN switches asigna usualmente un usuario por puerto, el cual da a ese usuario un ancho de banda efectivo de 10 Mbps.

4.2.1 VLAN´s y Switches

Una virtual LAN (VLAN) es un grupo de hosts o dispositivos de red, tales como routers (corriendo puentes transparentes) y puentes, que forman un dominio único de "bridging". Los protocolos de "bridging" capa dos, tales como IEEE 802.10 y Inter-Switch Link (ISL) permiten que una VLAN exista a través de una variedad de equipos, tales como los LAN switches.

VLAN´s están formadas para agrupar usuarios relacionados sin importar que las conexiones físicas de sus hosts a la red. Los usuarios pueden estar dispersos a través de la red o incluso dispersos geográficamente. Una variedad de estrategias pueden ser usadas para agrupar usuarios. Por ejemplo, los usuarios pueden ser agrupados de acuerdo a su departamento o equipo funcional. En general, la meta es agrupar usuarios dentro de VLAN´s de manera que su tráfico se mantenga dentro de la VLAN.

Cuando se configuran VLAN´s, la red puede tomar ventaja de los siguientes beneficios:

- **Control de broadcast.** Como los switches físicamente aislan dominios de colisión para hosts unidos y solamente envían tráfico a un puerto particular, VLAN´s proporcionan dominios lógicos de colisión que confina el tráfico broadcast y multicast al dominio de "bridging".

- **Seguridad.** Si no se incluye un ruteador en una VLAN, ningún usuario fuera de la VLAN podrá comunicarse con los usuarios en el VLAN y viceversa. Este extremo nivel de seguridad puede ser altamente deseable para ciertos proyectos y aplicaciones.

- Desempeño. Se pueden asignar a usuarios que requieren alto desempeño de la red, dentro de sus propias VLAN´s. Podemos, por ejemplo, asignar a un ingeniero que esta probando una aplicación multicast y los servidores que utiliza este ingeniero a una sola VLAN. El ingeniero experimenta entonces un desempeño mejorado de la red al disponer una LAN dedicada, y el resto del grupo de ingeniería experimenta un desempeño mejorado de la red debido a que el tráfico generado por la aplicación intensiva de red es otra VLAN aislada.

- **Administración de la red.** El software en el switch nos permite asignar usuarios a VLAN's, y posteriormente reasignarlos a otra VLAN. Cablear de nuevo para cambiar la conectividad no es necesario en el ambiente conmutado LAN debido a que las herramientas de administración de red nos permiten reconfigurar la LAN lógicamente en segundos.

En la figura 4.20 una Ethernet 10 Mbps. conecta los hosts en cada piso a LAN switches. Una Ethernet 100Mbps conecta los switches A,B,C y D al switch E. Los switches en la figura se comunican unos a otros usando ISL, que es un protocolo que mantiene la información VLAN conforme el tráfico fluye entre los switches. Con ISL, una trama Ethernet es encapsulada con un "header" de 30 bytes que contiene un ID VLAN de 2 bytes. La figura muestra que la VLAN 20 consiste del puerto 4 en el slot 2 en el switch A y puertos 1 y 3 en el slot 4 en el switch B. Las tramas intercambiadas entre los puertos ¼ y ¾ que no es destinado para los puertos ¼ y ¾ es encapsulada en un "header" ISL que incluye un identificador VLAN 20 y es enviado al switch E. El switch E examina el encabezado ISL y determina que la trama es destinada para la VLAN 20 y envía la trama hacia afuera en el puerto 2/2 al switch A. El switch A examina el "header" ISL para determinar la VLAN hacia la cual la trama esta destinada, remueve el encabezado, y lo conmuta a todos los puertos en VLAN 20 (si la trama es broadcast o multicast) o al puerto 2/4 si la trama es unicast.

Existe un malentendido común respecto a que el modo de transferencia asíncrona (ATM) especifica switching, cuando de hecho ATM no es una tecnología de switching sino una tecnología de formato de información. Esto quiere decir, que las especificaciones que están siendo desarrolladas por los cuerpos de estandarización y el foro ATM, se concentran en como es manipulada y formateada la información dentro de una red. No existe nada en los estándares que determine como construir o diseñar un switch. Lo que es importante para un switch es su habilidad para proporcionar una interface consistente y un arreglo de servicios de transmisión para datos recibidos.

En el mercado de LAN switching, encontramos que la parte interna de un switch es menos importante que la estandarización de las interfaces hacia afuera de la red. Por lo que no existe requerimiento de que un LAN switch use una "switching fabric" ATM como sistema de conmutación. Para la mayoría de los ambientes LAN, un sistema de conmutación LAN que conmuta tramas LAN, más que celdas ATM, es el mecanismo apropiado, proporcionando no solo alto

desempeño sino evitando el requerimiento de convertir las tramas LAN en celdas ATM para conmutarlas.

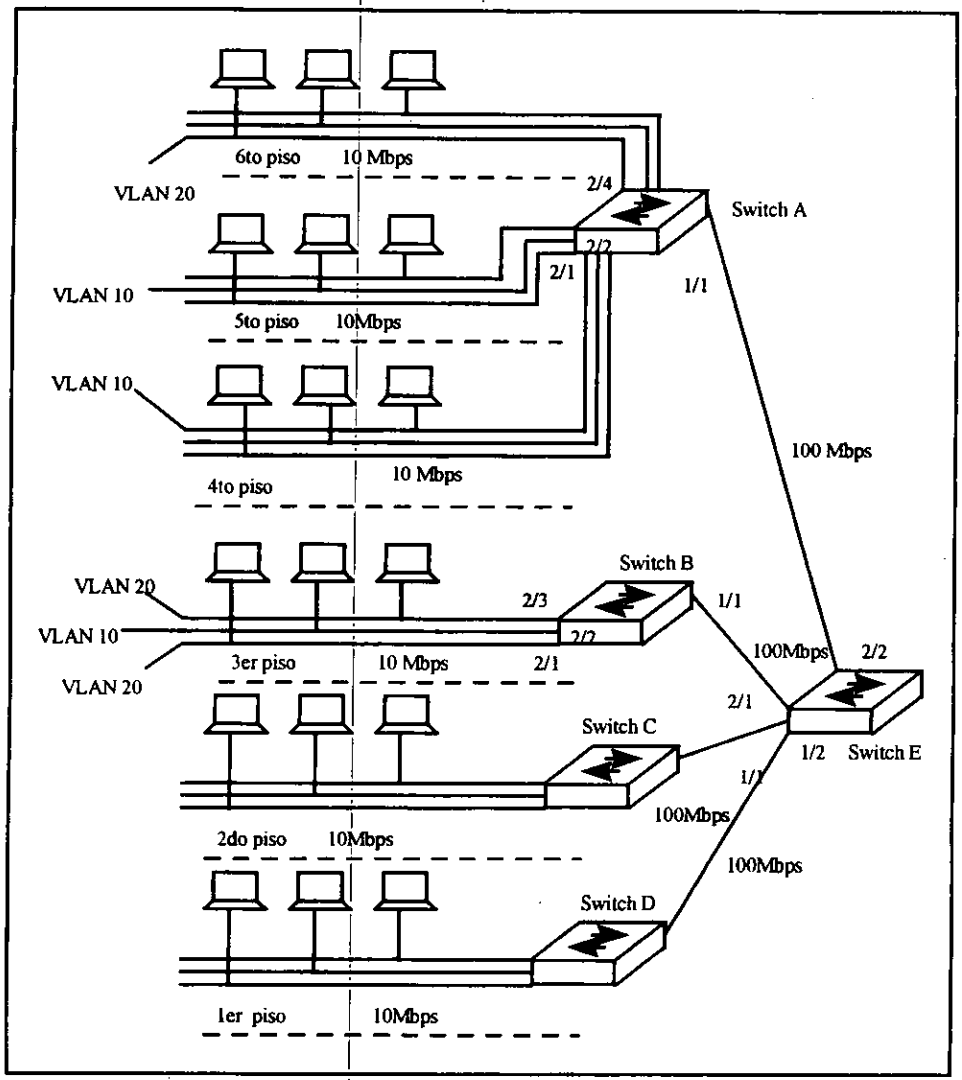


Figura 4.20 Ethernet de baja velocidad interconectada por LAN switches a una LAN de alta velocidad.

En una gran red distribuida, el uso de ATM como mecanismo de conmutación puede ser justificado a través de eficiencias que pueden ser ganadas por un diseño basado en hardware y orientado a celdas. ATM puede también ofrecer ventajas donde la mezcla de medios tecnológicos pueden ser soportados (redes con gran capacidad de datos y voz). El escenario más probable para el desarrollo de ATM LAN que involucre un campus o una red backbone que este basada en ATM con grupos de trabajo LAN basados en Ethernet, Token Ring o FDDI. Proporcionando adaptación de tramas LAN a celdas podría ser requerido para tráfico a través del backbone. En esta situación, una arquitectura universal de conmutación basada en ATM puede agregar valor.

Como sea, para el mercado de LAN switches actuales. El requerimiento para ATM de LAN switches es como una interface.

4.2.2 Clases de LAN switches

Los LAN switches pueden ser divididos en dos tipos separados, los que son designados para conmutar tráfico entre múltiples LAN's compartidas (Ethernet tradicional) y los que son diseñados para conmutar tráfico entre usuarios individuales. Cuando tenemos a un solo usuario conectado a un puerto LAN switch, ese usuario tiene control total del ancho de banda para el segmento entero LAN. Este es el último resultado de la segmentación; una LAN es segmentada hasta el punto donde existe un solo usuario por LAN.

Los actuales LAN switches, en su mayoría pueden soportar tanto conmutación por segmentos o conmutación de LAN privada. La diferencia entre los LAN switches de segmentación y los privados es el número de direcciones MAC fuente que pueden ser filtrados por un solo puerto. Mientras los switches de segmentación pueden a menudo filtrar direcciones MAC de miles de dispositivos fuentes , los LAN switches privados generalmente solo soportan una sola dirección MAC por puerto. En ambos casos, un ilimitado número de direcciones fuera de frontera son soportadas (los switches de segmentación permiten mucho-a-mucho, mientras que los switches LAN privados permiten transmisión uno-a-muchos), Figura 4.21.

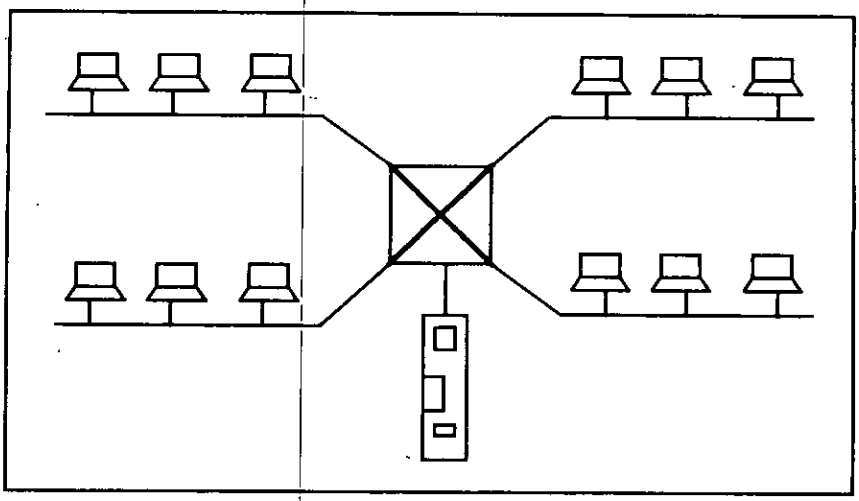


Figura 4.21 Switch de segmento.

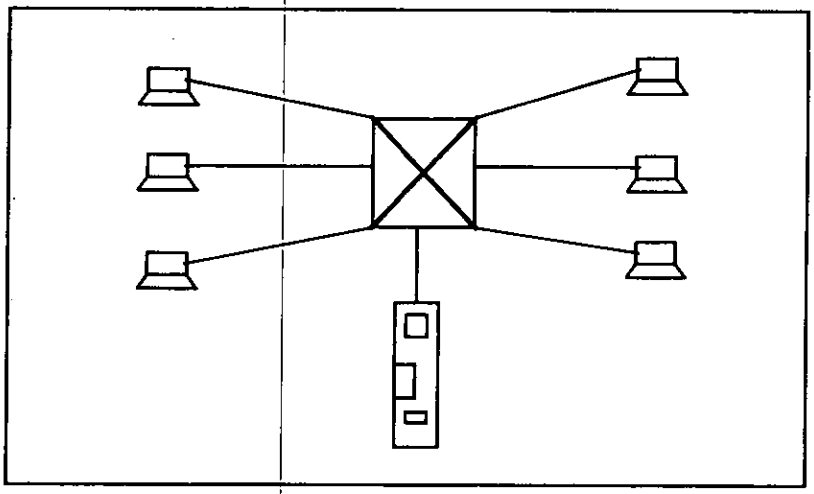


Figura 4.22 Switch privado

Otra diferencia entre LAN switches de segmentación y privados es el costo. Requiriendo menos memoria y menor diseño del switch (todos los paquetes

recibidos de un puerto LAN privado hacia un switch debe ser retransmitido a través del switch debido a que existe un solo dispositivo por LAN), los LAN switches privados son generalmente menos caros que los de segmentación. Conforme el mercado madura, otras diferencias entre distintos productos se desarrollarán, tales como alta densidad de puertos y gran modularidad para los LAN switches privados conforme ellos inicien a tomar mercado aparte de los concentradores de LAN compartidos.

Además de las diferencias entre los LAN switches de segmentación y los privados, existen muchas otras características que diferencian a los LAN switches. Estas incluyen capacidades inteligentes de filtrado, soporte para VLAN, y la integración de funcionalidad de ruteadores. No obstante, todas estas características de valor agregado pueden ser realizadas en ambos tipos de switches y no eliminar la diferencia esencial entre ellos.

Los primeros filtros en aparecer en el mercado fueron relativamente básicos, emulando la funcionalidad encontrada en muchos bridges de simple aprendizaje. De acuerdo a que los LAN switches se han hecho más valiosos, estamos viendo un nivel incrementado de funcionalidad en los sistemas de filtrado que se están desarrollando. La habilidad de realizar decisiones de filtrado basadas más allá del direccionamiento de capa MAC, tales como el tipo de protocolo, aplicación, o la congestión de tráfico dentro del switch o los switches de la red, agrega importancia al funcionamiento total del LAN switch.

La habilidad de soportar virtual LAN's (VLAN's) es otra característica clave que esta emergiendo en muchos productos LAN switch. El propósito clave de un LAN switch es eliminar el broadcast de todas las tramas LAN a cada estación en la red de tal manera que los usuarios se puedan comunicar directamente sin impactar o ser impactados por el tráfico de otros usuarios. De cualquier forma, si prohibimos el broadcast de todas las tramas en la red, entonces corremos el riesgo de no mandar en broadcast aquellas tramas que realmente necesiten serlo.

Los protocolos de red tales como Novell IPX/SPX y AppleTalk a menudo cuentan con la naturaleza broadcast de la LAN's tradicionales de medio compartido para propagar información de status tal como el anuncio de una nueva estación. Por lo que la habilidad de poder colocar un grupo limitado de usuarios de LAN switch para que sean tratados como grupo broadcast es muy importante. Este grupo broadcast "artificial" es llamado Virtual LAN.

Una de las características más poderosas de la VLAN es la habilidad de agrupar usuarios juntos en dominios broadcast independientemente de su localización física en la red. Esto da a los usuarios la habilidad de distribuir el grupo de trabajo tradicional sin requerir que los usuarios sean conectados al mismo segmento físico de LAN. Este también puede ayudar físicamente, los crecimientos, movimientos y procesos de cambio permitiendo a los usuarios ser localizados o relocalizados en la LAN, vía software VLAN.

4.2.3 Integración de switches con ruteadores.

Conforme proliferan los LAN switches a lo largo de la red, deben ser integrados dentro de internets preexistentes basadas en ruteo. La mayoría de los campus o redes de backbone son ruteadas, requiriendo que los LAN switches se conecten vía un segmento de LAN a un puerto de ruteo. Segundo, un ruteador es requerido para conectar múltiples VLAN's juntas, tal como un ruteador sería requerido para conectar múltiples LAN tradicionales juntas.

Hemos ya visto los primeros pasos para integrar switches con ruteadores; la adición de módulos de ruteo a LAN switches. Un ruteador es modificado para residir en una tarjeta en el LAN switch, muy parecido a como vemos tarjetas de ruteo integradas dentro de hubs LAN existentes.

Integrar una tarjeta de ruteador en un LAN switch mejora su valor, tal como lo hace el integrar un ruteador en un LAN hub. Sin embargo, la habilidad de integrar funciones capa 2 y distribuidas capa 3 en un sistema de conmutación es igualmente poderoso, si no es que más ventajoso para una evolución LAN de largo plazo.

Existen muchas características claves en la integración de ruteo en LAN switches. Primeramente tenemos la habilidad de soportar conmutación de multicapa. La mayoría de los productos LAN switching en el mercado actual funcionan basados en una función de capa MAC. No obstante, la habilidad de realizar decisiones de conmutación basados en la información completa de capa de red (3) puede ser de gran valor, especialmente donde la interacción de diferentes VLAN's (probablemente basadas en direccionamiento de lógica de capa de red) es utilizada. La habilidad, por ejemplo, de enlazar tablas de conmutación a tablas de ruteo, puede también mejorar notablemente la eficiencia de la red en una red de gran tamaño. Este también es crucial en la habilidad de

extender VLAN's (basadas en direccionamiento de capa MAC) a través de conexiones WAN basadas en ruteo, especialmente donde la información de la configuración debe ser compartida entre múltiples sistemas de conmutación conectados vía redes ruteadas.

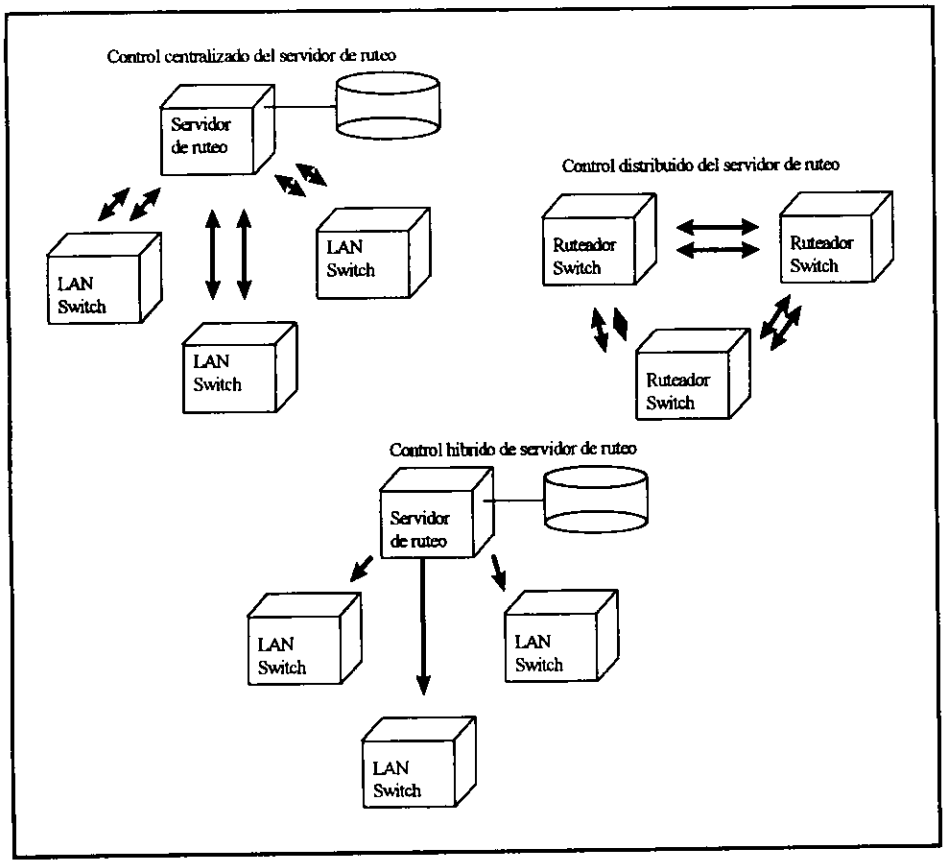


Figura 4.23 Sistemas híbridos entre LAN switches y ruteadores.

La segunda característica involucra, el como integrar información de ruteo en un ambiente de conmutación (a menudo conocido como una función de servidor de ruteo). Existen tres opciones diferentes aquí: control centralizado, control descentralizado, y una implementación de control centralizado/descentralizado.

Un servidor de ruteo centralizado acerca llamadas a un dispositivo de ruteo que contiene toda la información acerca del componente de "ruteo" de la red. Esto incluye rutas o caminos a través de la red tanto como la localización de la información para el direccionamiento de la subred de capa 3 (incluyendo VLAN's). En un sistema centralizado, LAN switches distribuidos enlistan al servidor centralizado cada vez que hay una pregunta acerca de un paquete LAN, tal como el puerto apropiado de destino en la red, o como tratar una dirección VLAN especial. Esto requiere un gran trabajo de comunicación interactiva entre todos los LAN switches y el servidor de ruteo centralizado.

Otra característica del servidor de ruteo es que no existe reposición centralizada de información. Por lo que cada LAN switch debe emular completamente a un ruteador en todas las funciones de cada de red. Esto tiene problemas al escalar redes muy grandes, tal como la mayoría de los ruteadores actuales. También requiere que cada LAN switch sea un dispositivo con alto desempeño y muchas características incluidas, algo que puede incrementar el costo y por lo tanto limitar los escenarios de desarrollo.

Un último análisis involucra un híbrido de los dos sistemas. Existe usualmente un servidor de ruteo que provee la funcionalidad de ruteo total. Sin embargo, la información contenida en el servidor centralizado es diseminada a través de los switches. Cada switch tiene la información necesaria para hacer la decisión de filtrado apropiado, pero no tiene que realizar funciones sofisticadas tales como calculo de ruteo o ser responsable de diseminar información de ruteo a otros LAN switches en la red.

Aparte de como se crea almacena o propaga la información de ruteo dentro de la red, esta el hecho de administrar información de ruteo dentro de la red. Aquí estamos buscando como un administrador de red puede accesar ala información de ruteo y como el componente de ruteo es visto desde una herramienta de administrador de redes, tal como un administrador Open View SNMP. Las características de administración de red son extremadamente importantes debido a que los LAN switches serán forzados a operar a lo largo de muchas implementaciones de ruteo en los próximos años. Al mismo tiempo, es el componente de valor agregado de administrador de red y VLAN's que tendrán que ser propietarias debido a la ausencia de estándares VLAN.

4.2.4 Protocolo ISL

El Inter-Switch Link o ISL es usado para interconectar 2 switches Ethernet VLAN usando la MAC Ethernet y medio Ethernet. Los paquetes en el enlace ISL contienen un estándar para trama Ethernet, FDDI, o Token Ring y la información VLAN asociada con la trama. Alguna información adicional esta también presente en la trama.

El ISL consiste de 3 campos primarios: el "header", el paquete original, y el FCS al final. El "header" esta dividido en campos como se muestra abajo:

- **DA Destination Address.** El campo DA del paquete ISL es una dirección destino de 40 bits. Esta dirección es de tipo multicast y se coloca en :0x00_00_OC__00__00. Los primeros 40 bits del campo DA le indican al receptor que el paquete tiene formato ISL.

- **TYPE.** El campo type indica el tipo de trama que esta encapsulada y puede ser usada en el futuro para indicar encapsulados alternativos. Los siguientes códigos de tipo han sido definidos:
  - 0000 Ethernet
  - 0001 Token-Ring
  - 0010 FDDI
  - 0011 ATM

- **USER.** Los bits user son usados para extender el significado del campo type. Por ejemplo, Las tramas Token Ring pueden tener más de un tipo. El default en el campo user es 0000. Para tramas Ethernet, dos valores del campo user han sido definidos de acuerdo a la tabla. El campo user será pasado sin cambio del paquete ISL a los encabezados internos del paquete en el switch. Para tramas Ethernet, los bits 0 y 1 del campo user indican la prioridad del paquete conforme pasa a través del switch. Por lo que cualquier tráfico puede ser manipulado de manera que permita que se enrutado más rápido, esos paquetes con este arreglo de bits deben tener ventaja de esta ruta rápida.
  - XX00 Prioridad normal
  - XX01 Prioridad 1
  - XX10 Prioridad 2
  - XX11 Alta prioridad

- **Dirección destino.** El campo SA es el campo de dirección destino en la trama ISL. Debe ser colocado a la dirección 802.3 MAC del puerto del switch que

transmite la trama. Es un valor de 48 bits. El dispositivo receptor puede ignorar el campo SA de la trama.

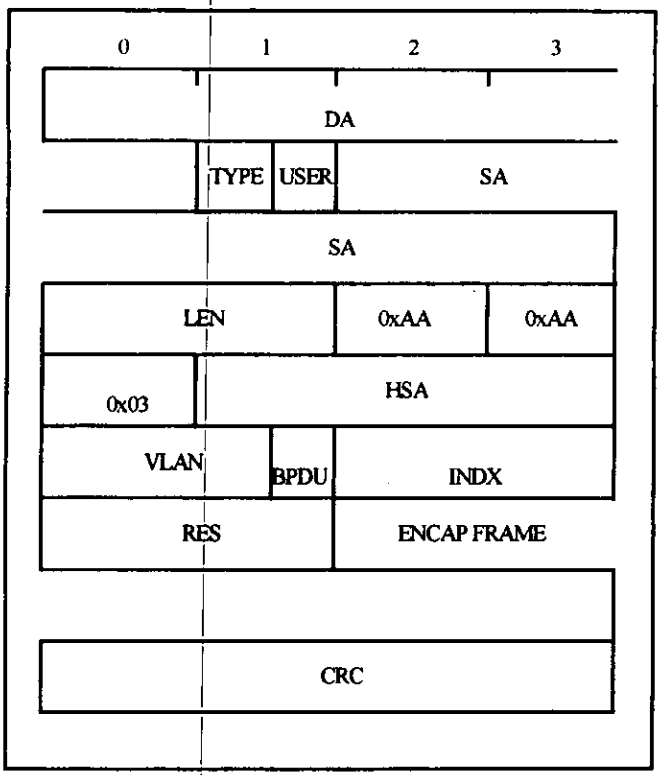


Figura 4.24 "header" del protocolo ISL

- **LEN.** El campo LEN es de 16 bits e indica el tamaño del paquete en bytes excluyendo los campos DA, T, U, SA, LEN y CRC. El largo total de los campos excluidos es 18 bytes así que el campo LEN es el largo total menos 18 bytes. Es almacenado como un valor de 16 bits.

- **AAAA03.** El campo AAAA03 es un valor constante de 18 bits de 0xAAAA03.

- **HSA.** El campo HSA es de 3 bytes, la porción de identificación del fabricante, del campo SA. Debe contener el valor 0x00_00_0C.

- **VLAN.** El campo VLAN es el identificador LAN virtual del paquete. Es un valor de 15 bits que es usado para distinguir tramas en diferentes VLAN's. Este campo es conocido a menudo como el "color" del paquete.

- **BPDU.** El bit BPDU es colocado para todas las unidades de datos de protocolo de puente que son encapsuladas por el paquete ISL. Los BDPU's son usados por el algoritmo Spanning Tree para determinar información acerca de la topología de la red.

- **INDX.** El campo INDX indica el puerto índice de la fuente del paquete por donde sale el paquete. Es usado para propósitos de diagnóstico solamente y puede ser puesto a cualquier valor por otros dispositivos. Es de 16 bits y es ignorado en los paquetes recibidos.

- **RES.** El campo RES es utilizado cuando se encapsulan paquetes Token Ring o FDDI en un paquete ISL. En el caso de tramas Token Ring, los campos AC y FC son colocados aquí. En el caso de FDDI, el campo FC es colocado en el byte menos significativo de este campo. Para Ethernet, el RES debe ser puesto a todos ceros.

- **ENCAP FRAME.** El ENCAP FRAME es la trama encapsulada, incluyendo su propio valor CRC, sin modificaciones. La trama interna debe tener un valor CRC que es válido una vez que los campos de encapsulado ISL son removidos. El largo de este campo puede ser desde 1 a 24575 bytes para acomodar Ethernet, Token Ring y FDDI. Un switch receptor puede quitar los campos de encapsulamiento ISL y usar este ENCAP FRAME como la trama recibida, asociando la VLAN apropiada y otros valores con la trama recibida como se indica arriba para propósitos de conmutación.

- **CRC.** El CRC es un valor estándar de 32 bits calculado en la trama encapsulada completa desde el campo DA al campo ENCAP FRAME. El MAC receptor checará este CRC y puede descartar paquetes que no tengan un CRC válido en ellos. Nótese que este CRC es extra al que se encuentra al final del ENCAP FRAME.

La trama (ISL)de encapsulado es de 30 bytes y el paquete FDDI mínimo es 17 bytes; no obstante, el paquete mínimo es de 47 bytes. El paquete máximo Token Ring es 18000 bytes; por lo que el máximo es 18030 bytes. Si solo se encapsulan paquetes Ethernet, el rango de tramas ISL puede variar de 94 a 1548 bytes.

4.2.5 Evaluando un switch

Después de lo que hemos revisando anteriormente podemos realizar una evaluación de un switch para su posible empleo en nuestra red. Para determinar si un LAN switch en particular cumplirá con nuestros requerimientos, el siguiente criterio nos ayudará a esta evaluación:

- ¿Qué clase de switch es el más adecuado para nuestro ambiente?
- ¿Comó garantiza la arquitectura del switch que cumplirá con nuestros requerimientos?
- ¿Será capaz de desempeñarse como se le requiera?
- ¿Qué tan flexible es?
- ¿Qué tan confiable es?
- ¿Cómo se administra el switch?

Los LAN switches se dividen básicamente en tres tipos:

1. **El switch nodo/grupo de trabajo.**
   El switch nodo esta creado para proporcionar un ancho de banda incrementado y velocidad para un grupo de trabajo (comúnmente un pequeño número de nodos 10Base-T). Estos grupos de trabajo usualmente tienen un servidor y cada cliente puede tener una conexión directa hacia el switch.

2. **El switch de segmento.**
   El switch de segmento proporciona interconexión para grupos de trabajo, Están desarrollados para conectar switches nodo/grupo de trabajo y/o hubs de medio compartido. Estos switches tienen grandes tablas de direcciones, y son más flexibles en la configuración de sus puertos, además de que soportan velocidades más altas.

3. **El switch de backbone.**
   Los switches de backbone están creados para interconectar una gran localidad y proporcionar conectividad para servicios remotos. El switch de backbone es modular y proporciona conexiones a ATM y FDDI. A menudo tienen opciones de servicios de ruteo.

Si evaluamos la arquitectura del switch debemos comenzar con el diseño ASIC, que quiere decir Application Specific Integrated Circuit (ASIC) o basado en procesador. Los switches basados en procesador están construidos con los procesadores existentes actualmente y realizando conmutación en el software. Los switches ASIC son más una combinación de hardware y firmware con los procedimientos de conmutación enteramente encapsulados dentro del ASIC. Los switches ASIC son en ocasiones preferidos sobre los switches basados en procesador porque son mucho más rápidos.

Otro punto importante en la arquitectura es el backplane compartido, idealmente los switches deben implementar una arquitectura de punto-cruzado. Una matriz es básicamente un ASIC único que mezcla múltiples rutas de comunicación con cada puerto teniendo una ruta dedicada a cada puerto; por lo que esta matriz no es muy apropiada para expandirse, por lo que lo ideal es que el switch este equipado con tecnología de backplane compartido que pueden fácilmente manejar múltiples conversaciones simultaneas.

Un elemento también importante en la evaluación del switch, es su habilidad para poder implementar VLAN's que es un punto básico en las redes LAN actuales. También debemos considerar el Port Trunking que nos permite conectar muchos puertos juntos y tratarlos como puerto único de alta velocidad; esto les permite conectarse a dos switches con múltiples enlaces con todos ellos actuando como uno solo de alta velocidad. Por ejemplo, con Port Trunking, podemos unir a dos switches con dos puertos 100VG Any-LAN. Esto duplicara el desempeño switch a switch con un solo puerto 100VG Any-LAN.

Si pasamos a la evaluación del desempeño el primer punto es la latencia. La latencia es el tiempo que le toma a un switch procesar un paquete. Es la cantidad de tiempo entre que un switch recibe una unidad de datos y cuando esa unidad es reenviada a hacia otro switch. Latencia es medida diferentemente dependiendo en que tipo de dispositivo se esta realizando la medición, ya sea "Store and Forward" o "Cut-through". La latencia en "Store and Forward" es medida en LIFO, mientras que en cut-through es medida en FIFO.

LIFO significa last (bit) in, first (bit) out. Este es el tiempo que toma desde el momento que el ultimo bit recibido entra al puerto, hasta que el primer bit de la trama es enviado hacia el puerto de destino.

FIFO significa first (bit) in, first (bit) out. Este es el tiempo que transcurre entre que el primer bit de la trama es recibido en el puerto hasta que el primer bit es enviado al puerto de destino.

Otro punto es son Throughput/Packet Loss Rate. Troughput es la velocidad de transferencia que el switch puede sostener sin perder paquetes. Mientras la letencia mide el retraso de una sola trama, throughput mide el número de paquetes, o tramas por segundo sin perdida de paquetes. En un switch, throughput es típicamente medido en paquetes por segundo (PPS), pero puede ser también referido como tramas por segundo. Packet Loss Rate (PLR) es el porcentaje de paquetes que el switch no envía dentro de una ventana de tiempo de cuando los datos fueron enviados. Bajo PLR, un paquete es llamado "perdido" si no es llevado dentro de cierto periodo de tiempo. El valor de PPS puede variar de acuerdo a la diferencia de los switches en su capacidad.

Otro elemento importante es el control de la congestión; la congestión ocurre en el momento que más paquetes son destinados a un segmento en particular de los que puede manipular. Es entonces cuando el switch no esta en posición de liberar datos hacia sus destinos. Por lo que esos datos tienen que ser almacenados en un buffer hasta que puedan ser enviados a su destino.

Si evaluamos la flexibilidad del switch, debemos decir que un switch de alto desempeño debe proporcionarnos conexiones de alta velocidad (100Mbps) para servidores de archivo y backbones, y conexiones de baja velocidad (10Mbps) para workstations y dispositivos de red.

Otro punto a considerar en la evaluación de un switch tiene que ver con la confiabilidad del switch que básicamente esta garantizada por: el tiempo que el switch funciona sin fallas, la garantía que el vendedor nos ofrece y el servicio y soporte.

Finalmente para la evaluación debemos considerar las características de administración del switch como serían:

- La administración In-band vía telnet o SNMP (tanto IP como IPX).
- La administración out-band, proporcionando comunicación vía modem a través de un emulador de terminal y una interface RS-232C.
- Monitoreo de tráfico, debido a que en una red conmutada, es importante poder identificar a los mayores usuarios en la red para colocar los switches en el lugar adecuado para optimizar la red.

A manera de conclusión mostramos una comparación entre ruteo contra conmutación.

Algunas ventajas de los **ruteadores** son:

1. Los ruteadores son extremadamente útiles cuando existen muchas rutas a través de varias redes. La ruta que los paquetes siguen entre los ruteadores esta determinada por el tráfico interredes. Si el tráfico es extremadamente alto en una vía, el ruteador selecciona otra. Si una LAN falla el ruteador puede enviar los paquetes por una vía alterna.

2. Un ruteador puede conectar 2 o más redes sin degradación de los datos. No hay limite en el número de ruteadores que pueden pasar los datos porque cada uno de ellos los regenera.

3. Un ruteador puede soportar una variedad de protocolos de comunicación. Puede transferir paquetes de datos entre diferentes medios; por ejemplo, Ethernet, Frame Relay, etc.

4. Un ruteador se autoconfigura en conocimiento de los otros ruteadores y la mejor ruta para llegar a cada segmento interconectado. Esta comunicando continuamente la información de sus tablas de ruteo con otros ruteadores para actualizarlas automáticamente.

5. Un ruteador puede mejorar la confiabilidad de un enlace al permitir "loops" - rutas redundantes- en una interred. Y proporciona más de una vía para llevar datos de una red a otra.

6. Un ruteador puede balancear tráfico a través de múltiples rutas potenciales del emisor al receptor. Puede calcular la ruta más eficiente entre los nodos de destino y de fuente. Le puede decir a una fuente rápida o a un nodo emisor que reduzca su velocidad para que el nodo de destino pueda procesar los datos.

7. Puede asegurar segmentos específicos de una red, basado en tablas que indiquen la autoridad para accesar a ciertas direcciones de redes o nodos.

8. Algunas desventajas de los ruteadores:

9. Un ruteador puede crear retraso en el tráfico porque necesita más cálculos para decidir como rutear los paquetes, especialmente, cuando las redes involucran diferentes velocidades.

10. Un ruteador requiere bastante conocimiento para administrarlo.

11. Un ruteador puede ser bastante caro. Un ruteador barato puede costar $2500 dlls. Mientras que un ruteador de alta calidad puede costar $50000 dlls.

Algunas ventajas de los **switches** serían:

1. Los switches ofrecen mejor desempeño que los bridges y hubs.

2. Son más fáciles de instalar.

3. Son más fáciles de mantener que los ruteadores.

4. Los switches les permiten a los administradores preservar su inversión en cables Ethernet, software y tarjetas de interface de red.

5. Cada computadora o pequeño grupo de computadoras puede tener un segmento dedicado de 10Mbps conectado a un switch Ethernet de alta capacidad en vez de tener que compartir 10Mbps usando el estándar Ethertnet .

6. Permiten un apropiado incremento en el ancho de banda para ser agregados a la red cuando sea necesario.

7. Los switches Ethertnet pueden proporcionar densidades de puerto de 6 a 128 puertos Ethernet por switch.

8. Tienen la habilidad de aceptar tecnologías de alta velocidad tales como ATM proporcionando puertos de alta velocidad para enlaces y conexiones de servidor.

9. Algunas características y funciones que los switches avanzados tienen incluidas son "bridging" avanzado, ruteo de multiprotocolo, control activo de congestión, garantía de calidad para tráfico de tiempo real, y tolerancia a fallas.

10. El precio por puerto para los switches varía de $400 a $1600 dlls.

Las **desventajas** serían:

- ¿**To "switch" or "not to switch**"?. Esta es la pregunta que los administradores de LAN están confrontando cuando tienen que decidir en las soluciones para mejorar el desempeño de su red.

- ¿Son los switches una solución táctica para la demanda de más ancho de banda?.

- ¿Están aquí los switches para quedarse o serán obsoletos en el futuro?.

CAPITULO 5

CONEXIÓN DE REDES LAN A REDES ATM

5.1 INTRODUCCION

Las tecnologías de banda ancha, tales como el Modo de Transferencia Asincrono (ATM por sus siglas en inglés), son necesarias por tres razones: incremento de tráfico en segmentos LAN locales, interconexion de LAN's locales y remotas, y aplicaciones de escritorio de un gran ancho de banda.

Entendiendo por tecnologias de banda ancha a aquellas que manejan mas de T1 o E1 (definidos mas adelante en este capitulo, cada uno con 1.544 Mbps y 2.048 Mbps respectivamente).

Al final de los 80's aplicaciones tales como: host a terminal y aplicaciones de LAN Token Ring y Ethernet han corrido a velocidades moderadas. Concretamente en las LAN's se incremento el numero de usuarios y por lo tanto el ancho de banda requerido. En muchos casos los administradores de red distribuyeron el trafico segmentado la red en subredes mas pequenas, mediante el uso de "puentes" y ruteadores. Sin embargo una vez que se alcanzo la capacidad de la red, se requirio de una solucion de banda ancha.

Arquitecturas de computo distribuido, basadas en microcomputadoras contribuyen a una segunda fuente de trafico interred, comunicación LAN a LAN. Dado que este trafico se incremento, viejas soluciones como 9.6Kbps y 56Kbps dedicados, fueron reemplazados por un circuito T1. Sin embargo este incremento de velocidad llego con un incremento de precio; ademas en ambientes distribuidos se requieren de multiples T1 o E1 dedicados.

Aplicaciones tales como: diseno asistido por computadora (CAD) y manufactura asistida por computadora (CAM), y bases de datos grandes distribuidas, tambien exigieron incremento en el ancho de banda LAN y WAN. Aplicaciones sensitivas al tiempo (Isocronas) como: video y multimedia, requieren un grans ancho de banda y bajo retardo de extremo a extremo.

Dado que las aplicaciones antes mencionadas crecen en popularidad, las redes LAN y WAN tendrán que soportarlas.

En la figura 5.1 se muestra una gráfica que hace notar el ancho de banda requerido por las aplicaciones.

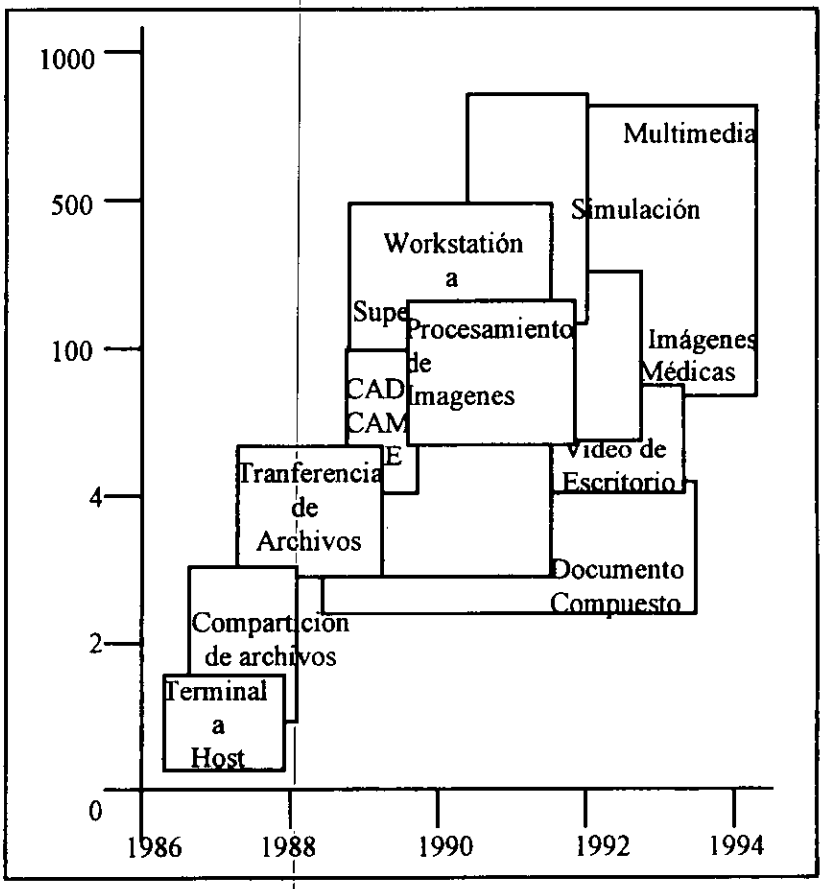


Figura 5.1. Requerimientos de ancho de banda para aplicaciones de banda ancha.

El gran ancho de banda que ofrecen tecnologías de banda ancha como: Frame Relay, Bus Dual de Cola Distribuida (DQDB) y ATM, además de otras muy recientes como Fast Ethernet y Gigabit Ethernet, ayudarán a satisfacer las necesidades de ancho de banda.

5.1.1 Tecnologías "Fast Packet"

Las tecnologías "Fast Packet", las cuales son el fundamento de tecnologías de banda ancha pueden dividirse en dos categorías:

- **Tecnología Frame Relay**

La tecnología Frame Relay usa una trama de largo variable para transmitir datos, es decir el tamaño de la trama transmitida en una LAN ó WAN pueden variar dependiendo de la cantidad de información que llegue de procesos de protocolos de capas más altas. Las tramas pueden contener miles de octetos de información de usuario. Como resultado el número de octetos que constituyen el enacabezador y el "trailer" de la trama, los cuales contienen información de direccionamineto, control de errores, etc., es insignificante.

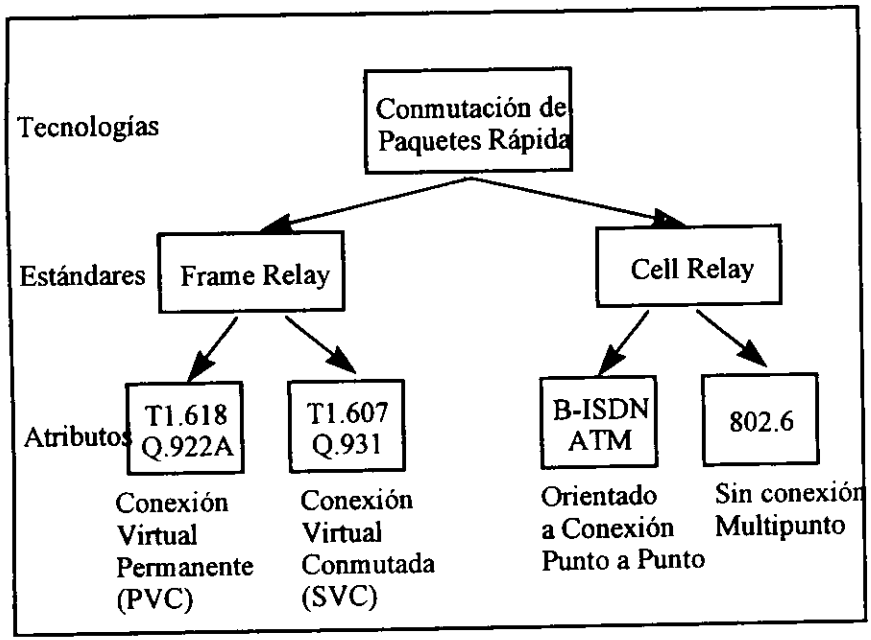


Figura 5.2 Tecnologías de Conmutación de Paquetes Rápidas.

♦ **Tecnología Cell Relay**

La tecnología Cell Relay por otra parte usa celdas de tamaño fijo, usualmente 53 octetos. Las celdas típicamente tienen 48 octetos de carga útil y 5 bytes de encabezador. Como resultado se tiene una celda de tamaño pequeño y puede transmitirse en intervalos regulares, lo cual es benéfico para aplicaciones tales como voz paquetizada, video o tráfico multimedia.

5.1.2 Tecnologías de conmutación.

Las interredes tradicionales consistían de un conjunto de estaciones de trabajo, hosts y LAN's conectadas mediante enlaces WAN tal como líneas dedicadas. Aquí hay dos tecnologías de conexión: tecnologías de conmutación y servicios que conectan el equipo final a la red.

Las tecnologías de banda ancha usan tres tipos de conmutación:

a) Conmutación de circuitos.
b) Conmutación de paquetes.
c) Conmutación de celdas.

La tecnología de conmutación de circuitos es la más antigua y garantiza al usuario final un ancho de banda predeterminado. La conexión de una llamada telefónica es un ejemplo claro de esta tecnología. Una conexión de circuitos puede consistir de una trayectoria física y una trayectoria virtual. La conexión física es la trayectoria de transmisión física (óptica ó eléctrica) a través de varios elementos de conmutación. Esta trayectoria puede cambiar con las condiciones de la red, tales como: falla del enlace, rutas congestionadas y más. Por otra parte, la conexión virtual describe la trayectoria entre dos puntos pero no necesariamente respecto de la ruta física. Al usuario final no le interesa los puntos intermedios, tanto como esto no afecte los parámetros de la comunicación, como retardo y throughput (el cuál determina la cantidad de tráfico que pasa a través de un nodo o enlace en cualquier unidad de tiempo dada, por ejemplo 10 Gbps).

Existen dos tipos de conexiones: permanente y conmutada. Una conexión virtual permanente (PVC) es análoga a una línea arrendada que la portadora establece y siempre mantiene conectada. Una conexión virtual conmutada (SVC) es similar a una llamada telefónica puesto que sólo se mantiene por poco tiempo y en el momento que el usuario lo desea la termina.

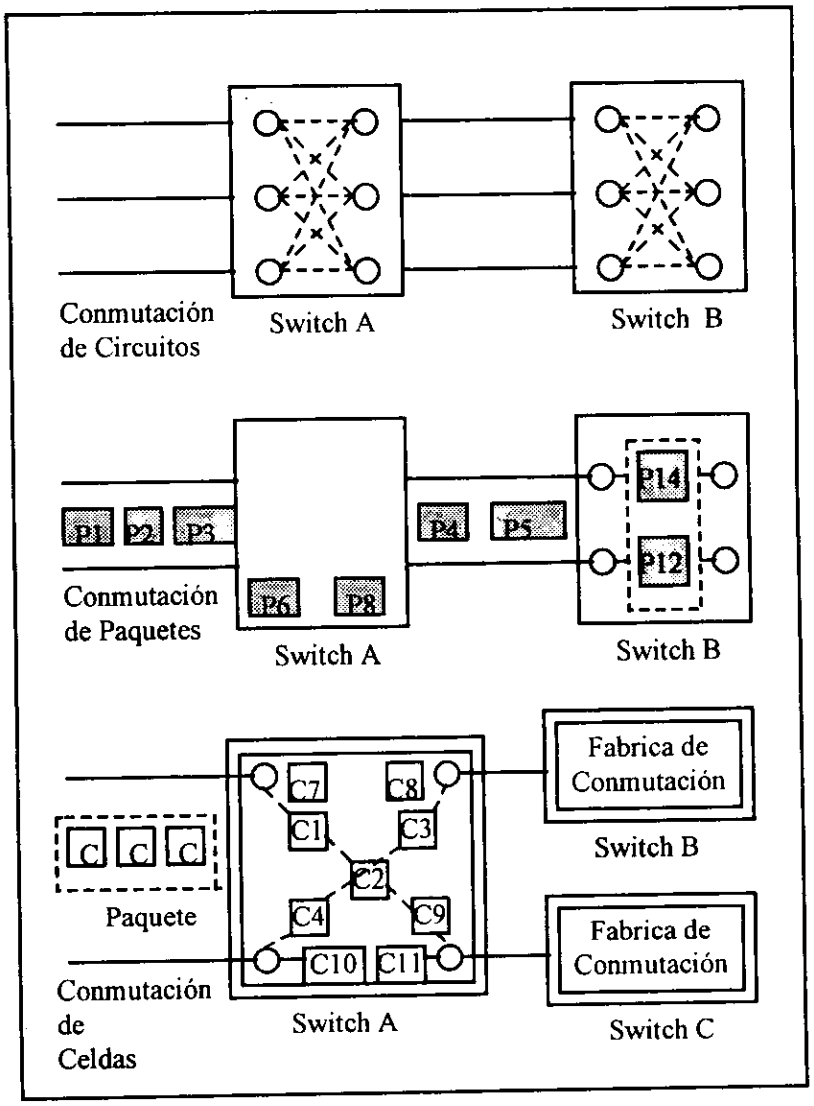


Figura 5.3 Tecnologías de Conmutación

Las redes de conmutación de paquetes mejoran a las de conmutación de circuitos permitiendo compartir dinámicamente el ancho de banda LAN o WAN disponible. Las estaciones de trabajo transmiten paquetes de información, los

cuales son ruteados hasta que estos alcanzan su destino. El largo del paquete puede variar dependiendo de la velocidad de transmisión, protocolo de red, etc.

En la conmutación de celdas se fija el tamaño de los paquetes en un valor pequeño. Esta tecnología ofrece la ventaja de un retardo predecible y un throughput más alto.

Existen dos tipos de servicios usados para conectar equipo de un usuario final a la red: servicio orientado a la conexión y servicio sin conexión. El servicio orientado a la conexión (usado por Frame Relay y ATM) requiere procedimientos de establecimiento de llamada para establecer la ruta, en este caso se le da seguimiento al proceso de transmisión de información. Un servicio sin conexión (Servicio de Datos Multimegabit Conmutado-SMDS y el Protocolo de Interred-IP) no requiere del establecimiento de conexión a priori para la transmisión de datos. En un servicio no hay una ruta predeterminada que los datos deben seguir a través de la red, por lo que los datos pueden llegar a su destino en un orden diferente al cual salieron del origen, además la entrega no está garantizada por lo que los protocolos de capas más altas ejecutan detección y corrección de errores de extremo a extremo y checa la integridad de los datos. El control de flujo en servicios sin conexión no existe, ó es mínimo si es que hay. Este servicio es algunas veces llamado servicio datagrama.

5.1.3 Concepto de ATM

La tecnología ATM está normalizada por el Sector de Telecomunicaciones la Unión de Telecomunicaciones Internacional (ITU-T), el Instituto de Estándares Nacionales Americanos (ANSI) y el Forum ATM.

Dos desarrollos significativos preceden a ATM:

a) Al inicio de los 80´s la ITU define la Red Digital de Servicios Integrados (ISDN por sus siglas en inglés) de banda angosta.
b) Al final de los 80´s, ITU define ISDN de banda ancha (B-ISDN).

La ISDN de banda angosta (N-ISDN) definió dos interfaces de acceso: una interface de velocidad básica (BRI) de 144 Kbps y una interface de velocidad primaria (PRI) operando a 1.544 Mbps y 2.048 Mbps. Estas interfaces fueron diseñadas para llevar voz, video y datos, además de información de control.

B-ISDN ofrece velocidades de transmisión de 622 Mbps y más; soportando todo tipo de tráfico. ATM es la tecnología seleccionada por la ITU para implementar la B-ISDN.

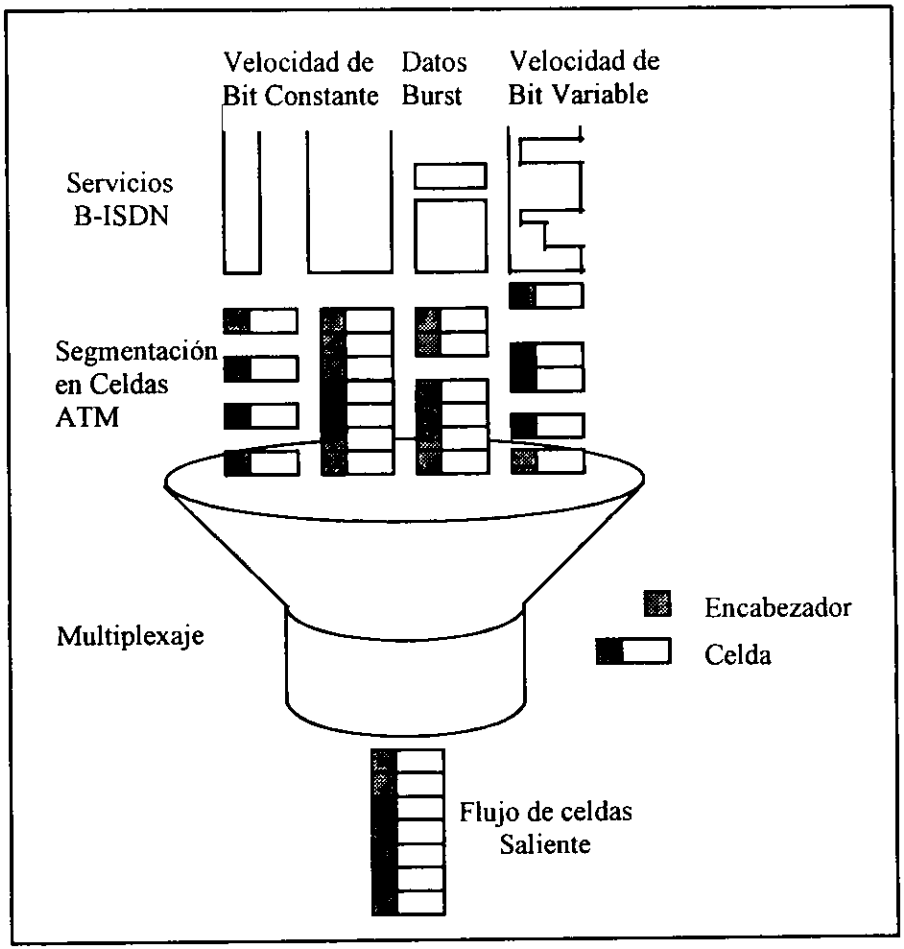


Figura 5.4 El concepto de ATM.

5.1.4 Principio de operación de ATM

El Modo de Transferencia Asíncrono es una tecnología de conmutación y multiplexaje basado en celdas.

En la figura 5.4 se ilustra como ATM transmite datos. El flujo de celdas ATM inicia con señales de usuarios individuales. Las señales pueden incluir servicio de velocidad de bit constante (CBR) tal como una línea DS1 (Data Stream nivel 1), servicio de velocidad de bit variable (VBR), video comprimido o datos en ráfaga (tráfico LAN). ATM entonces segmenta las señales en bloques de información de 48 octetos y entonces les adhiere un encabezador de 5 octetos, el cual contiene información de direccionamiento. El paquete resultante de 53 octetos es llamado celda. En este punto ATM toma las celdas de las varias fuentes individuales y las mezcla para después enviarlas al switch ATM. El switch multiplexa las celdas y entonces estas contienden por ranuras de tiempo en el flujo de celdas saliente.

En la figura 5.4, el concepto "burst" se refiere a tráfico de datos en ráfaga, tal como tráfico LAN. ATM es un servicio orientado a conexión, lo que significa que este requiere el establecimiento de una conexión antes de que se pueda enviar información de usuario. Existen dos tipos de conexiones, que serán explicadas en detalle en secciones posteriores, ellas son: conexión virtual permanente (PVC) y conexión virtual conmutada (SVC).

5.1.5 Características y ventajas de ATM

Algunas de las características más sobresalientes de la tecnología ATM son:

- Manejo de todo tipo de tráfico.
  ATM es un tecnología única desde el punto de vista que es capaz de multiplexar, conmutar y transportar cualquier tipo de tráfico sin importar su naturaleza (video, voz y datos; en todas sus modalidades); lo cual se hace con capas de adaptación adecuada para cada tipo de tráfico, excepto E2. Esta característica hace que ATM sea la tecnología escogida para B-ISDN.

- ATM contiene algunas de las características de la conmutación de paquetes (asignación dinámica de ancho de banda) y también características de conmutación de circuitos, tal como el retardo.
- Multiplexaje estadístico.
  Como se vio en la figura 5.4, las celdas pertenecientes a diferentes fuentes se ponen en un enorme tubo y se mezclan de una forma tal que la transmisión del tubo es optimizada. La optimización es hecha mediante multiplexaje

estadístico.

En una red ATM, varias fuentes son combinadas en un enlace sencillo. Si se tiene un red con Multiplexaje por División en el Tiempo (TDM por sus siglas en inglés) el ancho de banda efectivo es simplemente la suma de los anchos de banda individuales. Si hay dos fuentes con ancho de banda X y Y, su ancho de banda efectivo es (X +Y).

Con multiplexaje estadístico (STDM) en ATM el ancho de banda es Z donde Z<(X + Y) debido a que todos los bits son empaquetados en celdas, el switch ATM entonces multiplexa únicamente celdas con información válida y descarta las celdas sin información. Entonces el ancho de banda efectivo es reducido.

En la figura 5.5 se muestra una comparación entre TDM y STDM, de donde podemos ver que con TDM el ancho de banda es desperdiciado, dado que la asignación del mismo es fija. Con STDM no se desperdicia ancho de banda y siempre hay más ancho de banda disponible que con TDM. Para utilizar STDM, todo el tráfico debe ser paquetizado incluyendo la voz, creando tráfico VBR.

- ATM como tecnología para LAN y WAN.

  En el ambiente WAN, ATM ofrece las siguientes ventajas:

  - Integración de servicios.

    El número de servicios ofrecidos por portadoras alrededor del mundo ha proliferado en los últimos años. Lo cual es una respuesta directa a las demandas del usuario. Uno de los beneficios de ATM es la habilidad para satisfacer la mayoría de los requerimientos de usuarios con una sola tecnología y reducir la proliferación de nuevas clases de redes.
  - Costo de red y equipo más bajo.

    El equipo de conmutación ATM, cuesta significativamente más que un equipo TDM , pero un ATM switch ofrece un costo-beneficio más alto respecto del multiplexor TDM.
  - Tecnología apropiada para ambiente de alta velocidad. ATM ofrece una tecnología que puede entregar servicios en velocidades muy altas que ahora llegan a ser disponibles y están siendo demandadas por los usuarios. Hay dos clases distintas de usuarios: el ambiente de portadora donde ATM es provisto como un servicio al usuario; el ambiente de red privada donde una organización compra líneas de una portadora, o ella misma las instala y construye una red privada ATM.

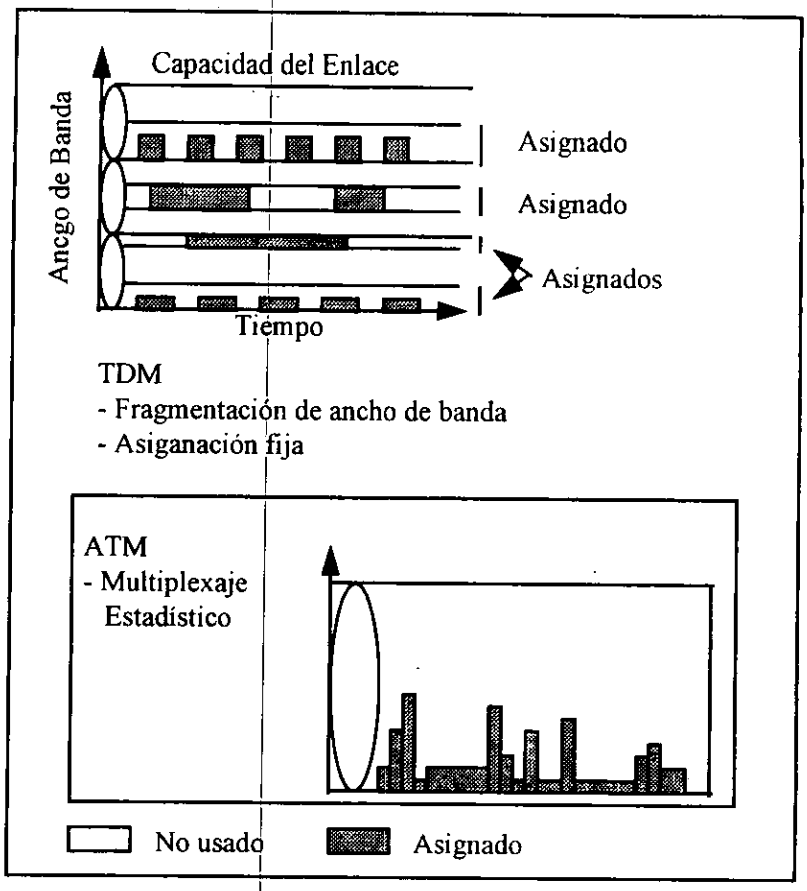


Figura 5.5 Comparación de TDM y Multiplexaje Estadístico

Con ATM en ambientes LAN:

- Los usuarios necesitan un sistema LAN de más alta capacidad. Comparada a las velocidades internas de las primeras PC´s, la LAN tenía una velocidad grande. Como las PC´s estaciones de trabajo han incrementado en capacidad, también se ha incrementado la demanda de la capacidad de las LAN. A corto plazo el problema puede ser resuelto reestructurando LAN´s grandes en unas más pequeñas, puenteando y ruteando; como la mejora en capacidad de las PC´s y estaciones de trabajo no parece estancarse, se necesita un sistema LAN más rápido.
- Costo/benéfico de ATM en ambientes LAN: la ventaja de un sistema conmutado sobre un sistema compartido se ve fácilmente de la

siguiente manera; suponiendo que se tienen 50 dispositivos conectados a una LAN Ethernet de 10 Mbps. Este es un sistema de medio compartido. Únicamente una estación puede transmitir datos en un momento dado. Esto significa que el througput POTENCIAL de la red es de 10 Mbps. Ahora si tenemos los mismos dispositivos conectados a través de un switch (suponiendo una velocidad por puerto de 10 Mbps), cada dispositivo es capaz de enviar en una velocidad de 10 Mbps puesto que el medio es dedicado. El througput POTENCIAL de la red no es 10 Mbps., si no 50 veces (50 enlaces de 10 Mbps), es decir 500 Mbps. La diferencia está en el costo de la tarjeta adaptadora de red que tienen que soportar 10 Mbps contra 500 Mbps en un sistema compartido. Un sistema ATM entregará un througput mucho más grande que un sistema LAN de medio compartido lo que trae como consecuencia un costo significativamente más bajo.

- ATM satisface las necesidades de ambientes LAN de alta velocidad. En cuanto a ancho de banda, en un ambiente LAN algunos usuarios requieren un througput mucho más alto que otros. En un ambiente compartido todos los dispositivos deben tener adaptadores que corran a la misma velocidad (velocidad de la LAN). Con ATM, estaciones individuales pueden tener conexiones a velocidades apropiadas a su capacidad. PC's a 10 Mbps y servidores a 100 Mbps.

- En una red ATM no hay recuperación de errores, por lo que esta es responsabilidad de usuarios finales. La red de conmutación de celdas ATM únicamente checa encabezadores y simplemente descarta las celdas erróneas. En ningún momento de la red ATM intenta recuperarse de errores mediante retransmisión de información, tampoco hay recuperación de errores a nivel de enlace, como los protocolos de enlaces tradicionales. Por ejemplo no tiene sentido, pedir retransmisión de información en una conexión de voz, dado que la información llegará demasiado tarde y será obsoleta cuando esto ocurra.

- No existe control de congestión y control de flujo a nivel de red. La lógica de procesamiento requerida es demasiado compleja para ser acomodada en las velocidades involucradas. En lugar de ello, ATM usa un conjunto de controles de velocidad de entrada (usando el esquema de control de velocidad "leaky-bucket" -cubo goteante-) que limita la velocidad de tráfico entregada a la red. Por otra parte, algunas celdas pueden ser marcadas de tal forma que ellas son las primeras a ser descartadas en caso de congestión. Los equipos finales no son notificados cuando las celdas son descartadas, es responsabilidad de los

protocolos de capas superiores recuperar la información de las celdas pérdidas, esto si es necesario y es posible.

Algunas ventajas adicionales de ATM son: escalabilidad de ancho de banda, de tal forma que siempre se contará con ancho de banda suficiente para satisfacer las necesidades que demanden aplicaciones futuras; número de redes reducido (red de voz, red de video y red de datos, juntas); protección de la inversión existente para usuarios que conecten sus sistemas actuales a redes ATM; ahorro de costos de administración y operación debido a la integración de redes; accesos de alta velocidad empezando por E1 y T1.

5.1.6Desventajas de ATM.

Existen ciertas desventajas de ATM derivadas del hecho de ser una tecnología nueva, por ejemplo:

- Existen tres tipos de direcciones ATM propuestos (se analizan en secciones posteriores) de los cuales no se vislumbra cual sea el definitivo, esto ha originado que los fabricantes de equipo ATM implementen los tres esquemas de direccionamiento, haciendo aún más complejo el equipo; ó sólo implementando el que el fabricante considere llegue a ser estándar, arriesgándose a que su equipo no pueda interoperar si se estandariza un esquema diferente.

- Para que las aplicaciones de LAN actuales puedan correr sobre ATM, ó las LAN´s utilicen a ATM como backbone, hay necesidad de una interface entre ATM y las LAN´s dada su naturaleza. ATM es orientado a conexión y las LAN´ son sin conexión. ATM es una tecnología punto a punto, ó multipunto; y las LAN´s son broadcast (medio compartido).

- Faltan sistemas de enrutamiento ATM por definirse en su totalidad : IISP (Protocolo Inter-switch Interino) y PNNI (protocolo de Interface Red-Red Privado).

5.1.6 La celda ATM

La unidad primaria de transmisión y multiplexaje es la celda. Existen factores

que deben tomarse en cuenta cuando se habla del tamaño de la celda:

- **Eficiencia de transmisión.**
  En paquetes más grandes, el retardo es más alto, pero la relación encabezador/información es pequeña, lo cual es bueno. En paquetes más pequeños, es más alta la relación de encabezador/información.

- **Retardo.**
  Diferentes retardos son encontrados por un paquete: retardo de transmisión básico, retardo en cada nodo de conmutación, retardo de paquetización y despaquetización.

- **Complejidad de implementación.**
  Teniendo una celda de tamaño fijo, el enrutamiento, la inserción, extracción y multiplexaje de celdas ATM se hace más rápido sin tener que ver el campo de información de la celda.

El tamaño de la celda fue resultado de un compromiso:

- Las portadoras europeas quisieron una celda de tamaño pequeño, tanto como 16 octetos, para minimizar el retardo y optimizar la transmisión de voz. Ellos querían simplificar la cancelación del eco. Muchas distancias entre los países europeos son lo suficientemente cortas para no necesitar canceladores de eco; pero el retardo adicional originado por celdas grandes lo requería.

- Las portadoras estadounidenses querían un tamaño de celda de 200 octetos, para reducir el número de encabezadores que tenían que ser procesados para completar una transferencia de archivos. Distancias más grandes en USA significaba que todo el equipo de transmisión necesitaba canceladores de ecos.

Hubo objeciones a una celda demasiado larga, basadas en el retardo introducido en una conexión de voz, cuando una celda de voz entra al switch detrás de una celda de datos. Dado que cada switch tiene una cola de transmisión, este retardo impredecible podría ser sumado muchas veces a medida que la celda avanza en la red. Celdas cortas eliminan la adición potencial de retardo de cola variable y grande.

La negociación entre eficiencia y retardo de paquetización versus tamaño de celda se ilustra en la figura 4.6. Como retardo de paquetización se refiere al tiempo requerido para llenar una celda a 64 Kbps, esto es la velocidad para llenar la celda con muestras de voz digitalizadas.

Cuando el tamaño de la celda estuvo a discusión en el Forum ATM, había un debate sobre si la carga útil de la celda era de 38 o 64 octetos. La decisión de 48 bytes fue un compromiso entre estas dos posiciones. El tamaño del encabezador fue una negociación separada, las dos opciones eran 3 y 8 bytes, finalmente se optó por un encabezador de 5 bytes.

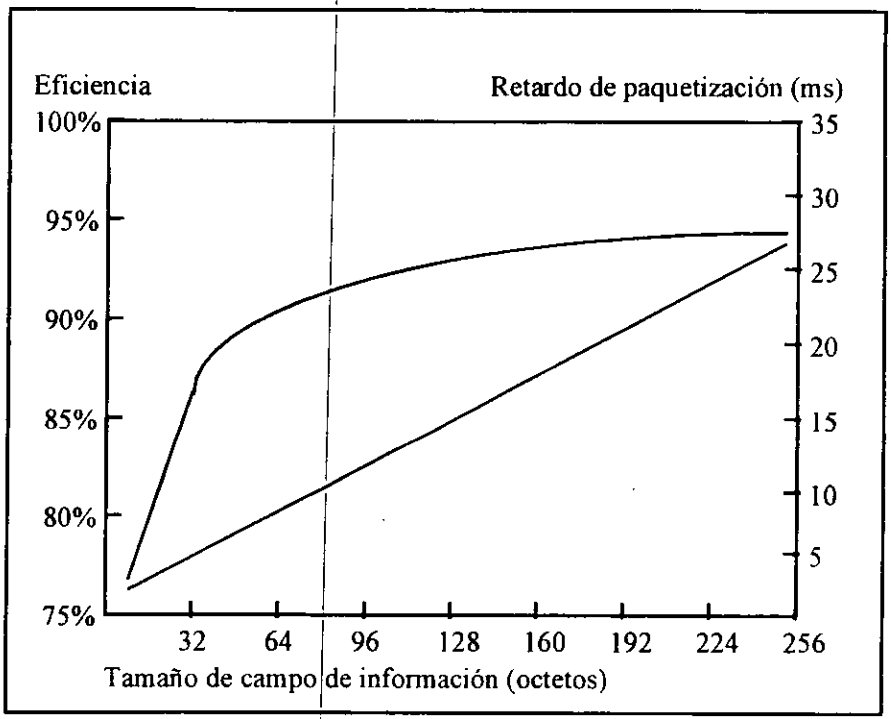


Figura 5.6. Tamaño de celda vs retardo.

5.1.7 Estructura de la celda ATM.

Los estándares ATM definen una celda de tamaño fijo con 53 octetos, compuestos de 5 bytes de encabezador y 48 bytes de campo de información. En la figura se muestra el formato de la celda ATM en la Interface Usuario-Red (UNI); a continuación se nombra cada uno de sus campos y posteriormente se explicaran en detalle.

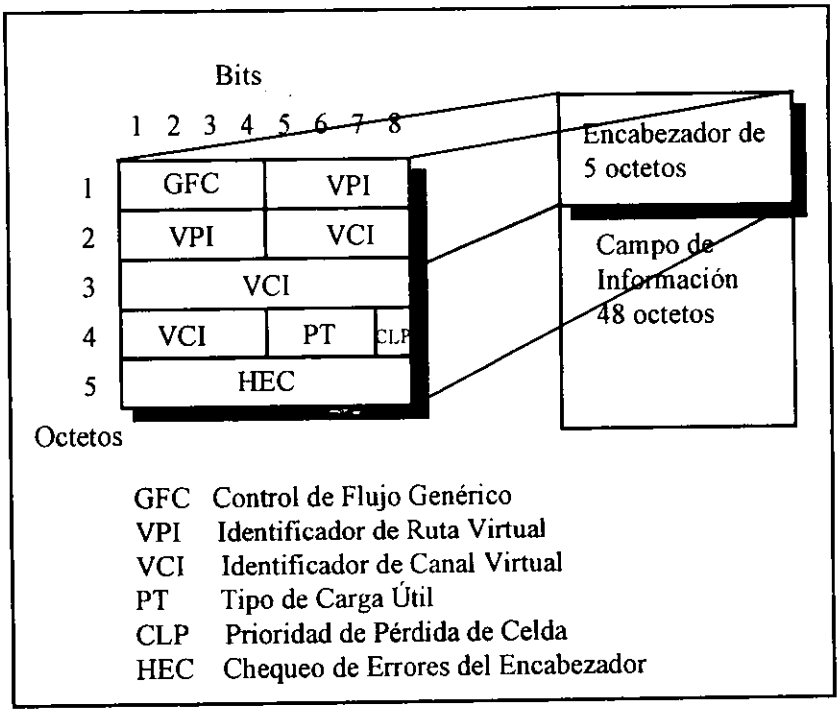


Figura 5.7 Estructura de la celda ATM en la interface UNI.

5.1.8 Arquitectura de B-ISDN

Dado que ATM es la tecnología que hará posible la implementación de B-ISDN, y por lo tanto forma parte de su modelo tridimensional de capas, es importante conocer la configuración de referencia de esta. Dicha configuración de referencia especifica varias entidades funcionales y puntos de referencia. A continuación se muestra un esquema con entidades funcionales y puntos de referencia.

Los puntos de referencia del modelo de referencia son:

- **R** Punto entre el equipo no B-ISDN y adaptador de terminal.
- **S** Punto entre el equipo de usuario (B-ISDN o TA) y el equipo de terminación de red de premisas de cliente.
- **T** Punto entre el equipo de terminación de red de premisas de cliente y el equipo de terminación de red pública (B-NT1).

- **U** Punto entre equipo de terminación de red pública y la red pública.

Como se puede observar en la figura del modelo de referencia, también tenemos grupos funcionales:

- **B-NT1** Terminación de red 1 de banda ancha, la cual maneja la terminación de la línea de transmisión, así como funciones de operación y mantenimiento, tal como la terminación de una línea SONET (Syncronous Optical Network).
- **B-NT2** Terminación de red 2 el cual incluye funciones de capas más altas, tal como multiplexaje y señalización. Por ejemplo un PBX (Private Branch Exchange).
- **BTE-1** Equipo B-IDSN.

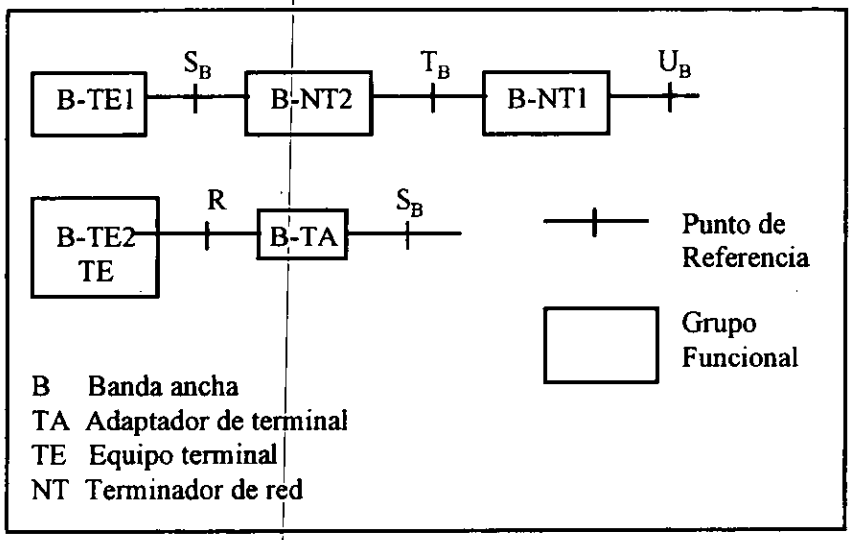


Figura 5.8. Modelo de referencia de B-ISDN.

- **BTE-2** Equipo no B-ISDN.
- **TE** Equipo no ISDN.
- **TA** Un adaptador de terminal, el cual acopla equipo no B-ISDN con equipo B-ISDN.

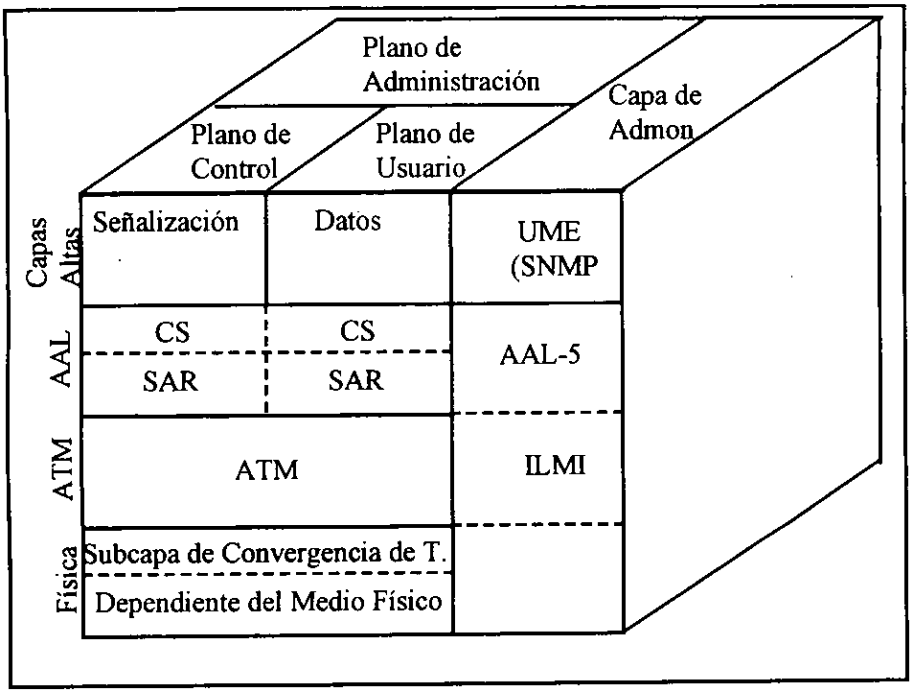


Figura 5.9. Modelo de B-ISDN.

5.1.9 Modelo de capas B-ISDN.

El modelo de la arquitectura B-ISDN es un modelo de capas vertical cubriendo el transporte, la conmutación, la señalización y el control, así como las aplicaciones. Esta arquitectura consta de tres planos como se ilustra en la figura 5.9. Los tres planos son designados como: plano de usuario, plano de control y plano de administración. El plano de usuario provee transferencia de información de usuario a usuario, y controles requeridos para al transferencia, tal como control de flujo y recuperación de errores. El plano de control provee funciones de control de conexión y control de llamada, tal como señalización. La señalización establece, supervisa y libera las llamadas y las conexiones.

En el plano de administración existen dos tipos de funciones: funciones de administración de capa y funciones de administración de plano. Todas las funciones de administración que se relacionan al sistema como un todo son localizadas en el plano de administración. Su función es coordinar a los diferentes planos. Una estructura sin capas es usada en este plano. Las

funciones de administración de capa están en una estructura de capas. La capa de administración ejecuta funciones de administración relacionadas con el desempeño, operación y administración de recursos y parámetros para cada una de las capas del plano de usuario.

5.2 PLANO DE USUARIO.

5.2.1 Datos de usuario en celdas

La meta es poner información de usuario en celdas ATM. Hay muchos tipos de información y ellas requieren ser pasados en celdas. En la figura 5.10 se tienen las capas y subcapas de ATM.

Como se verá posteriormente la capa física envía y recibe bits en el medio de transmisión, y este envía y recibe celdas de la próxima capa más alta, capa ATM. La capa ATM entonces conmuta celdas al circuito apropiado para conectar a un sistema final a su aplicación específica o proceso. El campo de información de la celda, es generado o destinado a la capa de adaptación ATM (AAL), que es la capa que actúa como interface entre las funciones más altas y procesos con la capa ATM. Las celdas ATM se encapsulan en una trama SONET, en una trama SDH (Sinchronous Digital Herarchy), o en una trama DS3 de PDH (Plesiochronous Digital Herarchy). El procedimiento se ilustra en la figura 5.11

5.2.2 Capa física ATM.

ATM fue definido para hacer la función de transporte de datos físico tan independiente como fuera posible de la función de conmutación ATM y las capas arriba de ATM. ATM es capaz de operar sobre una amplia variedad de enlaces físicos. Estos varía en velocidad, medio y estructura. A continuación se describen las características más sobresalientes de la Jerarquía Digital Plesiócrona (PDH), de la Jerarquía Digital Síncrona (SDH) y de la Red Óptica Síncrona (SONET), los cuales son sistemas de transmisión digital que pueden ser utilizados para transportar celdas ATM.

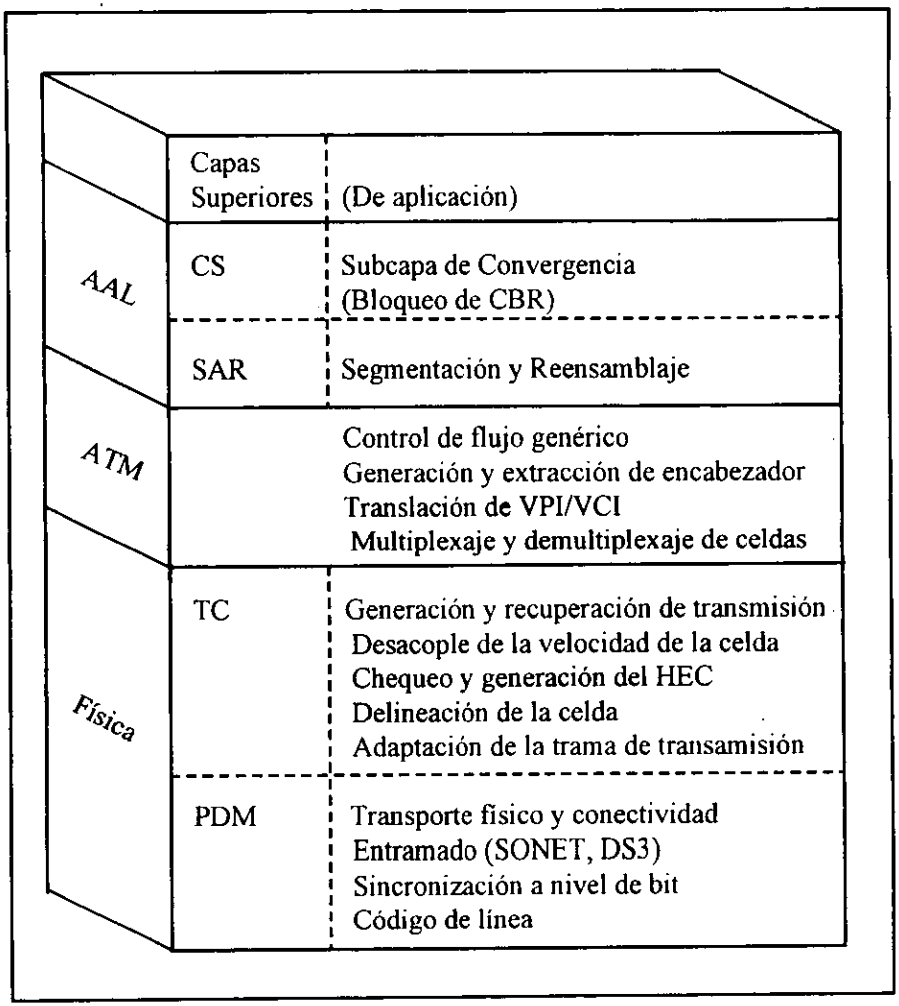


Figura 5.10. Capas y subcapas del plano de usuario.

5.2.2.1 Jerarquía Digital Plesiócrona

La jerarquía digital plesiócrona (PDH) es el sistema de transmisión existente utilizado hoy en día a través del mundo, para transmisión de voz (aunque también se esta usando para llevar datos y videoconferencia en líneas dedicadas). Para estos sistemas los medios de transmisión van desde cobre y

radioenlaces, hasta fibra óptica.. Los equipos que proveen los servicios antes mencionados, son multiplexores y sistemas de interconexión digital serán utilizados para transportar celdas ATM.

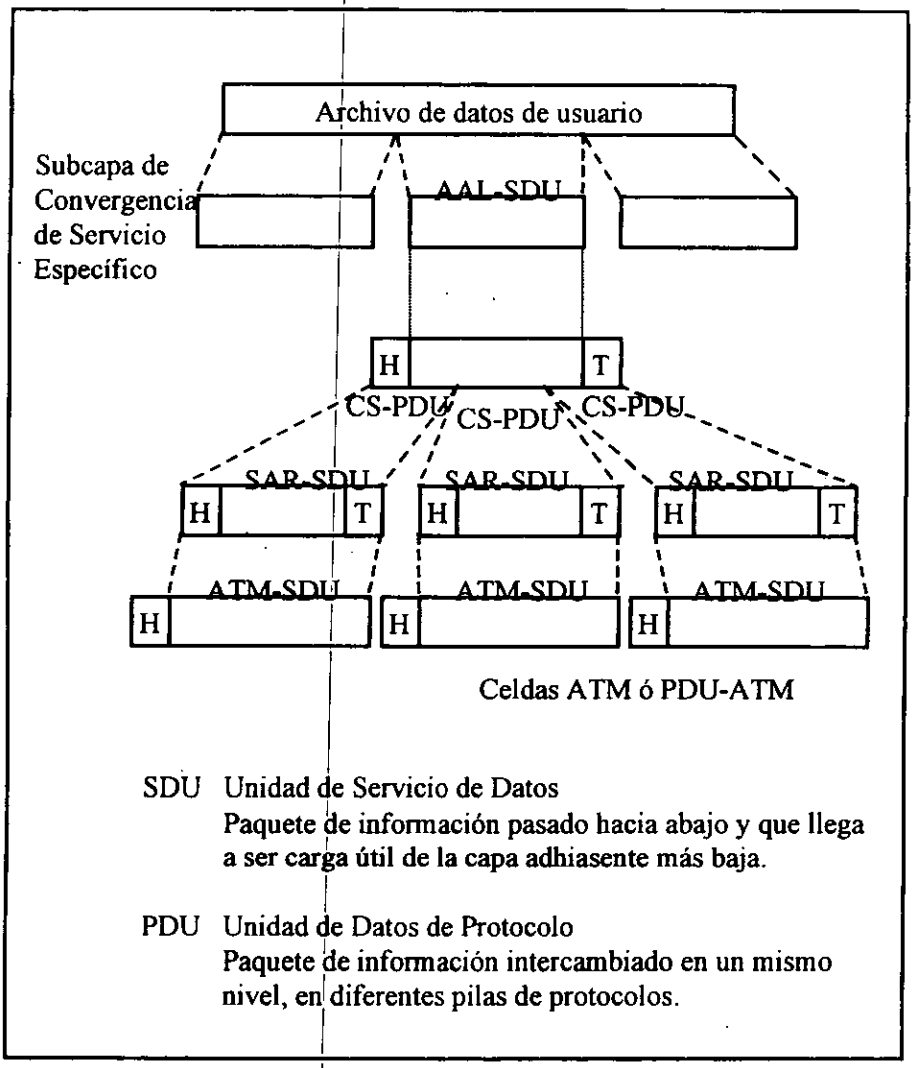


Figura 5.11. Diagrama esquemático de la obtención de celdas ATM.

Velocidad Mbps	Europa	Norte América	Japón
0.064	E0	DS0	
1.544		DS1	X
2.048	E1		
3.152		DS1C	
6.312		DS2	X
8.448	E2		
34.368	E3		
44.736		DS3	
139.264	E4		
274.176		DS4	100 Mbps
			400 Mbps

Tabla 5.1 Velocidades de PDH.

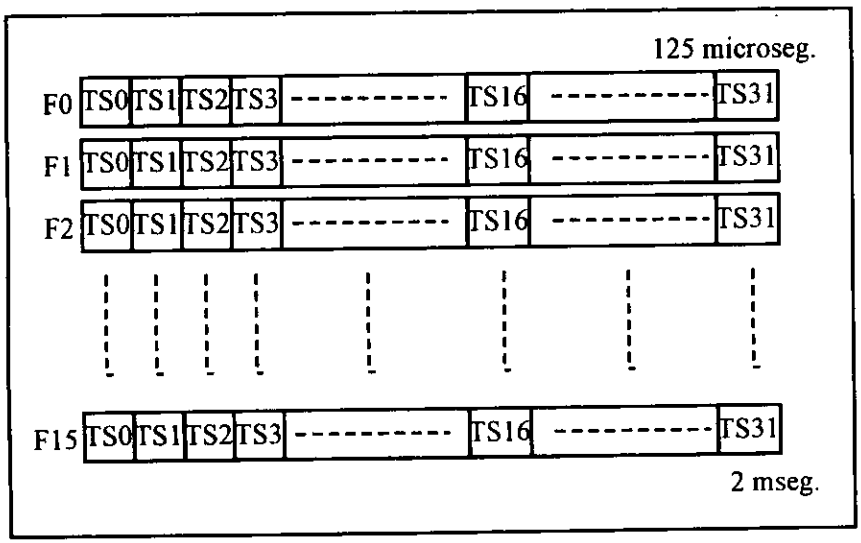


Figura 5.12. Multitrama de 16 E1´s.

Existen tres variantes de PDH, ellas son utilizadas en diferentes zonas geográficas alrededor del mundo. La tabla 5.1 muestra la gama de velocidades que se tienen con PDH. Para la PHD recomendada por el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) e implementada en

Europa la trama básica de transmisión es el E1 y su formato es el mostrado en la figura 5.12.

Se trata de una trama de 32 ranuras de tiempo que se repite cada 125 microsegundos. La velocidad de cada ranura de tiempo (TS - time slot) es de 64 Kbps. En el TS0 se tiene una señal de alineación de trama (FAS) y señal de indicación de alarma (AIS), así como un CRC-4. El TS16 se tiene una señal de alineación de multitrama (MFAS) y señalización de línea de los TS 1-15 y 16-31. Con 16 tramas E1 se forma una multitrama. En el TS16 de la trama 0 (F0) de la multitrama se tiene la señal MFAS y en las siguientes 15 tramas el TS16 sirve para señalización de línea. El la figura 5.12, se muestra una multitrama de 16 tramas E1.

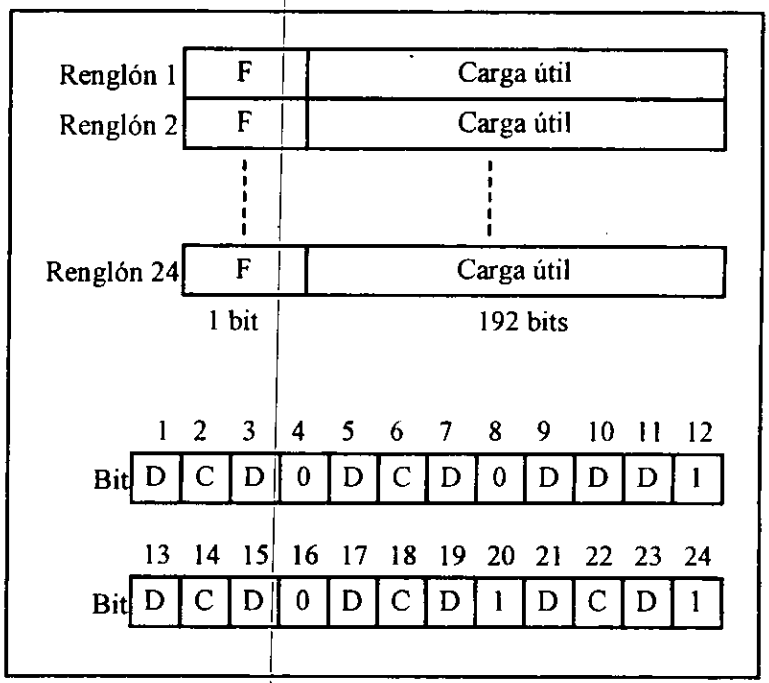


Figura 5.13. Supertrama Extendida (ESF) y bits de sincronía de la ESF.

Para la PDH de Norte América, la trama básica es la DS1 que es una trama de 24 TS de 64 Kbps cada uno, y un bit F. El protocolo dependiente del medio

físico DS1 está basado en la supertrama extendida (ESF) ilustrada en la figura 5.13. Esta es una trama de 3 ms de duración que está compuesta de 24 renglones de 193 bits cada uno. El primer bit de cada renglón bit F es usado para entramado y varias funciones de operaciones y mantenimiento. Los bits de entramado de una ESF sigue el patrón mostrado en la figura 4.13. Los bits D forman un canal de 4 Kbps que es usado para llevar información de desempeño al otro extremo. El bit C es usado para CRC. El CRC que es usado es el CRC-6. Los bits restantes F son usados para alineación de trama. La señal de alineación de trama es 001011_B.

5.2.2.2 SONET

La red óptica síncrona es una forma de entramado TDM en una línea de transmisión que provee marcas de referencia tales que el receptor sabe como interpretar los flujos de bits. Aunque las tramas imponen un encabezador de al menos 4.4 %, SONET ofrece dos ventajas:

- **Apuntadores**
  En la porción del encabezador de la trama SONET se cuentan con apuntadores que indican donde empieza un octeto explícitamente. Dado que las celdas son alineadas en octetos y fluyen juntas en la carga útil SONET, los apuntadores hacen más fácil la delineación de la celda.
- Hay ancho de banda en los bytes del encabezador SONET para canales de comunicaciones y operaciones, separados de la información, lo que facilita el control y la administración de la red.

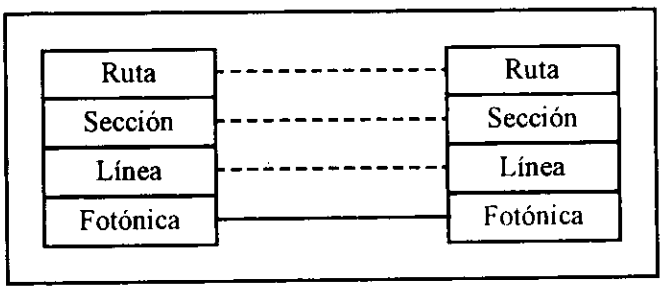


Figura 5.14. Modelo de capas de SONET.

SONET está definida como una estructura de capas jerárquica, además para administrar mejor la información en SONET, la información es accesada a nivel de byte en lugar de a nivel de bit. Cada capa puede manejar comunicaciones

intracapa independientemente y es responsable por una por una porción de la administración completa del enlace.

En la figura 5.14 se muestran las diferentes capas en SONET, que son:

- **Fotónica**
  Esta capa provee transmisión óptica en una muy alta velocidad. Las características negociadas con esta capa incluyen forma de pulso óptico, niveles de potencia de transmisor y receptor. Los equipos electro-ópticos se comunican en este nivel. La función principal de esta capa es convertir la señal eléctrica a señales ópticas y mapear una trama STS-n en una trama OC-n. La razón para esto es que las capas más altas ejecutan sus funciones en un dominio eléctrico, mientras que el sistema de transmisión físico es en una dominio óptico.

SONET va más allá de las funciones de transmisión existentes establecidas en el equipo de un nodo, para negociar en detalle con líneas de transición y secciones de líneas. Esto lo hace dedicando encabezadores en la trama SONET a cada una de las siguientes capas:

- **Capa de sección.**
  La capa de sección negocia con el transporte de tramas STS-n a través del medio físico. Las funciones incluyen entramado, monitoreo de errores de sección y comunicación y adición del encabezador de nivel de sección. Una sección de la facilidad de transmisión incluye puntos determinación entre un elemento terminal de red y un repetidor o entre dos repetidores. El encabezador de sección (SOH) en la trama SONET se aplica únicamente al largo del cable de fibra óptica entre elementos activos. Cualquier dispositivo activo como un repetidor, termina estos encabezadores de sección, por lo tanto pueden ser llamados equipos determinación de sección (STE).

- **Capa de línea**
  La capa de línea negocia con el transporte confiable del "payload" de la capa de ruta y su encabezador. A través del medio físico la capa de línea provee sincronización y multiplexaje para la capa de ruta. La línea es el medio de transmisión requerido para transportar información entre dos elementos de red consecutivos (por ejemplo, un multiplexor OC-n/OC-m), uno de los cuales origina la señal de línea y otro que la transmite. Los elementos de red son llamados equipos determinación debido a que las señales terminan en ellos. Los canales de encabezador de línea (LOH) se extienden a través de múltiples secciones de cable y repetidores, los cuales hacen el medio físico

entre un equipo de terminación de línea (LTE) y el próximo. LTE usualmente significa nodos de conmutación y multiplexaje. Un multiplexor en el fin de la línea también termina el fin de sección de la línea.

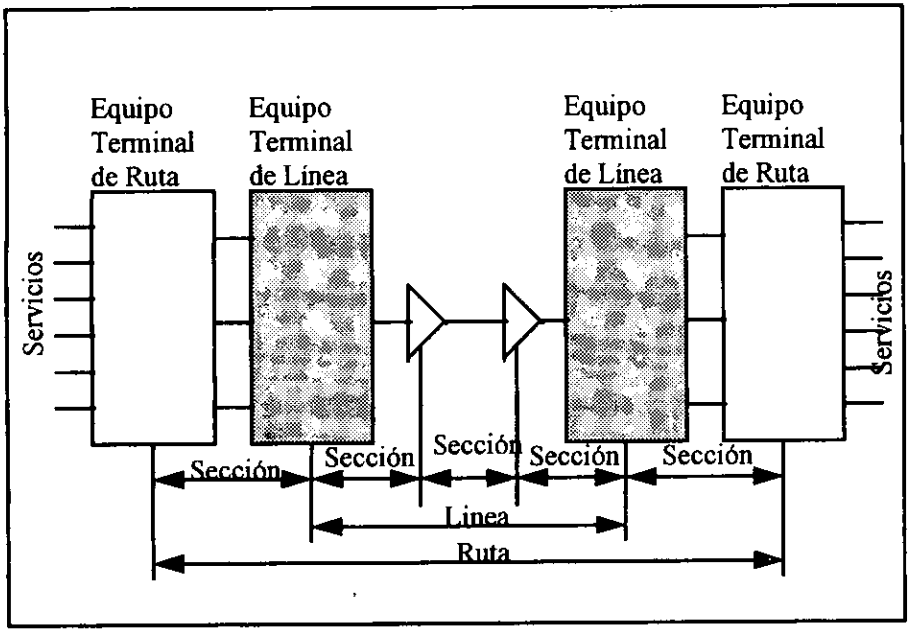


Figura 5.15. Alcances de la red SONET.

- **Capa de ruta.**
  La capa de ruta negocia el transporte de servicios (por ejemplo, DS1 o DS3) entre equipos de terminación de ruta (PTE). La función principal de la capa de ruta es mapear los servicios del encabezador de ruta (POH) en una envoltura de campo de información síncrona (SPE) de una STS, el cual es el formato requerido por la capa de línea. El encabezador de ruta usa apuntadores para identificar el inicio de señales DS1 o DS3. Los canales del encabezador de ruta son definidos en cada trama y subtrama que representa un agregado de canales más bajos. Una ruta puede ser menos que la capacidad de la línea completa. Pero hay también POH dedicado a cada
  carga útil STS-1. El POH permanece intacto con su trama o subtrama a medida que ellos son conmutados, y multiplexados en velocidades agregadas más rápidas, o de otro modo procesados. El POH termina en el dispositivo que toma la subtrama en datos individuales. El equipo de terminación de ruta

(PTE) también termina líneas y secciones pero en diferentes niveles lógicos.

Cada tipo de canal de los encabezadores se comunica con un nivel diferente de equipo para aislar fallas. La meta es tener la red entera administrable por la autoridad apropiada. La portadora dejará al cliente usar el POH para controlar el equipo de premisas de cliente (CPE). Pero los switches de la portadora serían administrados con LOH.

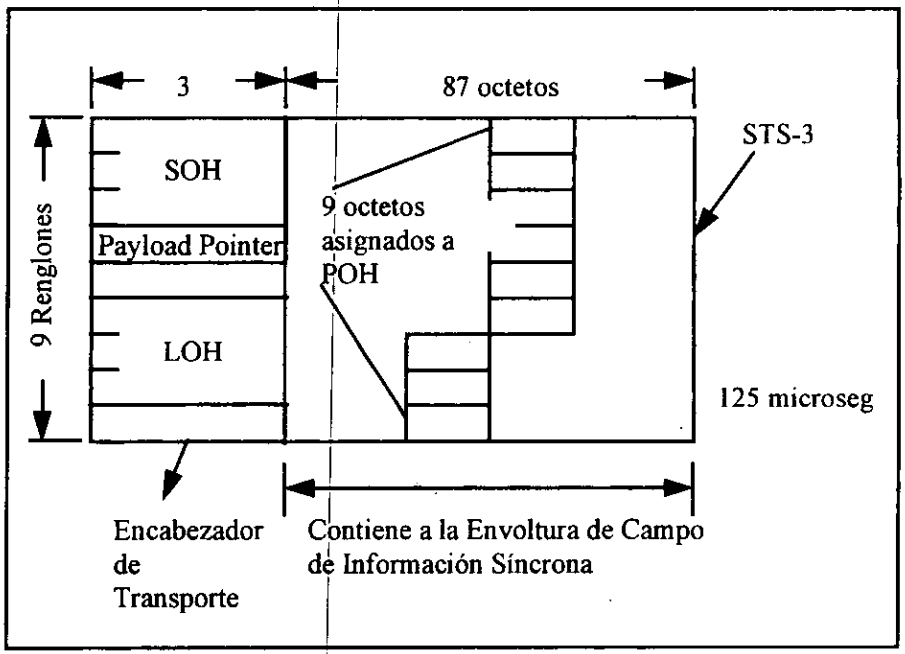


Figura 5.16. Trama SONET STS-1

La señal de transporte síncrona (STS) es la versión eléctrica de la señal SONET, la cual está definida únicamente para fibra. STS-1 es equivalente a OC-1, aquí la velocidad manejada es 51.84 Mbps. SONET es algunas veces asociado con "paquetes", SONET es en realidad un formato de entramado que puede llevar cualquier clase de tráfico (E1, T1, DS3, celdas ATM), y es una forma de TDM. La idea de definir una nueva forma de TDM (PDH ya existía) es soportar el futuro crecimiento en telecomunicaciones de todo tipo y ofrecer la flexibilidad demandada por el incremento de usuarios sofisticados (ATM).

SONET tiene la misma base de tiempo de PDH, es decir el tiempo tomado para enviar una trama OC es 125 microsegundos, el mismo tiempo que toma enviar una trama E1 o T1. La trama SONET OC se repite 8000 veces por segundo, sin importar la velocidad agregada. La trama básica de transmisión SONET es STS-1, ilustrada en la figura 5.16. Dicha trama está compuesta por 90 columnas y 9 renglones. Cada columna es de 1 byte, y cada byte de 8 bits. Esto da 810 bytes por trama, que transmitidos en 125 microsegundos da una velocidad de 51.84 Mbps. Este ancho de banda está compuesto por ancho de banda de carga útil y ancho de banda dedicado a encabezadores.

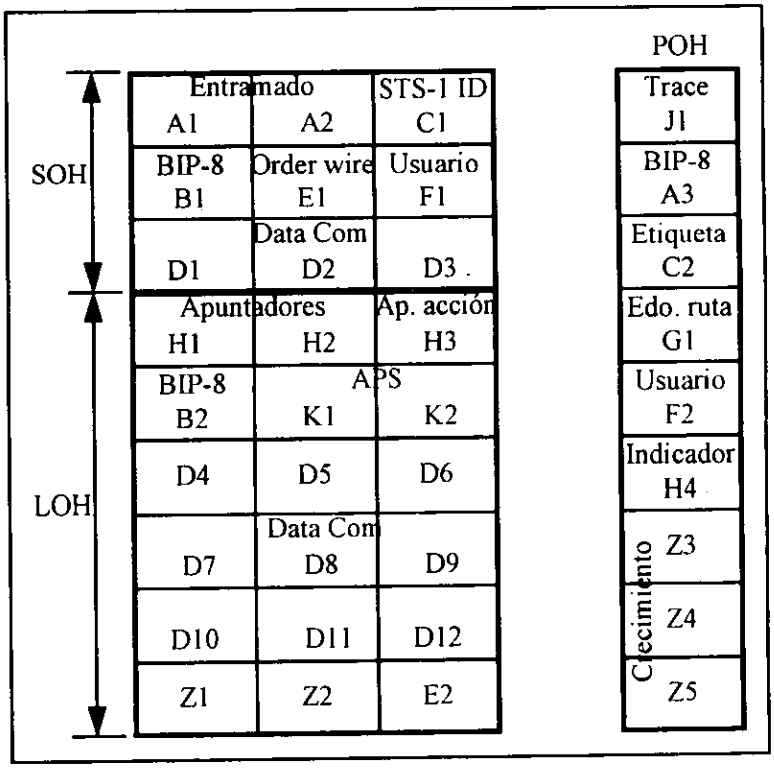


Figura 5.17. Encabezadores de la trama STS-1.

♦ ENCABEZADORES

Los encabezadores de la trama STS-1 de sección, línea y ruta se muestran en la figura 5.17.

♦ Encabezadores de ruta

Los encabezadores de ruta de la trama STS-1 hacen funciones tales como
- Transporte de servicios de extremo a extremo.
- Secuencia de celdas.
- Ver el estado del elemento de terminación de ruta.
- Detección de errores.
- Funciones definidas por el usuario.

El POH de la trama SONET consiste de 9 bytes de la STS-1. El POH es llevado dentro de la SPE de la STS y sus encabezadores son:

- **J1** El byte J1 es usado para transmitir repetidamente información. Este consiste de largo fijo, tal que una conexión continua a la fuente de la señal de ruta puede ser verificada en cualquier terminal de recepción a lo largo de la ruta.
- **B3** El byte B3 provee detección de error de ruta con BIP-8 (Bit Interleaved Parity) que es un código de chequeo de errores. El BIP-8 es calculado sobre todos los SPE previa y puesto en el byte B3 antes de mezclar el SPE (Envoltura de Carga Util Sincrona) y el POH.
- **C2** El byte C2 indica la construcción de la SPE de la STS por medio de un valor asignado de una lista de 256 valores (8 bits).
- **G1** El byte G1 sirve para regresar al equipo de terminación de ruta (PTE) de la STS, el estado y desempeño de la terminación de ruta.
- **F2** Este byte es utilizado para propósitos de usuario entre terminaciones de ruta.
- **H4** Este byte provee una indicación de fase de multitrama para carga útil de tributarias virtuales.
- **Z3** a **Z5** Son reservados para uso futuro.

♦ Encabezadores de línea.

Las funciones generales de los encabezadores de línea son:
- Comunicaciones entre equipos terminales de línea.
- Sincronización entre LTE´s.
- Localización de la carga útil (campo de información).
- Multiplexaje.

- Detección de errores.
- Conmutación de protección automática.

Cada uno de los bytes se listan a continuación:

- **H1** a **H3** Estos tres facilitan la operación del apuntador de carga útil y son provistos para todas las STS-1 de la STS-n.
- **B2** Este byte provee monitoreo de errores de línea con BIP-8. El BIP-8 es calculado sobre todos los bits del encabezador de línea y la capacidad del campo de información de la trama STS-1 previa, y el valor calculado es colocado en el byte B2 antes de mezclarse. Este byte es provisto para todas las tramas STS-1 de la trama STS-n.
- **K1** a **K2** Estos do bytes proveen señalización de protección automática (APS) entre equipos de terminación de línea. Estos bytes son definidos únicamente para una STS-1 en una STS-n.
- **D4** a **D12** Estos 9 bytes proveen un canal de comunicación de datos a 576 Kbps para mensajes de administración, monitoreo, mantenimiento y alarmas, y otras necesidades de comunicación entre equipos de terminación de línea. Estos bytes son definidos únicamente para la STS-1 de la STS-n.
- **Z1** a **Z2** Estos bytes están reservados para uso futuro.
- **E2** Este byte provee un canal de comunicaciones de voz entre el equipo terminal de línea y está únicamente definido para STS-1 de una señal STS-n.

♦ **Encabezadores de sección.**

Las funciones de los encabezadores de sección son:

- Alineación de trama.
- Identificación de la trama STS-1.
- Canal de comunicaciones de datos.
- Comunicación de voz.
- Canal de usuario.

- **A1** y **A2** Estos dos bytes proveen un patrón de alineación de trama (11110110, 00101000). Estos bytes son provistos en todas las STS-1 dentro de la trama STS-n. Estos bytes identifican el inicio de la trama SONET STS-1.
- **C1** Este byte es puesto a un número binario correspondiente a su orden de aparición en la trama STS-n. Este byte es provisto en todas las tramas STS-1 dentro de la trama STS-n y en el primer STS-1 se pone a 00000001.
- **B1** Este byte provee monitoreo de errores de sección con BIP-8 usando paridad par. El BIP-8 es calculado sobre todos los bytes de la trama STS-1

previa y el valor obtenido es colocado en B1 de la trama STS-1 antes de mezclarse.

- **E1** Este byte provee un canal de comunicación de voz entre regeneradores y elementos de red.
- **F1** Este byte es asignado para propósitos de usuario y es terminado en todo equipo a nivel de sección.
- **DI** a **D3** Estos bytes proveen un canal de comunicación de datos para mensajes de monitores, alarma, mantenimiento, etc. a 192 Kbps entre equipo de terminación de sección.

♦ **Concepto de SPE**

El formato de la envoltura de carga útil síncrona (SPE) se muestra en la figura 5.18. La carga útil es una trama flotante dentro de la estructura de la trama física. La SPE cabe exactamente dentro de una sola trama SONET, pero la SPE se le permite iniciar en cualquier lugar dentro de la trama física SONET y en este caso abarcará dos tramas físicas consecutivas, esto se ilustra en la figura 5.19. El inicio de la carga útil es apuntado por los bytes H1 y H2.

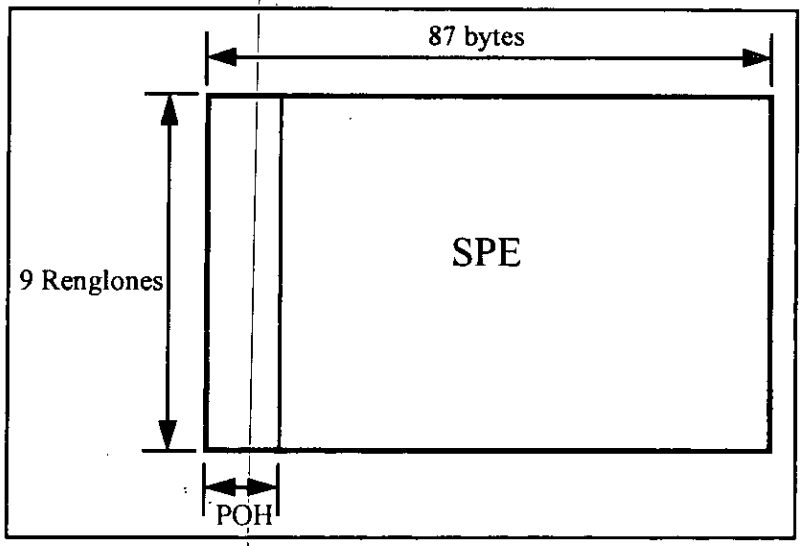


Figura 5.18. Envoltura de carga útil síncrona (SPE) de la STS-1.

Muy pequeñas diferencias en velocidades de reloj de la trama y la carga útil pueden ser acomodadas mediante el incremento o decremento temporal del

apuntador (un byte extra, si se necesita es encontrado en POH, el byte H3). Nunca diferencias grandes de reloj son acomodadas de esta forma.

En conclusión, básicamente los apuntadores permiten operación asíncrona en una red síncrona.

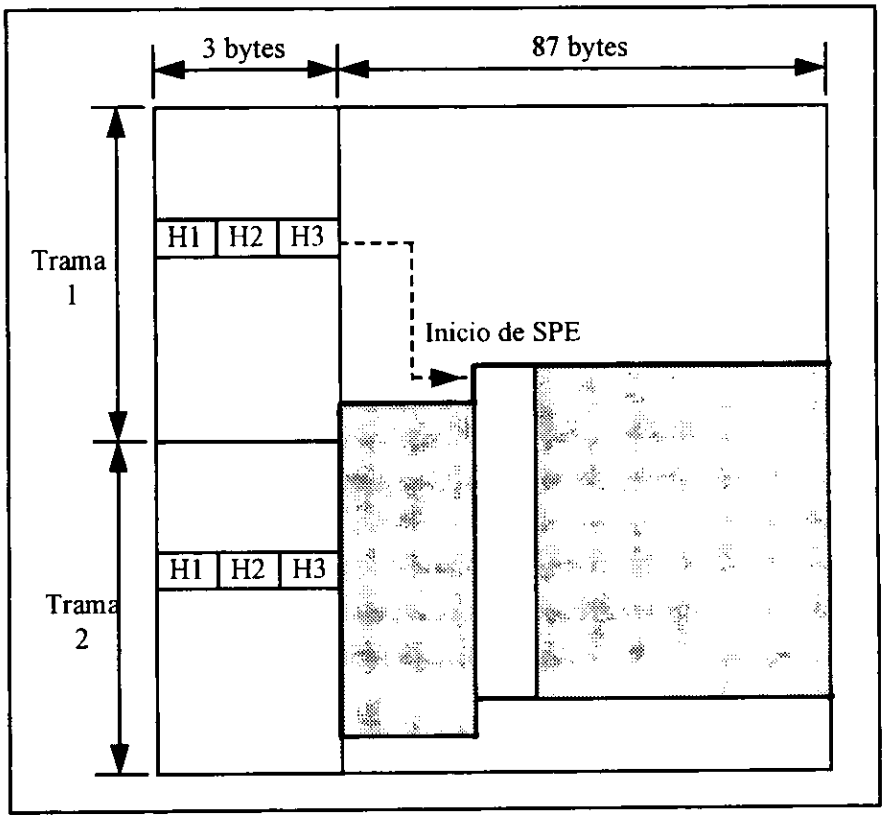


Figura 5.19. Tramas STS-1 consecutivas.

♦ **Trama STS-3c**

Múltipples tramas STS-1 pueden ser multiplexadas en bytes juntas, para formar señales de velocidad más alta. Cuando esto se hace se tiene lo que se llama STS-2, STS-3, etc. donde el número indica la cantidad de STS-1 presentes y por lo tanto la velocidad involucrada.

Un método alternativo es alinear en fase las múltiples tramas STS-1 y sus cargas útiles. Esto significa que una SPE más grande ha sido creada. Esto se

llama concatenación y es indicado en el nombre de la señal. Por ejemplo cuando tres STS-1 son concatenadas de tal forma que las tramas son alineadas en fase y hay una sola SPE más grande, esto es llamado STS-3c. El formato de esta trama se indica a a continuación.

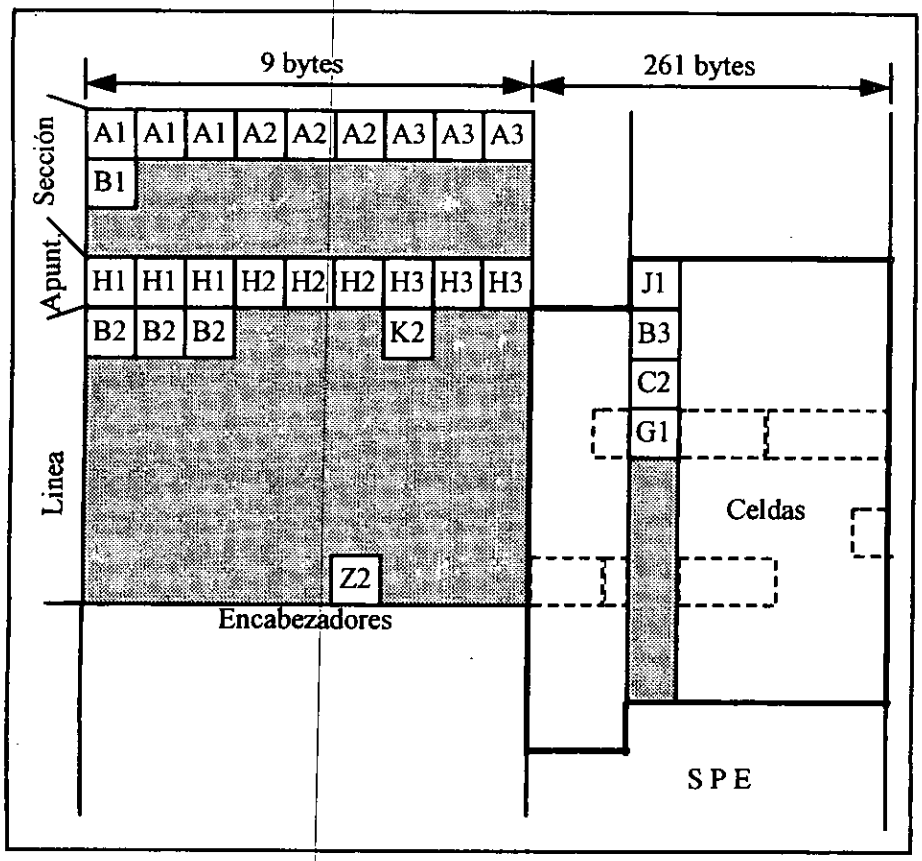


Figura 5.20. Trama STS-3c, como se definió en ATM UNI.

Dentro de SONET y la envoltura de carga útil síncrona STS-3c, el valor del apuntador (H1, H2) localiza el inicio de la SPE. Dentro de la SPE, H4 apunta a la primera celda de 53 octetos con el offset a su inicio; más tarde las celdas empiezan a intervalos de 53 octetos.

♦ **Tributarias virtuales**

A pesar de que la velocidad básica de SONET con STS-1 es 51.84 Mbps, también existen velocidades menores llamadas tributarias virtuales.

Al proceso de ensamblar la señal tributaria en la SPE se conoce como mapeo de carga útil. El ensamblaje de la tributaria se auxilia de bits de relleno para sincronizar las tributarias con la SPE. En el lado receptor se recupera la tributaria quitando los bits de relleno y el POH del SPE.

Como ejemplo, un DS3 puede ser mapeado directamente en una STS-1; o 28 VT 1.5 pueden ser mapeadas en 86 columnas de la capacidad de carga útil de la SPE de la STS-1, quedando en este caso dos columnas de sobra para ser ocupadas como bytes de relleno.

Tributarias Virtuales SONET	Contenedores virtuales de SDH	Velocidad SONET Mbps	Velocidad SDH Mbps
VT 1.5	VC-11	1.544	
VT 2.0	VC-12		2.048
VT 3.0		3.152	
VT 6.0	VC-2	6.312	6.312
	VC-3	44.736	34.368
	VC-4		139.264
STS-1		51.84	
STS-3	STM-1	155.52	155.52
STS-12	STM-4	622.68	622.68
STS-18	STM-6	933.120	933.120
STS-24	STM-8	1244.180	1244.180
STS-48	STM-16	2488.37	2488.37

Tabla 5.2 Tributarias vituales.

Las tributarias virtuales pueden operar en dos modos:

- **Modo flotante**

  Este modo ha sido diseñado para minimizar el retardo de la red y proveer un "cross-conection" eficiente de transporte de señales en el nivel de tributarias virtuales dentro de la red síncrona. Esta meta es conseguida permitiendo a la envoltura de carga útil (SPE) de la tributaria virtual flotar con respecto a la SPE de la STS-1, para evita el buffer de deslizamiento en cada "cross-conect" de tributaria virtual, entre sistemas de transporte diferentes sin retardo de red

no deseado. El problema esta en el modo de identificar el inicio de la VT debido a que a la fuente de la VT no es fija.

- **Modo cerrado**

Este modo ha sido diseñado para minimizar la complejidad de la interface y soportar transporte en masa de señales DS1 para aplicaciones de conmutación digital. Esto se consigue manteniendo la SPE de la VT en posiciones fijas con respecto a la SPE de la STS-1. Cada SPE de una VT 1.5 no es provisto con sus propios apuntadores de carga útil. No es posible enrutar una VT 1.5 seleccionada a través de una red SONET sin retardo de red no deseado y costo extra causado por la provisión de buffers de deslizamiento para conseguir las características de sincronización. Este modo tiene la ventaja de mapear VT´s en un lugar predefinido de la carga útil; la desventaja es el retardo y el uso ineficiente de la SPE.

5.2.2.3 Jerarquía Digital Síncrona

La jerarquía digital síncrona (SDH) es el plan de multiplexaje para la capa 1 del modelo OSI (Interconexión de Sistemas Abiertos) adoptado por la mayoría del mundo, excluyendo a Norte América. SDH está diseñado para ser compatible con SONET en el nivel OC-3. En realidad una trama STM-1 (Módulo de Transporte Síncrono 1) es equivalente a una trama STS-3c en estructura.

El transporte SDH es definido en términos del STM-1 en 155.52 Mbps. Pero como con SONET, hay unidades de ancho de banda más pequeñas, que en SDH se denominan *contenedores virtuales* (VC).

Las estructuras de las subtramas, SPE´s y multiplexaje son las mismas aunque la tecnología es diferente. Por ejemplo la nomenclatura y numeración de una VT SONET y un VC SDH. Los VC´s son numerados por nivel de señal digital más que por velocidad de bit usado por la nomenclatura de VT´s. Entonces el primer 1 en VC 11 de SDH significa DS1 y el segundo 1 significa 1.5 Mbps. VC 12 es de nivel 1 y 2 Mbps o E1. En SONET estos contenedores virtuales se traducen a las tributarias virtuales VT 1.5 y VT 2.

Existen otras diferencias substanciales:

- En SDH el concepto de línea (línea de SONET) se pierde. En SDH una línea es únicamente el cable entre los dos dispositivos, lo que SONET llama

sección. El encabezador de línea LOH es llamado SOH y la posibilidad de encabezadores dedicados a subsecciones transparentes está aún bajo estudio

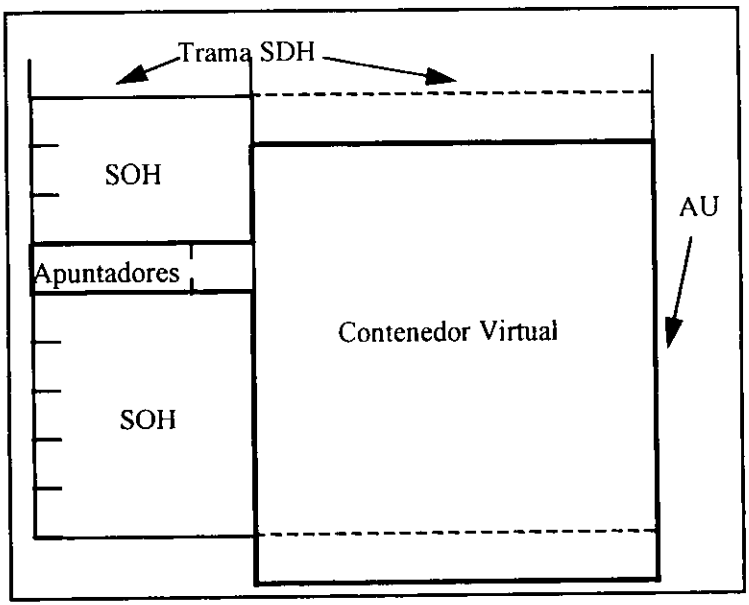


Figura 5.21. Unidad adminitrativa SDH.

- Consecuentemente, los octetos de encabezadores en la trama STM-1 están divididos entre encabezadores de sección y apuntadores, más que en SOH y LOH de SONET.

- Separar los apuntadores (H1, H2, H3) de SOH permite una unión lógica de apuntadores y el contenedor virtual que ellos apuntan. Un VC grande puede corresponder a una SPE . La combinación de VC y apuntadores hace una unidad tributaria (TU) SDH o unidad administrativa (AU) SDH.

- La "unidad" refleja el hecho de que una justificación negativa. El tercer octeto apuntador (H3) lleva datos y actúa como parte del VC.

- El STM-1 de SDH contiene únicamente un byte C1, identificador de subtrama, debido a que hay únicamente un AU en la trama STM-1. En la trama SONET del mismo tamaño puede haber tres tramas SONET STS-1 cada

una con un identificador. Por lo tanto dos o más bytes C1 pueden ser requeridos por SONET en la columna 8 y 9 del renglón 1 (inmediatamente después de C1 que está siempre presente). Sin embargo una STM-1 es idéntica a una STS-3c. Un nodo que soporte STM-1 y 0C-3 puede cruzar canales en ambos lados. Si el nodo es un switch ATM, este podría terminar líneas y secciones, y conmutar celdas.

5.2.2.4 Mapeo de celdas ATM

♦ **Celdas en STS-3c**

El mapeo SONET es ejecutado directamente en la STS-3c SONET (155 Mbps). Las celdas ATM se vacían en la carga útil continuamente, dado que un número entero de 53 octetos no cabe en una trama STS-3c. Esto resulta en mejor eficiencia que llevar DS3´s mapeados o VT 1.5 multiplexados sobre SONET. El canal de comunicación de datos en el encabezador no es usado en la UNI.

Cuando la STS-3c lleva celdas ATM, el byte C2 (etiqueta de la señal) en el POH, es puesto a 00010011. Este valor está siendo estandarizado por el Instituto Nacional de Estándares Americanos (ANSI). Otras formas de tráfico son indicadas con otros códigos. Los apuntadores H1 y H2, en la trama STS-3c, identifican la localización del primer byte en la SPE SONET, llevada dentro de la trama SONET como un offset de H3. Únicamente 10 bits de H1 y H2 son usados para apuntar como el SPE siempre inicia en el primer STS-1 o en el primero de los tres del STS-3c.

Dentro de la SPE hay una columna de POH (encabezador de ruta). En el resto de la SPE las celdas siguen una de otra, en intervalos de 53 bytes. El byte H4 es otro apuntador, en el POH, seis bits de los cuales indican el inicio de una celda como un offset en bytes desde H1. Únicamente 6 bits se necesitan, ya que siempre habrá un inicio de celda dentro de 53 bytes. El apuntador H4 cambia con cada trama SONET.

Las celdas también pueden ser transportadas sobre VT DS1 ó VT DS3 puestas dentro de un bloque de carga útil más pequeño dentro del la SPE SONET. En este caso el apuntador H4 localiza la VT y no el inicio de la celda. En una VT sería necesario, recurrir al método del HEC para delinear celdas.

La velocidad de transferencia de celdas es de 149.760 Mbps. La forma en que se depositan celdas ATM en la STS-3c se muestra en al figura 5.22.

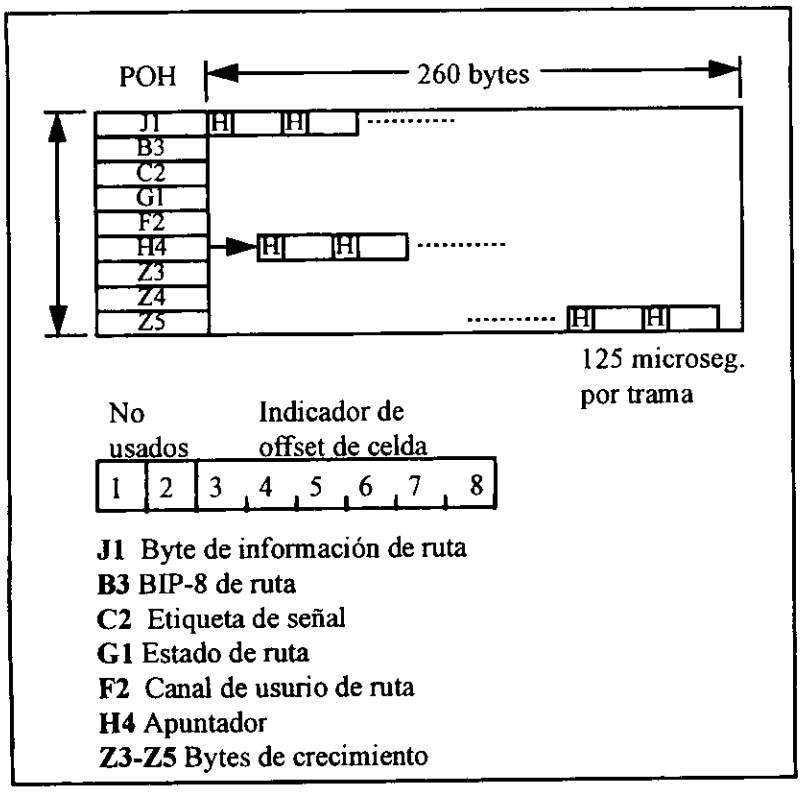


Figura 5.22. Mapeo de celdas ATM en el campo de información de una señal STS-3c de SONET.

♦ **Celdas ATM sobre DS3**

El servicio de transmisión a 45 Mbps ofrecido en Norte América. maneja celdas ATM mediante la adición del Protocolo de Convergencia de Capa Física (PLCP) en la subcapa de convergencia de transmisión. El PLCP es un subconjunto del PLCP definido previamente para celdas SMDS. Figura 5.23.

El PLCP es intentado para servicio T-3 de tal forma que se pueda remover el relleno variable del estándar T3 cuya velocidad adapta 28 T1´s mientras permite relojes no sincronizados ligeramente. En el mapeo ATM, PLCP ejecuta la adaptación de velocidad mediante relleno opcional con "nibbles" adicionales de 4 bits, al final de cada trama PLCP. Debido a los encabezadores, el througput

máximo de celdas es 40.704 Mbps. Los bytes A1 y A2 (11110110 y 00101000) son para sincronización.

En T-3 la carga útil de la celda no es mezclada . El byte C1 alerta al receptor si un relleno ocurre (13 o 14 "nibbles" en el "trailer"). Figura 5.23.

Un chequeo BIP es incluido en el byte B1. BIP-x (Bit Interleaved Parity / Paridad Intercalada de Bit) es un método de chequeo de errores donde cada x bits es paridad de cada x^{th} bit en un bloque de datos (x=8 en SONET, 16 en ATM). Para el caso de DS3 cada bit en ese campo refleja una paridad par en todos los bits en la misma posición (1-8) de los bytes en la trama previa PLCP. Excluyendo a los bytes A1, A2 y P.

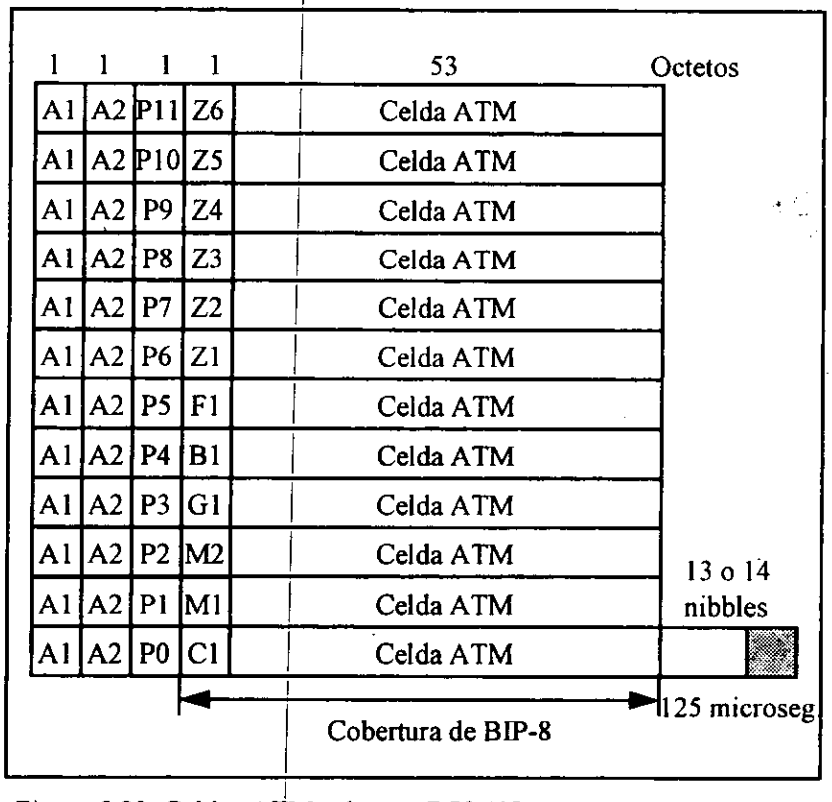


Figura 5.23. Celdas ATM sobre un DS3 (45 Mbps).

El byte G1 lleva dos campos de alarmas:

- **FEBE**
  Errores de bloque de extremo lejano (FEBE), en los primeros 4 bits (0000 y1000 binario) en el previo BIP-8 que no cuente con el chequeo de paridad par. Un FEBE de 1111 es usado para indicar BIP/FEBE no activo.

- **RAI**
  Indicación de alarma remota, el quinto bit de G1 es regresado en ON cuando alguna falla ocurre.

Los bytes P son indicadores de encabezador de ruta (POH). Cada uno tiene un valor diferente para identificar el campo en el encabezador de ruta de la trama PLCP que sigue inmediatamente. En la figura 5.23 se tiene el PLCP para celdas ATM en un DS-3 (45 Mbps) plesiócrono. Incluye relleno ajustable (13 ó 14 "nibbles") para acomodar diferencias de reloj entre SONET y PDH.

Valor de subtrama PLCP	Byte C	Nibbles
1	11111111	13
2	00000000	14
3	01100110	13 (no relleno)
	10011001	14 (rellenado)

Tabla 5.3. Control de relleno en la trama PLCP DS-3.

- **Celdas sobre T1**
  El mapeo de celdas ATM en un T1 es como se muestra en la figura 5.24.

La trama PLCP DS1 es llevada dentro de la carga útil de la supertrama extendida citada en la sección de PDH, y cada bit siguiendo un bit-F es el inicio de un byte PLCP. La trama PLCP DS1 puede empezar dentro de cualquier byte dentro de la carga útil de la supertrama extendida (ESF). La trama contiene 4608 bits, lo cual es exactamente el tamaño de la carga útil de la ESF (192 x 24 = 4608). Por lo tanto, el periodo de la trama PLCP DS1 es 3 ms. Como se ve esta trama es muy similar a la trama DS3, solo 10 celdas son empaquetadas en una trama PLCP DS1, se eliminan dos de los encabezados Z; el relleno de la trama es está fijo a 6 bytes.

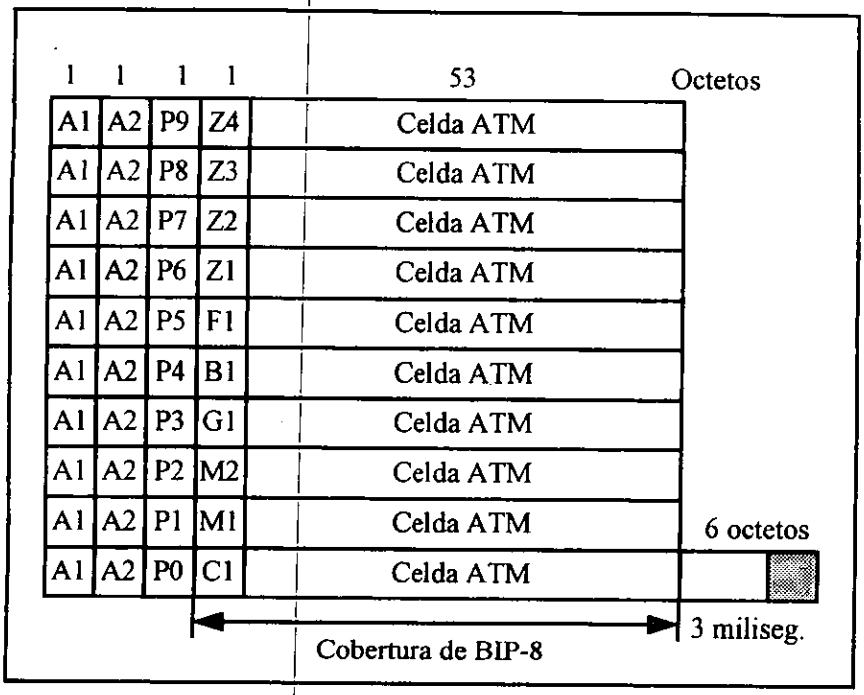


Figura 5.24. Trama PLCP T1 para celdas ATM.

♦ **Celdas ATM sobre un E1**

El sistema de entrama do para un E1 a 2 Mbps tiene dos variantes: una que proyecta celdas dentro de un caudal de bits E1 y otra que utiliza una trama PLCP para celdas SMDS.

En la figura 5.25 se muestra una trama PLCP para celdas SMDS, la cual puede ser utilizada para llevar celdas ATM. El formato es muy similar a la trama PLCP DS1, pero en este caso la trama consiste de 10 renglones de 57 bytes.

Las primeras dos columnas, el patrón de entramado de 16 bits y la identificación de renglón son idénticas con la trama PLCP DS1. La próxima columna es en gran parte la misma, y tiene únicamente dos diferencias. El byte F1 es reservado para estandarización futura de comunicación entre los puntos en que circula la trama PLCP E1. El byte F1 es puesto a ceros. Ningún relleno es necesitado en la trama PLCP E1

Dado que no hay que indicar algún tipo de relleno, el byte C1 no tiene función y es puesto a ceros. La trama PLCP E1 contiene 4560 bits, los cuales

corresponden a la carga útil de 19 tramas E1 (no contando el TS0 y el TS16). Por lo tanto, el periodo de la trama PLCP E1 es de 19x125 microsegundos = 2.375 ms.

1111011000101000	00100101	00000000	Celda ATM
1111011000101000	00100000	00000000	Celda ATM
1111011000101000	00011100	00000000	Celda ATM
1111011000101000	00011001	00000000	Celda ATM
1111011000101000	00010101	F1	Celda ATM
1111011000101000	00010000	B1	Celda ATM
1111011000101000	00001101	G1	Celda ATM
1111011000101000	00001000	M2	Celda ATM
1111011000101000	00000100	M1	Celda ATM
1111011000101000	00000001	C1	Celda ATM
2 bytes	1 byte	1 byte	53 bytes

B1 Paridad intercalada de bit (BIP)
G1 Estado de la trama PLCP
M1, M2 Usado sólo en SMDS
C1 Contador de relleno

Figura 5.25. Formato de la trama PLCP E1.

5.2.2.5 Funciones de la capa física ATM

La capa física ATM provee transmisión de celdas sobre un medio físico que conecta dos dispositivos ATM. La capa física está dividida en dos subcapas: la capa dependiente del medio físico (PDM) y la subcapa de convergencia de transmisión.

- **Subcapa PDM**

La subcapa PDM provee capacidad de transmisión de bit, por sí misma provee codificación de línea y si es necesario conversión óptico-eléctrica. La capa física define el medio físico de transmisión como: fibra, coaxial y UTP; así

como sincronización a nivel de bit.

Hay tres cuerpos de estándares, que han definido la capa física para ATM: el Instituto Nacional de Estándares Americanos (ANSI), la Unión de Telecomunicaciones Internacional -Telecomunicaciones (ITU-T) y el Forum ATM.

- **Estándares ANSI**

El estándar ANSI T1-624 define tres interfaces ATM basadas en SONET sobre fibra monomodo para ATM UNI:
- STS-1 a 51.84 Mbps.
- STS-3c 155.52 Mbps.
- STS a 622.08 Mbps.

ANSI también define operación a la velocidad DS3 de 44.736 Mbps usando el protocolo de capa de convergencia física (PLCP) del estándar 802.6 de la IEEE.

- **ITU SDH**

La recomendación I.432 de la ITU-T define dos interfaces físicas basadas en SDH para ATM, estas son:
- STM-1 155.52 Mbps.
- STM4 a 622.08 Mbps.

ITU-T estandariza interfaces físicas eléctricas adicionales, entre ellas tenemos:
- DS1 a 1.544 Mbps.
- E1 a 2.048 Mbps.
- DS2 a 6.312 Mbps.
- E3 a 34.368 Mbps.
- DS3 a 44.736 Mbps usando PLCP.

- **Interface del Forum ATM**

El Forum ATM ha definido cuatro velocidades de interface de capa física. Dos de ellas son interfaces para redes públicas, y son: la DS3 y la STS-3c estandarizadas por ANSI e ITU-T. La interface STS-3c de SONET puede ser soportada en un OC-3, ya sea en fibra monomodo o multimodo. Las siguientes tres velocidades de interface y medio son para aplicación de red privada:
- FDDI a 100 Mbps.
- Fiber Channel a 155.52 Mbps.
- STP a 155 Mbps.

El Forum ATM está especificando transmisión de celdas ATM sobre UTP nivel

3 y 5.

♦ **Subcapa de Convergencia de Transmisión**

Esta subcapa es la segunda capa de la capa física y ejecuta las siguientes funciones:

- **Desacople de la velocidad de celda**

  La subcapa TC ejecuta un desacople de velocidad de celda. El medio físico que es síncrono (DS3, SONET, SDH), requieren de esta función mientras que un medio asíncrono como FDDI no la requiere.

  Para entender esta función, se debe saber que hay dos tipos de celdas relacionadas: celdas desocupadas o no asignadas y celdas asignadas. Estas últimas son generadas en la capa ATM. En la figura 5.26 se muestra la operación entre los dos dispositivos.

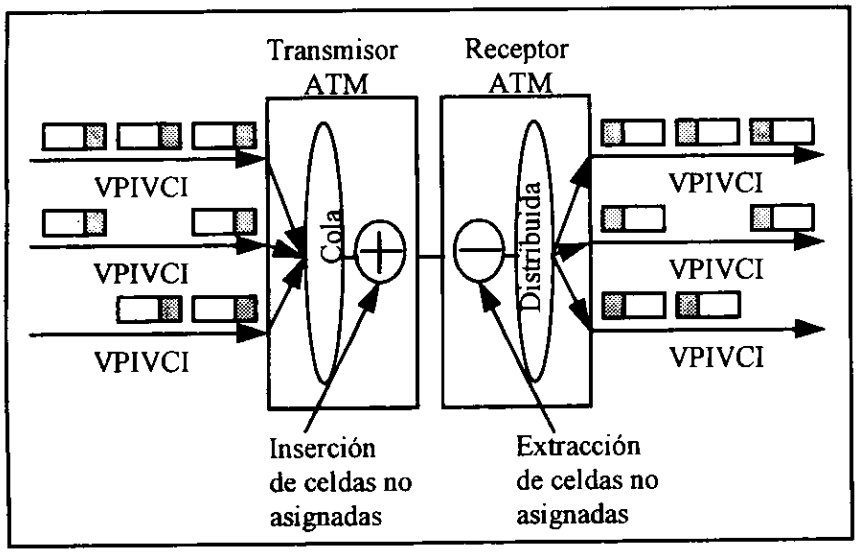


Figura 5.26. Desacople de velocidad de celda.

La transmisión multiplexa múltiples ráfagas de celda VPI/VCI poniéndolas en una cola de espera, si un "slot ATM" no está disponible inmediatamente. Si la cola está vacía, debido a que no hay celdas para transmitir, para llenar la próxima "ranura ATM" de celda síncrona, entonces la subcapa TC inserta celdas desocupadas y distribuye las otras celdas asignadas a sus destinos.

La recomendación I.321 coloca esta función en la subcapa TC de la capa física, usa celdas desocupadas, mientras que el Forum ATM coloca esta función en la capa ATM y usa celdas no asignadas.

- **Verificación del HEC.**

  El HEC es un código de 1 byte aplicado al encabezador (4 bytes) de la celda ATM. El código HEC es capaz de corregir errores de un sólo bit en el encabezador. Este también es capaz de detectar muchos patrones de errores multibit. La subcapa TC genera el HEC en la transmisión y lo usa para determinar si el encabezador tiene un error. Si los errores son detectados en el encabezador, entonces la celda recibida es descartada. Dado que el encabezador le dice a la capa ATM que hacer con la celda, es muy importante que no tenga errores; si así fuera podría ser entregada a un usuario erróneo.

  La subcapa TC también usa el HEC para localizar celdas cuando ellas son mapeadas directamente en el campo de información de un sistema de transmisión TDM. El HEC no encontrará relación de los datos aleatorios de la carga útil de la celda cuando los 5 bytes que están siendo checados no son parte del encabezador. Así, esto puede ser usado para encontrar celdas en una flujo de bits recibidos. Una vez que varios encabezadores de celdas han sido localizados a través de sus del HEC, entonces la subcapa TC sabe que tiene que esperar 53 bytes de una celda. Este protocolo es llamado delineación de celdas basado en HEC.

- **Adaptación a la trama de transmisión**

  Esta adaptación es responsable por todas las acciones necesarias para adaptar el flujo de celdas de acuerdo a la estructura de la carga útil del sistema de transmisión, usada en la dirección de la transmisión. En la dirección opuesta, se hace el proceso inverso. La estructura de la carga útil puede ser una SPE de SONET o una trama PLCP.

- **Generación y recuperación de la trama de transmisión**

  La más baja de la funciones es la generación y recuperación de la trama de transmisión. Su función básica es generar la tramas requeridas para que las celdas ATM puedan ser mapeadas. El tamaño de la trama depende de la velocidad de transmisión. En el lado de recepción, la recuperación de la trama es ejecutada de tal forma que las celdas ATM puedan ser identificadas y recuperadas de la envoltura de la carga útil.

5.2.3 CAPA ATM

Esta capa contiene características independientes del medio físico. Las funciones provistas por esta capa pueden ser categorizadas como sigue:

- Control de flujo genérico.
- Generación del encabezador.
- Multiplexaje.
- Traslación de VPI/VCI.

En la dirección de transmisión la capa ATM multiplexa celdas de rutas virtuales individuales y canales virtuales individuales en flujo de celdas compuesto. En la dirección de recepción, demultiplexa las celdas del flujo de celdas compuesto a la ruta virtual o canal virtual apropiado. También los campos VPI/VCI en la celda entrante pueden requerir mapeo a nuevos valores VPI/VCI, según la tabla de conmutación del switch ATM. La capa ATM genera el encabezador ATM y lo adhiere al campo de información para su transmisión o extrae el campo de información de una celda recibida y pasa ese campo de información a la próxima capa más alta. Finalmente la capa ATM puede generar celdas para llevar información de control de flujo genérico.

A continuación se detalla cada una de sus funciones:

- **Control de flujo genérico.**
  La función de control de flujo genérico (GFC) está definida únicamente para la interface usuario-red (UNI) para proveer control de flujo de acceso (al medio, cuando se proyecta celdas en medio compartidos). Este soporta flujo de tráfico ATM desde una red cliente ó un equipo terminal.

- **Generación y extracción del encabezador de celda.**
  Esto es hecho en los puntos terminales de la información en la capa ATM. En la dirección de la transmisión, después de recibir el campo de información de la celda ATM de la capa de adaptación ATM (48 bytes), el encabezador de la celda es adherido excepto por el byte de chequeo de errores de encabezador (HEC). El VPI y VCI que son parte del encabezador de la celda, son obtenidos del identificador de punto de acceso al servicio (SAP). En la dirección de recepción, el encabezador de la celda ATM es extraído y el campo de información de la celda es llevado a la capa de adaptación ATM (AAL). Únicamente el campo de información de la celda es pasado a la capa AAL.

Aquí los VPI/VCI son trasladados a un valor de SAP (Punto de Acceso al Servicio).

- **Traslación de VPI/VCI.**
  La traslación de VPI/VCI es la base de la conmutación ATM. Esa traslación es ejecutada en los nodos de conmutación ATM. En un switch de ruta virtual (VP), los VPI entrantes dentro de la celda son trasladados en nuevos valores VPI salientes. Aquí, los valores VCI dentro de los VPI son conservados. En switch de canales virtuales (VC), los valores de VPI así como los valores de VCI son trasladados. El switch VP es llamado "cross-conetc" ATM y el switch VC es llamado un switch ATM. No es necesario que los valores VPI/VCI sean trasladados sólo porque el tráfico pasa a través de un switch.. Uno puede conservar los valores VPI/VCI de extremo a extremo, si es necesario.

- **Multiplexaje y demultiplexaje de celdas.**
  En la dirección de la transmisión, las celdas de VP's y VC's individuales son multiplexadas en un flujo de celdas resultante. El flujo compuesto de celdas es normalmente continuo (gracias a celdas ociosas insertadas). En el lado de recepción, las celdas son demultiplexadas y cada una de ellas fluye en un VP y VC apropiado a su destino.

5.2.3.1 Conexiones ATM

ATM ofrece dos tipos de conexiones:

♦ **Circuitos virtuales conmutados (SVC's)**

Un circuito virtual conmutado opera como una llamada telefónica de voz convencional. Un host se comunica con su switch ATM para solicitar que el switch establezca un SVC. El host especifica la dirección completa de una computadora remota y la calidad de servicio solicitado. Entonces el host espera una señal de la red ATM para crear un circuito. El sistema de señalización ATM establece y define un trayectoria desde el host local hasta el host remoto. La computadora remota debe acordar la aceptación del circuito virtual.

Durante la señalización, cada switch ATM, a lo largo de la ruta, examina la calidad de servicio solicitado para el circuito. Si se acuerda enviar datos, un switch graba información sobre el circuito y envía la solicitud hacia el próximo switch en la ruta. Cuando la señalización se completa, el switch ATM local

reporta el éxito de la operación hacia ambos lados del circuito virtual conmutado.

La interface UNI ATM se vale de 24 bits en el encabezador de la celda ATM para identificar cada circuito virtual. Cuando un host crea o acepta un circuito virtual nuevo, el switch ATM local asigna un identificador para el circuito. El paquete transmitido a través de la red ATM no contiene direcciones de fuente y destino. De hecho, un host etiqueta cada paquete que sale y el switch etiqueta cada paquete entrante con un identificador de circuito.

La comunicación entre dos vías requiere que se reserven recursos a lo largo de la ruta inversa así como en la ruta de envía.

♦ **Circuitos virtuales permanentes**

En un circuito virtual permanente, un administrador interactúa con los switches ATM para configurar los circuitos virtuales a mano. El administrador especifica la fuente y el destino del circuito, la calidad de servicio que el circuito recibirá y los identificadores que cada host utiliza para accesar al circuito. Aun cuando los circuitos virtuales conmutados proporcionan accesabilidad, los circuitos virtuales permanentes son importantes por tres razones. En primer lugar, hasta que todos los vendedores acuerden un mecanismo de señalización estándar, los switches que provengan de diferentes vendedores deberán valerse de PVC's para operar entre si. En segundo lugar, PVC puede emplearse en líneas arrendadas. Por último, los PVC's pueden utilizase en redes de mantenimiento y depuración.

5.2.3.2 Interfaces ATM

La interface usuario-red (UNI) conecta la red ATM y el equipo del cliente, el cuál puede incluir un switch ATM. Hay dos tipos de UNI's: pública y privada. La UNI pública conecta un switch ATM privado a una red del proveedor de servicio ATM público. Un UNI privada conecta usuarios ATM con un switch ATM.

La interface red-red (NNI), describe la interconexión de switches dentro de una red ATM ó entre dos redes ATM. El Forum ATM llama a la NNI que interconecta portadoras ATM públicas una interface inter-portadora de banda ancha (BICI por sus siglas en inglés). La ubicación de las interfaces ATM se muestran en la figura 5.27.

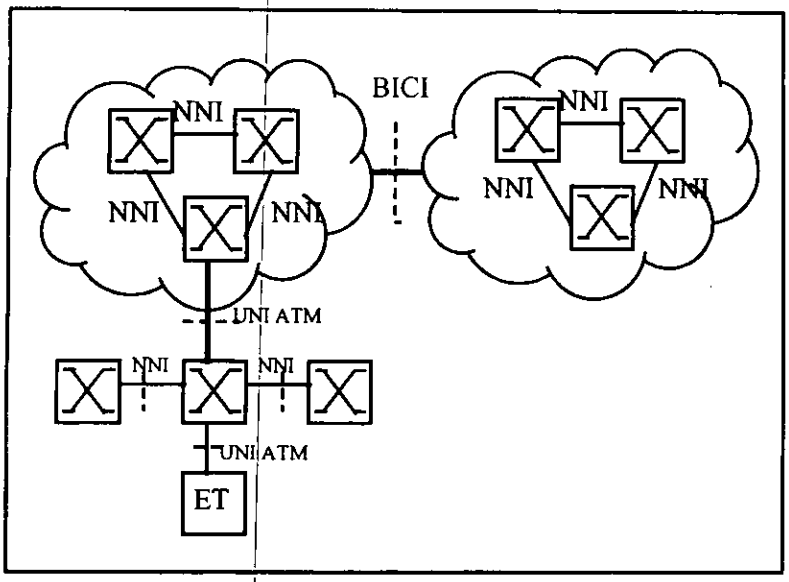


Figura 5.27. Interfaces ATM.

5.2.3.3 Estructura de la celda en UNI y NNI

Dos tipos de celdas existen respecto de los tipos de interfaces: la celda en la UNI y la celda en la NNI. El formato de la celda en la interface UNI se muestra a continuación, figura 5.28.

Como puede verse, el encabezador de la celda ATM se divide en varios campos, estos son:

- **Control de Flujo Genérico (GFC)**

Es un campo de 4 bits que puede proveer funciones locales, tales como control de flujo. Este campo tiene significancia local y no de extremo a extremo. Y es sobrescrito por switches ATM intermedios. La especificación UNI 3.0 establece que el host que transmite llenaría este campo con 0000.

- **Identificador de Ruta Virtual (VPI)**

El identificador de ruta virtual (VPI) es un campo de 8 bits (en la UNI) que identifica una ruta virtual dentro de una ruta física y es usado para establecer una conexión de ruta virtual (VPC) para uno o más VCI's equivalentes

lógicamente en términos de ruta y características de servicio. El VPI permite direccionamiento de red simplificado. El VPI tiene 8 ó 12 bits dependiendo de la interface (UNI ó NNI). El VPI es usado en el establecimiento de conexiones de ruta virtual de extremo a extremo de múltiples segmentos de ruta virtual. Una ruta virtual contiene múltiples canales virtuales.

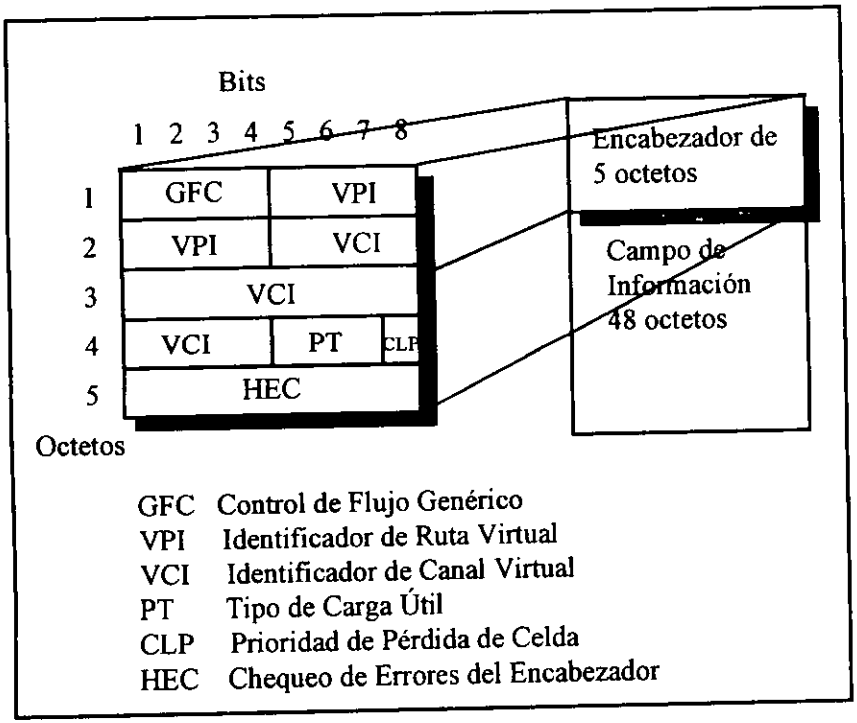


Figura 5.28 Estructura de la celda ATM en la interfaz UNI.

- **Identificador de Canal Virtual (VCI).**

Es un campo de 16 bits que identifica el canal virtual dentro de una ruta virtual a través de la interface. El VCI es usado para establecer conexiones, usando tablas de translación en los nodos de conmutación, que mapea un VCI entrante a un VCI saliente. Los circuitos establecidos usan conexiones VCI que son referidos como circuitos virtuales, y conexión de extremo a extremo llamado conexión virtual. La especificación UNI define algunos valores de VPI/VCI para funciones específicas, tales como meta-señalización, usada para establecer el canal de señalización; señalización punto a punto; y celdas de Operaciones de

Administración y Mantenimiento (celdas OAM). Algunos ejemplos de valores preasignados de VPI/VCI:

Función	VPI	VCI
No asignadas y ociosas	0	0
Meta-señalización	0	1
Flujo F4 (Datos de segmento)	0	3
Flujo F4 (Datos de extremo a extremo	0	4
Señalización	0	5
SMDS	0	15
ILMI	0	16

Tabla 5.4. Valores preasignados de VPI/VCI.

Las celdas no asignadas tienen que ser usadas en enlaces fisicos que tienen estructuras de tramas (generalmente SONET y SDH) cuando no hay datos para enviar.

PT	Significado
000	Datos de usuario, sin congestión (SDU tipo=0)
001	Datos de usuario, sin congestión (SDU tipo=1)
010	Datos de usuario, con congestión (SDU tipo=0)
011	Datos de usuario, con congestión (SDU tipo=1)
100	Datos OAM, F5, flujo relacionado.
101	Datos OAM de extremo a extremo, F5, flujo relacionado
110	Reservado, Control de tráfico futuro y administración de recursos
111	Reservado, Funciones futuras

Tabla 5.5 Valores definidos del campo PT.

- **Tipo de carga útil (Payload Type).**

Se trata de un campo de tres bits, que indica el tipo de información, tal como datos de usuario, datos de operaciones de administración y mantenimiento, y si una congestión fue experimentada en algún lugar a lo largo de la ruta de la celda; contenida en los 48 bytes de carga útil de la celda. El campo PT también puede ser usado por capas más altas (la capa AAL-5 usa este campo para indicar el fin de un bloque de datos de usuario). El campo tiene 8 valores definidos, que se listan en la Tabla 5.5.

- **Prioridad de Pérdida de Celda (CLP).**

Cuando este bit es puesto a "1" significa que si el sistema necesita librarse de una congestión, entonces esta celda debe descartarse primero.

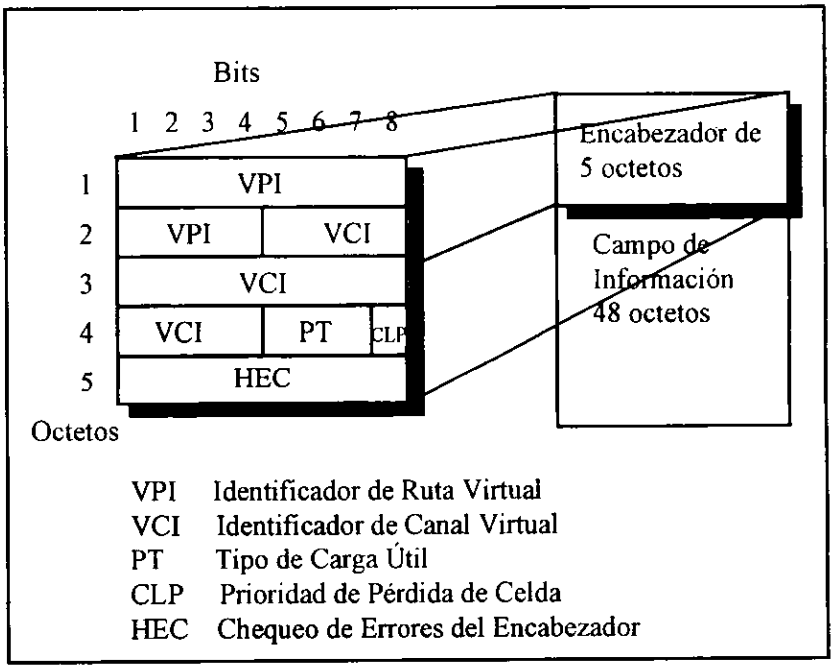


Figura 5.29. Estructura de la celda ATM en NNI.

- **Chequeo de Errores del Encabezador (HEC).**

Este campo permite la corrección de todos los errores de un sólo bit en el encabezador de la celda ó detección de la mayoría de los errores multi-bit o de bit sencillo. El HEC es un CRC de 8 bits, cubriendo únicamente 4 bytes (del encabezador) lo cual introduce una redundancia considerable. Como su nombre lo indica el HEC sólo se aplica al encabezador de la celda ATM, y no al campo de información. La detección y corrección de errores del campo de información es ejecutada por protocolos de capas superiores.

La protección de la dirección fue aplicada para evitar que la celda sea entregada a donde esta no pertenece. Sin protección, una celda puede llegar en la cola equivocada con una dirección válida que causaría que esta fuera

reensamblada en una trama. Una celda extra causaría un error en la trama de información recibida, forzándola a ser descartada.

En la figura 5.29 se ilustra el formato de la celda NNI. El formato es idéntico al formato de la celda en UNI con dos excepciones:

- No hay control de flujo genérico.
- La NNI usa cuatro bits (dedicados para control de flujo genérico en la interface UNI) para incrementar el campo VPI a 12 bits. Los SVC's involucran el plano de control para la NNI.

5.2.3.4 Valores del encabezador preasignados

Es importante notar que existen diversos valores del encabezador de la celda ATM ya asignados. En la tabla 5.6 se tiene una lista de dichos valores, para la celda en UNI.

5.2.3.5 Celdas no asignadas

En la mayoría de las interfaces, cuando no hay celdas generadas por el usuario (celdas asignadas) para enviar; celdas de relleno, también llamadas celdas no asignadas son enviadas para ocupara el ancho de banda disponible. Estas celdas tienen reservados los valores VPI/VCI 0/0 y patrón de carga útil fijo. Las celdas no asignadas son generadas y descartadas en la capa ATM, y pueden ser reemplazadas por celdas asignadas si es necesario.

Función	VPI	VCI	PT	CLP
Celda no asignada	00000000	00000000,00000000	xxx	0
Celda ociosa	00000000	00000000,00000000	000	1
Reservado para capa física	00000000	00000000,00000000	PPP	1

Tabla 5.6 (a). Valores preasignados del encabezador de la celda ATM.

Meta-señalización (I.311)	xxxxxxxx	00000000,00000001	0A0	C
Señalización broadcast general	xxxxxxxx	00000000,00000010	0AA	C
Señalización punto a punto	xxxxxxxx	00000000,00000101	0AA	C
Celdas de flujo F4 OAM de segmento	yyyyyyyy	00000000,00000011	0A0	A

Celdas de flujo F4 OAM de extremo a extremo	yyyyyyyy	00000000,00000100	0A0	A
Celdas de flujo F5 OAM de segmento	yyyyyyyy	zzzzzzzzz,zzzzzzzz	100	A
Celdas de flujo F5 OAM de extremo a extremo	yyyyyyyy	zzzzzzzzz,zzzzzzzz	101	A
Celdas de administración de recursos	yyyyyyyy	zzzzzzzzz,zzzzzzzz	110	A

x= No importa
y= Cualquier valor VPI
z= Cualquier valor de VCI no cero
A= Uso por una función apropiada
C= Originado para CLP
P= Reservado para capa física.

Tabla 5.6 (b). Valores preasignados del encabezador de la celda ATM.

Es necesario mencionar que otro tipo de celda tiene un valor de 0/0, la celda de capa física. Cuando el valor VPI/VCI es 0/0, los 4 bits usados para PT y CLP son interpretados como sigue:

Interpretación	Valor	
No asignado	0000	Celda de capa ATM
Ociosa	0001	Celda de capa física
Flujo F1 (CBPL)	0011	Celda de capa física
Flujo F3 (CBPL)	1001	Celda de capa física

Tabla 5.7. Valores de PT y CLP para celdas no asignadas.

Las celdas ociosas son usadas para adaptación de velocidad (celdas de relleno) en la capa física. A diferencia de las celdas no asignadas, las celdas ociosas no pueden ser reemplazadas por celdas asignadas.

5.2.3.6 Celdas OAM

Para soportar un buen desempeño la ITU-T desarrolló la recomendación I.610 para definir las funciones de Operaciones de Administración y Mantenimiento (OAM) de capa física y de la capa ATM. Estas funciones son divididas en 5 fases:

- Monitores de desempeño, verificación periódica.
- Detección de falla y defecto, detección de mal funcionamiento y alarmas.
- Protección del sistema, aislar un componente de falla para restaurar el sistema.
- Información de desempeño, alarmas y reportes.
- Localización de la falla, prueba para determinar el componente de falla.

Las funciones OAM operan en 5 niveles dentro de las capas física y ATM. Estas funciones son llamadas flujos OAM, que van de F1 a F5. La capa física contiene tres niveles OAM: la sección de regenerador F1 (nivel de sección en SONET), nivel de sección digital F2 (nivel de línea en SONET) y nivel de transmisiones (nivel de ruta en SONET). La capa ATM contiene dos niveles OAM: nivel de canal virtual (F4), y nivel de ruta virtual (F5).

La operación OAM esta definida en la UNI 3.0 del Forum ATM y la Recomendación I.610 de la ITU-T.

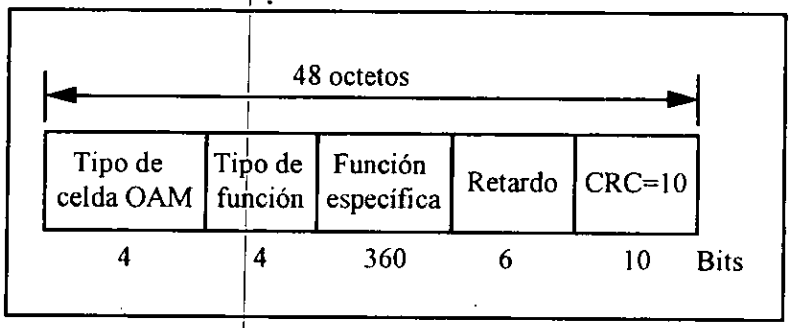


Figura 5.30. Formato de la celda OAM.

Las celdas OAM son enviadas en VCI´s preasignados. Para flujo OAM F4, VCI= 3 identifica un flujo OAM a nivel de segmento, en tanto que VCI= 4 identifica el flujo OAM de extremo a extremo. Para el flujo OAM F5, la celda es enviada con los mismos valores de VPI/VCI que los datos de usuario, sin embargo el valor de campo PT, en el encabezador de la celda identifica el tipo de conexión OAM ya sea de segmento o de extremo a extremo.

La figura 5.30. muestra la Unidad de Datos de Protocolo (PDU) de administración de la capa ATM (o celda OAM).

El campo de información de la celda se divide a su vez en tres campos:

- Tipo de OAM.
  Identifica el tipo de comunicación OAM (administración de fallas, administración de desempeño, y activación ó desactivación).
- Tipo de función.
  Define la función ejecutada por esta celda.
- Campo específico de función.
- Reservado, bits no usados.
- Código de detección de errores, CRC-10.

Tipo de OAM	Valor	Tipo de Función	Valor
Admón. de fallas	0001	Señal de indicación alarma	0000
		Indicación de defecto remoto	0001
		Loopback de celdas OAM	0010
		Chequeo de continuidad	0100
Admón. de desempeño	0010	Monitoreo hacia adelante	0000
		Reporte hacia atrás	0001
		Monitoreo y reporte	0010
Activación y desactivación	1000	Monitoreo de desempeño	0000
		Chequeo de continuidad	0001
Administración de sistema	1111	No aplicable	

Tabla 5.7. Tipos de celdas OAM.

5.2.3.7 Conexiones ATM

♦ **Asíncronía de ATM**

En un enlace serial el flujo de celdas es constante, ya que se tendrá celda asignada o no asignada, pero todas vienen una tras de otra y no hay espacio entre ellas por lo que se puede considerar síncrono. La velocidad de llegada de las celdas es constante y sincronizada a la misma transmisión o reloj del sistema de conmutación. ¿Por que se dice que las celdas son transmitidas asíncronamente ?: la asíncronía se refiere al tiempo indeterminado cuando la próxima unidad de información de la conexión lógica puede empezar. Para ATM la unidad a que nos referimos no es cualquier celda, si no la próxima celda en una conexión específica. El tiempo no usado por una conexión lógica puede ser dado a otras conexiones o llenadas con celdas ociosas.

La próxima celda en el flujo físico podría ser de cualquier conexión lógica de

cualquier usuario. La celda precedente no dice nada a cerca de la próxima celda, excepto que esta empezará inmediatamente después de la celda actual. La próxima celda podría estar vacía o destinada a cualquier conexión. Por lo tanto las celdas para una conexión dada llegan asíncronamente.

De aquí que las celdas deban ser etiquetadas individualmente para indicar a que conexión pertenecen. Esta es la función de las direcciones. El sistema ATM entero usa las direcciones para definir como las celdas pasan a través de la red. Este es un sistema con el que los switches crean y mantienen conexiones.

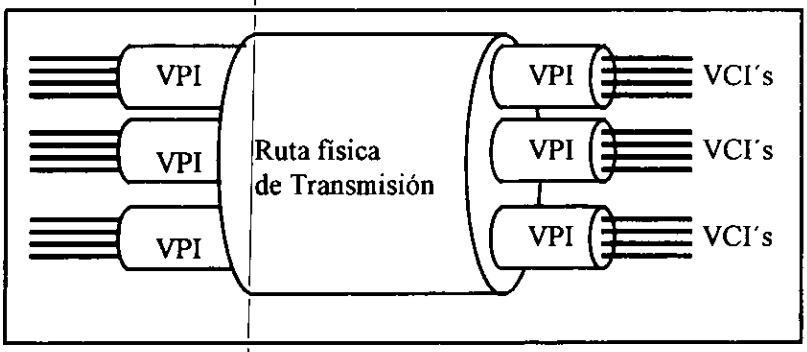


Figura 5.31. Relación entre ruta física, VPI y VCI.

♦ **Conexiones de la capa ATM**

Antes de explicar una conexión ATM es preciso entender la relación entre VPI's y VCI's. La figura 5.31 muestra la relación entre ruta física, VPI y VCI. Una ruta física puede ser un DS3, un T1, un E1, una trama STS-3c, etc., cada una con sus respectivo medio físico. Dentro de esa ruta física una cantidad dada de VPI's puede existir. El número de rutas virtuales (VP's) depende de los bits asignados a VPI en el encabezador de la celda (8 bits asignados a el VPI da para 256 rutas virtuales en la interface UNI, y 65,536 VCI's con 16 bits asignados en UNI y NNI). Usando el valor de VPI en el encabezador de la celda ATM, cada ruta virtual es identificada. Por otra parte, dentro de una ruta virtual, hay muchos canales virtuales. El número de canales virtuales depende del número de bits asignados al VCI en la celda ATM. Cono ya se mencionó, se han asignado 16 bits para VCI lo cual nos da 65536 posibles valores de VCI. La red ATM usa los valores de VPI y VCI para enrutar la celda.

En el mundo real ATM existen 2 tipos de conexiones: conexión de canal virtual (VCC) y conexión de ruta virtual (VPC). Una conexión de canal virtual (VC) es una conexión lógica entre dos puntos finales para la transferencia de celdas, así un VPC es una combinación lógica de VCC´s. A cada VCC es asignado un valor de VCI y cada VPC es asignada a un valor de VPI. Las VC´s que pertenezcan a diferentes VP´s pueden poseer el mismo VCI que haya sido usado en otra VPC. Un VC puede ser identificado en base a su VCI y su VPI. Si en una red ATM el valor VCI no se modifica pero el valor VPI si, esta función es ejecutada por un "cross.conect" ATM. Si ambos identificadores son cambiados, entonces la función es ejecutada por un "switch" ATM. La figura 5.32 muestra el concepto de conexiones VP y VC.

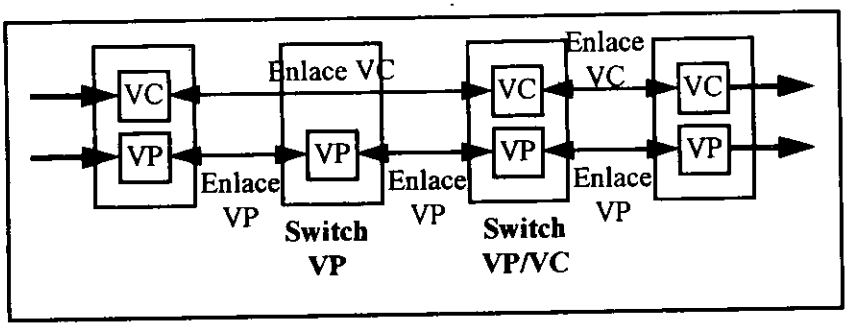


Figura 5.32. Conexiones VP y VC.

Las conexiones VP y VC son definidas basados en los elementos de conmutación usados. Un VCC se refiere a la concatenación de líneas VC para conseguir la conexión entre puntos de acceso al servicio ATM. En el VC el VCI es trasladando al llegar al switch. El VCC provisto por un elemento de conmutación ATM puede ser una conexión semipermanente o permanente. La integridad de la secuencia de la celda es asegurada dentro de un mismo VCC. Un VCC es provisto con un conjunto de parámetros tal como retardo de celda, pérdida de celda, etc. En el momento de establecer un VCC, los parámetros de tráfico son establecidos a través de una negociación entre el usuario y la red. La red manifiesta estos parámetros durante la duración de la conexión.

En la UNI, cuatro métodos pueden ser utilizados para crear un VCC:

- El procedimiento de señalización. En esta conexión, establecer o liberar es conseguido a través de la reservación. Este método se aplica a creaciones de circuitos permanentes o semipermanentes.

- El procedimiento de meta-señalización VC, donde es establecida o removida a través del uso de meta-señalización VC.
- Procedimiento de señalización usuario-red. Una señalización VCC es usada para establecer o liberar una comunicación VCC extremo a extremo.
- El procedimiento de señalización usuario-usuario. Una señalización VCC es usada para establecer o liberar una VCC interna a una VPC preestablecida entre dos UNI.

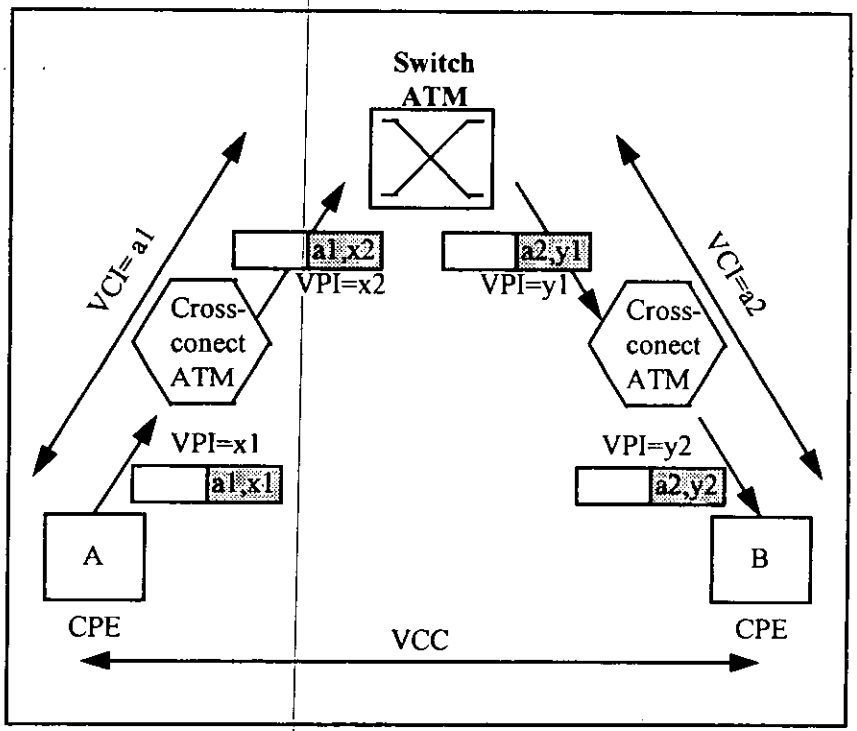


Figura 5.33. Conexión VCC y asignación VPI/VCI a través de dispositivos ATM.

Una vez que una VCC es establecida usando cualquiera de los métodos mencionados anteriormente, las celdas fluyen a través de la red ATM. Cada encabezador de la celda (VPI/VCI) es procesado para alcanzar su destino. En la figura 5.33, se muestra una conexión VCC y la asignación de VPI/VCI a través de dispositivos ATM.

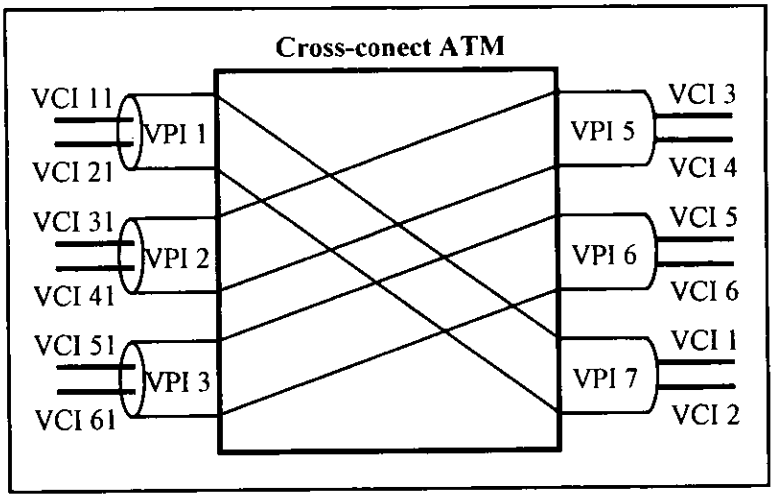


Figura 5.34. Operación de un cross-conect ATM.

Una VPC se refiere a la concatenación de enlaces de VP para conectar los puntos en los cuales un VPI es asignado, trasladado o removido. Una VPC puede ser provista a través de un equipo de conmutación, y puede ser permanente o semipermanente. La secuencia de celdas es asegurada para cada VCC dentro de un mismo VPC. Hay dos formas de establecer un VPC:

- Sin un procedimiento de señalización. El establecimiento y liberación de una conexión es conseguido usando una reservación.
- Mediante control de red. Los VPI's son asignados por el proveedor de la red.

5.2.3.8 Conmutación ATM

En la figura 5.36 se muestra el principio de conmutación ATM. Aquí las celdas entrantes ATM son físicamente conmutadas de la entrada I_n a una salida 0_q mientras que los valores de los encabezadores son trasladados de un valor β entrante a un valor α saliente. Cada enlace entrante o saliente tiene valores de encabezador únicos, pero encabezadores idénticos pueden haber en enlaces distintos. Las tablas de translación mapean, el valor del encabezador entrante a un valor de encabezador saliente.

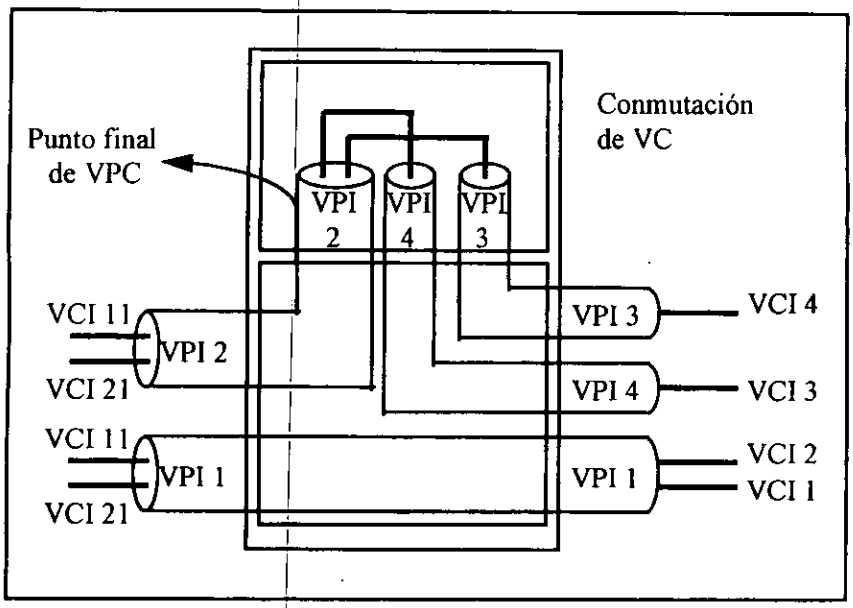
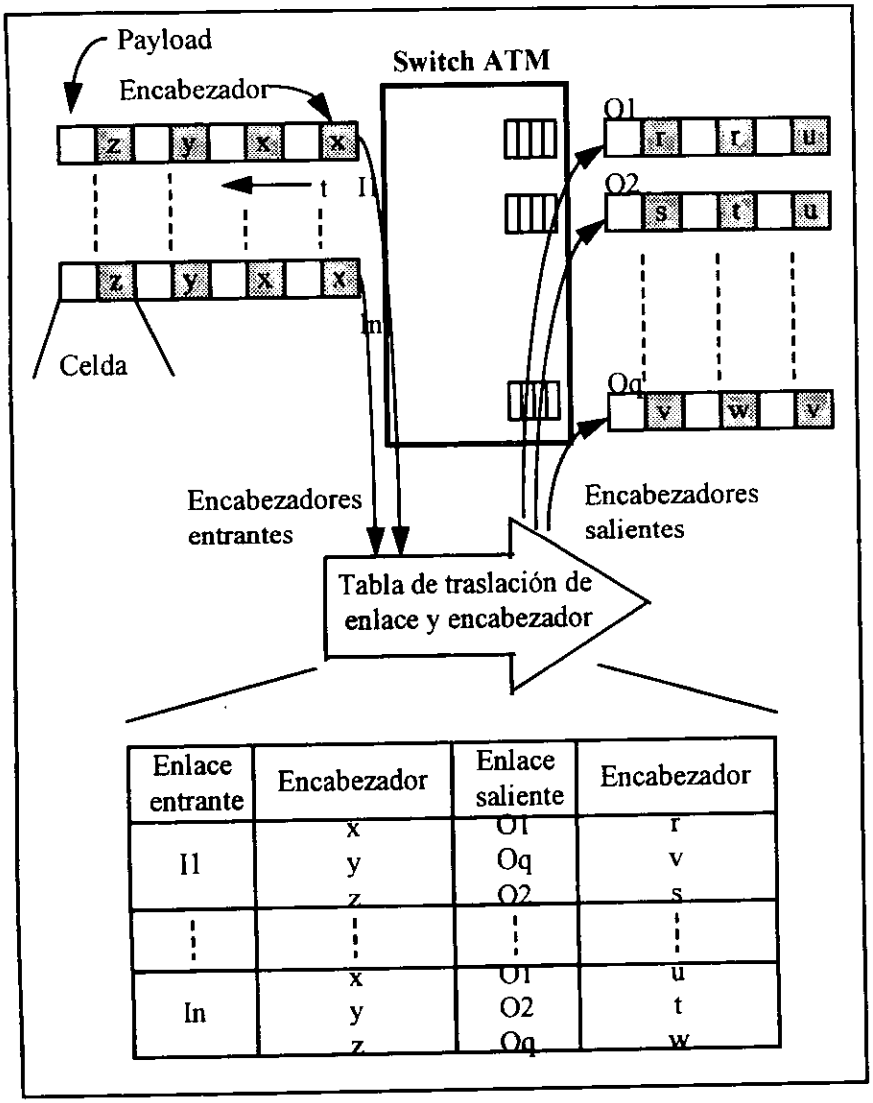


Figura 5.35. Operación de un switch ATM.

En este sistema de conmutación sin embargo, es posible que dos celdas de entrada I_1 e I_n lleguen simultáneamente al switch ATM y son destinadas a la misma salida (O_n). En tal caso las celdas no pueden ser puestas al mismo tiempo y el switch debe mantener momentáneamente en el buffer las celdas que no pueden ser llevadas al enlace saliente. Los buffers son típicos en los switches ATM.

5.2.3.9 Calidad de servicio (QOS)

La recomendación I.330 de la ITU-T define parámetros para medir la calidad de servicio (QOS), o desempeño extremo a extremo orientado al usuario de una B-ISDN. El Forum ATM a trabajado en algunas configuraciones de referencia para QOS, que en resumen son configuraciones con diversas redes ATM entre usuarios finales. La QOS siempre se mide de extremo a extremo.



Enlace entrante	Encabezador	Enlace saliente	Encabezador
I1	x y z	O1 Oq O2	r v s
⋮	⋮	⋮	⋮
In	x y z	O1 O2 Oq	u t w

Figura 5.36. Principio de conmutación ATM.

Los parámetros definidos para la QOS en la recomendación I.350 y documentos ATM UNI son:

Razón de celdas erroneas (CER)= (Celdas erroneas) / (Celdas trans. exitosamente + Celdas erroneas)

Razón de bloques de celdas severamente erróneos (SECBR) = (Bloques de celdas severamente erróneos) / (Bloques de celdas transmitidas totales)

El tamaño del bloque es tomado como aquel marcado por celdas OAM consecutivas, lo cual es fácilmente medible dado que cada celda OAM lleva un conteo de las celdas de datos que fueron enviadas desde la celda OAM previa.

Razón de celdas pérdidas (CLR)= (Celdas pérdidas) / (Celdas transmitidas totales)

Razón de inserción de celdas (CMR)= (Celdas insertadas) / (Intervalo de tiempo)

Las celdas insertadas son aquellas que llegan al destino, pero no fueron enviadas por el originador. Esto puede ocurrir debido a un error en el encabezador de la celda no detectado. Hay tres parámetros más que miden la velocidad de la red:

- El retardo de transferencia de la celda (CTD), que es el intervalo de tiempo entre cuando la celda deja la UNI originante y el momento en que esta llega a la UNI destino para una conexión en particular.
- El retardo de transferencia de la celda medio (MCTD), que es un promedio aritmético de CTD especificada para una o más conexiones.
- La variación de retardo de la celda (CDV), mide la variabilidad de eventos de llegada de celdas en puntos de medida diferentes de la red.

El CER, SECBR y CMR afectan la seguridad de la red, CLR afecta la confiabilidad de la red.

La especificación UNI del Forum ATM versión 3.0 define 5 clases de QOS, las cuales se listan en la Tabla 5.8. La QOS es definida por al menos los siguientes parámetros:

- Razón de pérdida de celda para el flujo CLP=0
- Razón de pérdida de celda para el flujo CLP=1
- Variación de retardo de celda para flujo agregado CLP=0+1
- Retardo promedio para flujo agregado CLP=0+1

Clase de QOS	Parámetros de QOS	Aplicación
1	No especificado	"Mejor esfuerzo"
2	Especificado	Emulación de circuitos
3	Especificado	VBR Vídeo/Audio
4	Especificado	Datos orientados a conexión
5	Especificado	Datos sin conexión

Tabla 5.8. Tipos de QOS.

El flujo CPO=0 se refiere únicamente a celda las cuales tienen el campo CLP del encabezador puesto a 0, lo mismo para CLP=1. El flujo agregado CLP=0+1 se refiere a todas las celdas en la conexión virtual.

Inicialmente cada proveedor de red definirá parámetros de desempeño de la red ATM para al menos las siguientes clases de servicio de la recomendación I.362:

- Servicio clase A: Emulación de circuitos, video de velocidad de bit constante.
- Servicio clase B: Audio y Video VBR.
- Servicio clase C: Transferencia de datos orientados a conexión (FR, X.25).
- Servicio clase D: Transferencia de datos sin conexión (SMDS, IP)

Así, tenemos las clases de QOS especificadas por el Forum ATM:

- QOS especificado clase 1. Soporta una QOS que satisface las necesidades de desempeño del servicio clase A.
- QOS especificado clase 2. Soporta una QOS que satisface las necesidades de desempeño del servicio clase B.
- QOS especificado clase 3. Soporta una QOS que satisface las necesidades de desempeño del servicio clase C.
- QOS especificado clase 4. Soporta una QOS que satisface las necesidades de desempeño del servicio clase D.

5.2.4 Capa de adaptación ATM

La capa de adaptación ATM (AAL) mapea las capas más altas (voz, datos, vídeo) sobre la capa ATM. AAL consiste de dos subcapas: la Subcapa de Segmentación y Reensamblaje (SAR) y la Subcapa de Convergencia (CS). La subcapa SAR segmenta la información de capas más altas de largo variable para ser transmitida en unidades de carga útil de largo fijo (48 bytes) de la celda

ATM; y reensambla las cargas útiles recibidas en información de capas más altas. La CS ejecuta las funciones requeridas por el tipo de AAL en uso y es por lo tanto dependiente del servicio. En algunos casos, la CS puede ser subdividida en Subcapa de Convergencia de Parte Común (CPCS) o la subcapa más baja; y la Subcapa de Convergencia de Servicio Específico (SSCS), o subcapa más alta.

5.2.4.1 Clases de servicio

La recomendación ITU-T I.362 define cuatro clases de servicio que dependen de tres parámetros o atributos, los cuales se tienen en la Tabla 5.9 y son:

Atributo	Clase A	Clase B	Clase C	Clase D
Relación de sincronía entre la fuente y el destino	Requerida		No Requerida	
Velocidad de bit	Constante	Variable		
Modo de conexión	Orientado a conexión			Sin conexión
AAL	AAL-1	AAL-2	AAL-3/4 ó AAL-5	AAL-3/4 ó AAL5
Ejemplo	Emulación de ctos. E1, T1	Audio y video en paquetes	Frame Relay, X.25	IP, SMDS, LANE

Tabla 5.10. Clases de servicio en ATM.

- Relación de síncronía entre la fuente y el destino (requerida o no requerida).
- Velocidad de bit (variable o constante).
- Modo de conexión (orientado a conexión o sin conexión).

5.2.4.2 Capa de adaptación 5

De las cuatro capas de adaptación disponibles (a la fecha), sólo abordaremos la capa de adaptación 5 (AAL-5) debido a que es esta capa la que soporta IP

y protocolos LANE. La interacción entre estos protocolos y ATM, será tratada en detalle más tarde.

Derivada de las LAN´s, AAL-5 trabaja mejor con unidades de protocolo de largo variable operando sobre velocidad de bit variable sobre servicios orientados a conexión. La AAL-5 ha reemplazado a AAL-3, como el modo más común para este tipo de datos, tal como Frame Relay; ofreciendo un alto throughput para el ancho de banda usado. La AAL-5 también trabaja con servicios sin conexión. El soporte de ambos servicios es provisto en el nivel de la Subcapa de Convergencia de Servicio Específico (SSCS).

El chequeo de errores provisto por AAL-3/4 tiene un precio en el encabezador de 4 bytes resultante en cada unidad de segmentación (zona de los 48 bytes de carga útil de la celda ATM). Algunos usuarios no soportarían esta sobrecarga de 4 bytes, dado que sólo se tendrían 44 bytes de carga útil por cada celda ATM.

La capa de adaptación eficiente y simple (SEAL por sus siglas en inglés) conocida como AAL-5, eliminó los bytes de sobrecarga dentro de la carga útil de la celda ATM. Estos bytes representan el 9% del ancho de banda asignado al usuario en la celda ATM.

Uno de los campos eliminados MID (identificador de mensaje) permitía a muchas unidades de datos de servicio (SDU´s) ser multiplexadas en un flujo sencillo de celdas. El receptor ordenaba las celdas tomando en cuenta el campo MID y reensambla las unidades de datos de protocolo (PDU´s) con celdas con el mismo MID. Al desaparecer el campo MID, también se eliminan las posibilidades de intercambiar celdas de diferentes mensajes sobre la misma conexión lógica. Con AAL-5 el multiplexaje debe ser hecho en el nivel de la trama (capa 3) o a nivel ATM (con valores VPI/VCI).

♦ **Parte común de convergencia de AAL -5**

AAL-5 dividirá archivos grandes de computadoras en SDU´s (de hasta 65535 bytes). En muchos casos esta operación no será necesaria en la parte común de AAL:

- La subcapa de convergencia de protocolo específico (PSCS) o parte específica de servicio hará esto.
- La aplicación entera estará basada en un servicio de capas más altas que por si mismo produce PDU´s menores de 64 Kbytes (Frame Relay no presentará un bloque de más de 8 Kbytes). El tráfico LAN generalmente está limitado a

tramas de 32 Kbytes para Token Ring y 1500 bytes para Ethernet.

La parte común de AAL-5 consiste de :

- **Datos de Usuario**
  Hasta 65 Kbytes. El bit más significativo es transmitido primero.

- **PAD**
  Se tiene un relleno de 0 a 47 bytes, con el fin de que la PDU de parte común sea múltiplo de 48 bytes. Alinear aquí al largo de la carga útil completa de la celda ATM, elimina la necesidad de un campo de largo en cada celda.

- **Usuario a Usuario (UU)**
  Es una información que es pasada transparentemente por la red de extremo a extremo. La función de este byte está determinada por el equipo de premisas de cliente o cualquier equipo que termine la conexión lógica. UU no está completamente definida por el CCITT.

- **Largo (Length)**
  Es un número binario de 16 bits representando los bytes de datos de usuario actuales en la CS SDU. El receptor usa este número para decir donde los datos terminan e inicia el PAD.

- **Indicador de Parte Común (CPI)**
  Esta reservado. Únicamente un registro de 0000,0000 es permitido indicando que el campo Length se refiere al tamaño de datos de usuario en bytes. CPI soportará funciones adicionales de AAL-5 definidas en el futuro.

- **CRC-32**
  Es un chequeo de redundancia cíclica que detecta errores en la Unidad de Datos de Protocolo de la Subcapa de Convergencia de Parte Común (CPCS-PDU). Este CRC-32 es el mismo que para IEEE 802.3. El CRC-32 no provee una certeza absoluta en la detección de todos los posibles errores en una SDU tan grande como 65 Kbytes.

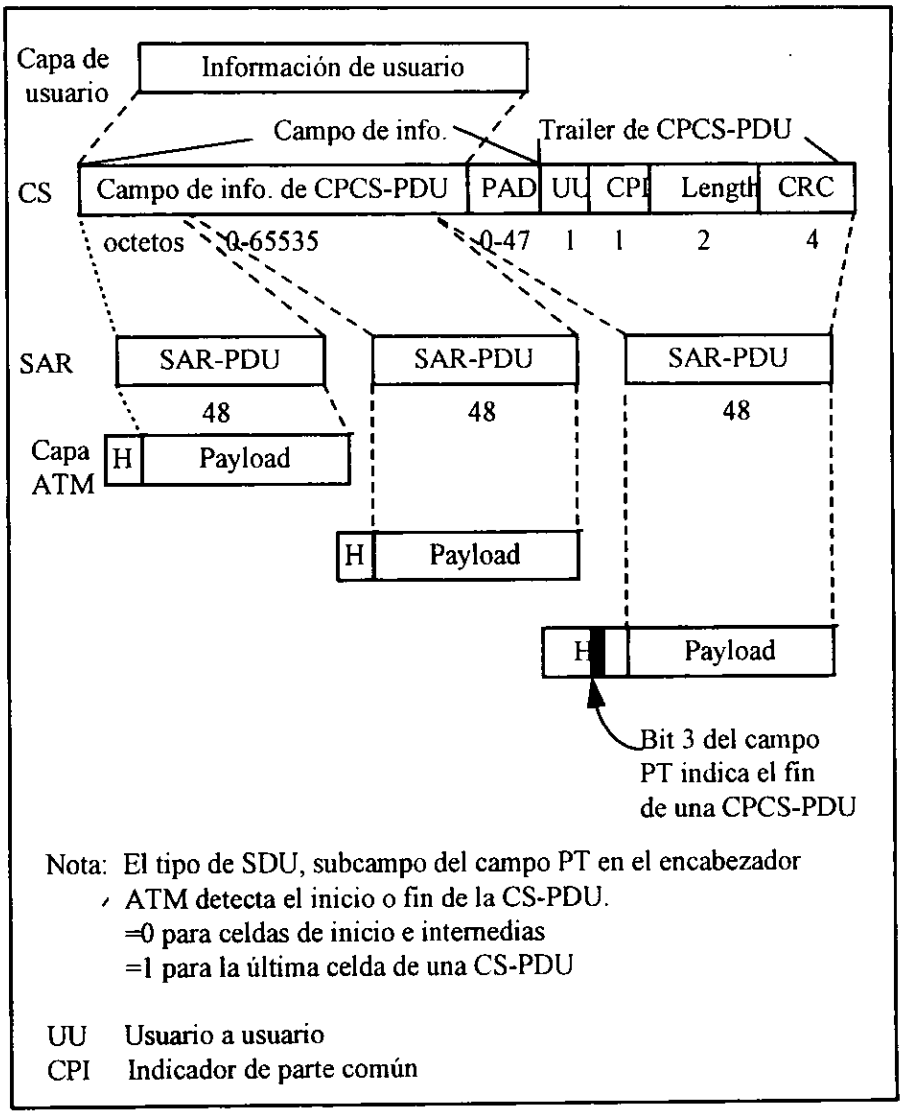


Figura 5.37. Operación de AAL-5.

♦ **Subcapa de Segmentación y Reensamblaje (SAR)**

En la segmentación es donde AAL-5 es realmente simple: segmentos de 48 bytes de la CS PDU (SDU a la capa SAR) son puestos dentro del campo de información de celdas sucesivas. No hay un encabezador adicional por celda

(dentro del campo de información). La dirección de la celda es determinada por la fuente lógica de datos dentro del equipo. En la práctica esto significa que las direcciones de la celda son asignadas a PVC´s cuando las celdas son generadas. Una tabla de enrutamiento del dispositivo "internetworking" ATM determina la dirección de la celda transmitida de la dirección de la trama (capas más altas) y la dirección de la trama de la dirección de la celda recibida.

Los SVC´s usaran mensajes de señalización para cambiar, la tabla de enrutamiento dinámicamente con el fin de establecer y quitar conexiones lógicas en demanda.

Dado que no hay un campo de largo en la celda después de la segmentación, la capa SAR pasa la responsabilidad a la CS la responsabilidad de rellenar la PDU de CS a múltiplos de 48 bytes. Cuando ocurre la segmentación no se dejan residuos de la CS-PDU de menos de un campo de información de celda.

El único encabezador de que se vale la capa SAR es del campo PT en el encabezador de la celda ATM. Con la invención de AAL-5, el bit en la posición 3 del campo PT es usado para indicar la última celda (fin de mensaje) dentro de una PDU. Esto es una SDU tipo 1 (PT=001, PT=011) define cualquier segmento de una PDU, excepto el último de una capa de protocolo más alta. Una SDU tipo 0 (PT=000, PT=010) es la SDU fin de mensaje, que termina una PDU de más alto nivel.

5.3 ESQUEMAS DE DIRECCIONAMIENTO EN ATM.

5.3.1 Introducción

Existen dos capacidades que son críticas para una red conmutada: direccionamiento y enrutamiento. El direccionamiento ocurre en el nivel VPI/VCI de ATM y en el nivel de red lógica. Dado que VPI/VCI son únicos para un ruta de transmisión física, hay necesidad de tener una dirección de nivel más alto que sea única a través de al menos cada red. Idealmente la dirección sería única a través de todas las redes para proveer conectividad universal. Una vez que cada entidad involucrada en la conmutación de conexiones virtuales tiene una dirección única, hay otro problema aún más serio, que es encontrar la ruta de la parte llamante a la parte llamada. Este problema es resuelto usando enrutamiento.

5.3.2 Direccionamiento a nivel VPI/VCI de la capa ATM

El protocolo de señalización automáticamente asigna los valores VPI/VCI a direcciones ATM y puertos UNI ATM físicos basado en el tipo de SVC pedido de acuerdo al siguiente conjunto de reglas: ya sea que se trate de una conexión punto a punto ó una conexión punto a multipunto. Una UNI ATM física debe tener al menos una dirección ATM única. Un puerto UNI ATM puede también tener más que una dirección ATM.

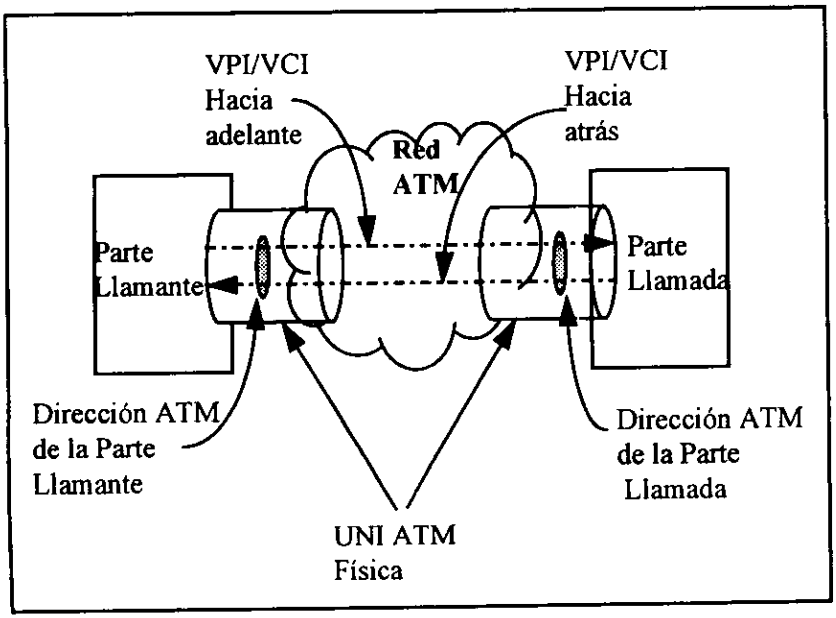


Figura 5.38. SVC punto a punto.

Recordando que un VCC o VPC está definido únicamente en una dirección: esto es, es simplex. Un SVC (ó PVC) punto a punto es un par de VCC's o VPC's: una conexión hacia adelante de la parte llamante a la parte llamada y una conexión hacia atrás desde la parte llamada como se ilustra en la figura 5.38 (Conexión virtual conmutada punto a punto). Los VCC o VPC hacia adelante o hacia atrás pueden tener diferentes parámetros de tráfico. Un SVC punto a punto es definido por el VPI (y VCI para un VCC) hacia adelante y hacia atrás así

como por la dirección ATM asociada con los puertos UNI ATM fisicos en cada extremo de la conexión. La asignación de VPI (/VCI) puede ser diferente para las direcciones hacia adelante o hacia atrás de un VPC o VCC en el mismo extremo de la conexión así también para el otro extremo de la conexión.

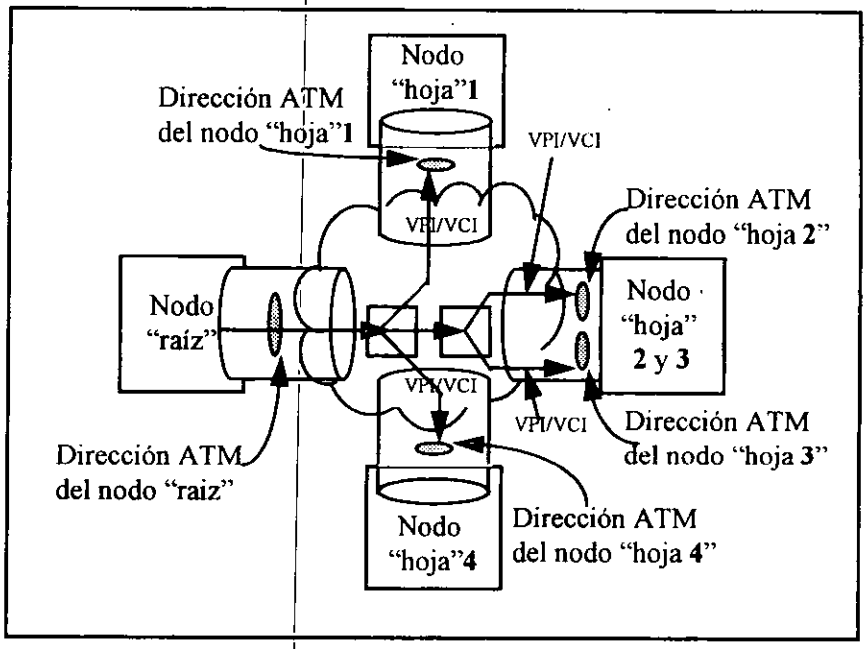


Figura 5.39. SVC punto a multipunto.

Un SVC (o PVC) punto a multipunto es definida por el VPI y la dirección ATM asociada con el puerto UNI ATM fisico del nodo raíz, y la dirección ATM y VPI (/VCI) para cada nodo "hoja" de la conexión. Fig. 5.39. Conexión Virtual Conmutada punto a multipunto.

Hay esencialmente únicamente una dirección debido a que la dirección hacia atrás se le asigna cero ancho de banda. Se puede ver que más que un valor de VPI/VCI y dirección ATM puede ser asignada una interface fisica como parte de una conexión punto a multipunto. Esto significa que el número de puertos UNI ATM fisicos es menor o igual que el número de puntos finales "hoja" de la conexión punto a multipunto.

5.3.3 Direccionamiento a nivel de la capa ATM

Existe un conjunto de atributos que son deseables cuando se diseña una esquema de direccionamiento de la capa ATM. El más importante por su puesto: la dirección debe ser única. Dichos atributos incluyen los siguientes:

- Simplicidad
- Asignación automática
- Facilidad de administrar cambios en direcciones
- Extensión del esquema de direccionamiento

5.3.4 Esquemas de direccionamiento propuestos para ATM

El Forum ATM ha definido tres formatos de dirección UNI privados basados en una dirección NSAP (Punto de Acceso al Servicio de Red) de OSI, cada uno de 20 octetos de largo. Debe notarse sin embargo, que una dirección ATM no es una dirección NSAP a pesar de su estructura similar; las direcciones ATM son mejor descritas como direcciones de red privada ATM ó identificadores de puntos finales ATM, y no identifican un Punto de Acceso al Servicio de Red, si no, puntos de subred de conexión.

La especificación UNI versión 3.0 establece que una UNI Privada debe soportar los tres formatos de dirección ATM Privados. Una UNI Pública soportara el formato de direcciones E.164, los tres formatos de dirección UNI Privados, o todos ellos.

Los tres formatos de direcciones UNI Privados se muestran en la figura 5.40. El formato ATM, Código de País de Datos (DCC) es identificado por un Identificador de Formato y Autoridad (AFI) de 39. El próximo campo contiene el DCC (2 octetos) que especifica el país donde la dirección es registrada. El campo del Identificador de Formato de Parte Específica de Dominio (DFI) de un octeto especifica la estructura del resto de la dirección. El campo reservado (RSRVD) de dos octetos esta reservado para posibles extensiones. El campo de Dominio de Enrutamiento (RD) especifica un dominio de enrutamiento único. El campo de Área (ÁREA) de dos octetos identifica una área única dentro del dominio de enrutamiento. El Identificador de Sistema Final (ESI) de 6 octetos identifica un sistema final dentro de un área. El campo Selector (SEL) de un

octeto, no está siendo usado para enrutamiento, pero puede ser usado por sistemas finales.

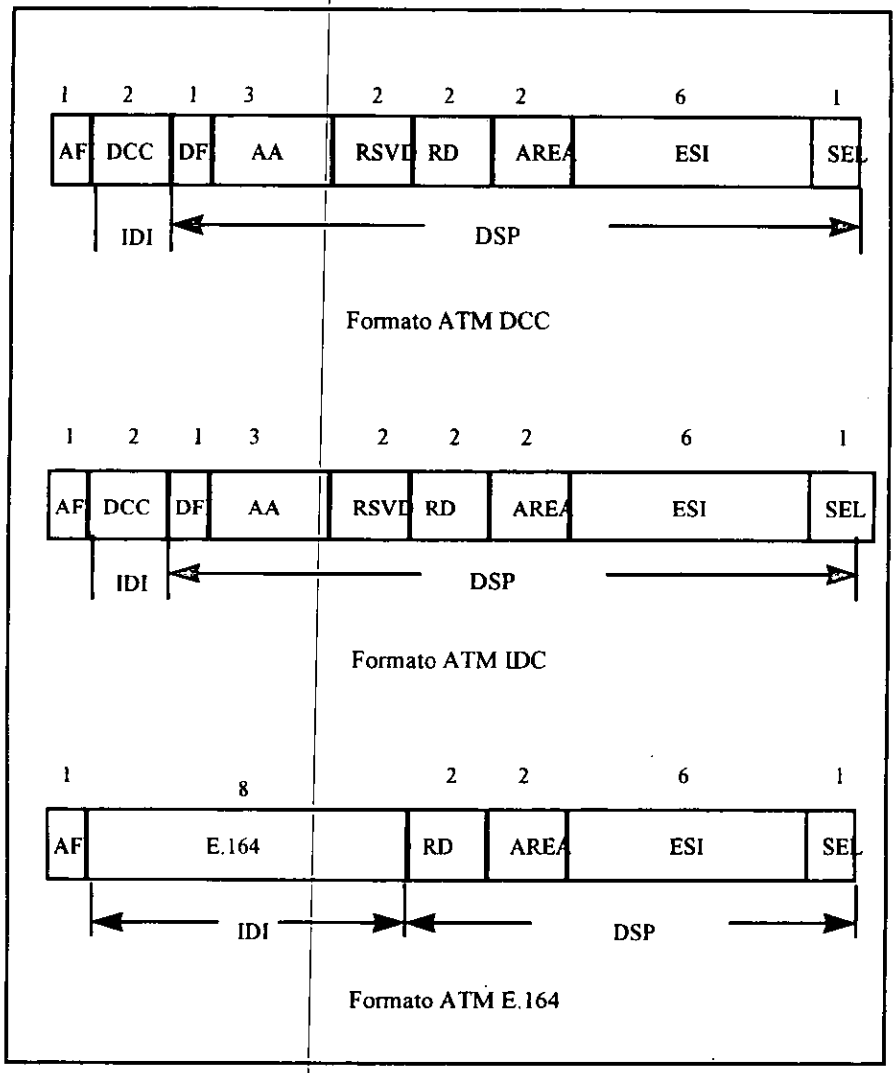


Figura. 5.40. Direcciones ATM.

El Formato ATM, Designador de Código Internacional (ICD) es identificado por un AFI de 47. El próximo campo contiene el ICD (2 octetos), el cuál identifica una organización internacional, y esta es administrada por el Instituto de Estándares Británicos. Los campos de dirección restantes son los mismos que en el formato ATM DCC.

El formato ATM E.164 es identificado por un AFI de 45. El próximo campo contiene una dirección E.164 (8 octetos). El resto de los campos de dirección son los mismos que para los formatos ATM DCC y ATM ICD.

Antes de que una conexión ATM pueda ser establecida en una UNI, el usuario y la red deben estar seguros de la dirección en efecto en esa UNI. Procedimientos de registro de dirección, los cuales son una extensión a la ILMI, consiguen esto. Para formatos de dirección UNI Privada, el lado del usuario de la UNI suple la "parte de usuario" de la dirección: campos SEL y ESI. La red suple el prefijo de red, el cual consiste de todos los campos que preceden al campo ESI. Cuando el formato de dirección E.164 es usado, la red suple la dirección de 8 octetos entera. Los elementos de dirección son intercambiados usando mensajes ILMI, y estos son almacenados en tablas en uno u otro lado de la UNI. Después de que la dirección ha sido registrada, estas pueden usarse en los elementos de información Número de la Parte Llamante y Número de la Parte Llamada transmitidos en mensajes de señalización.

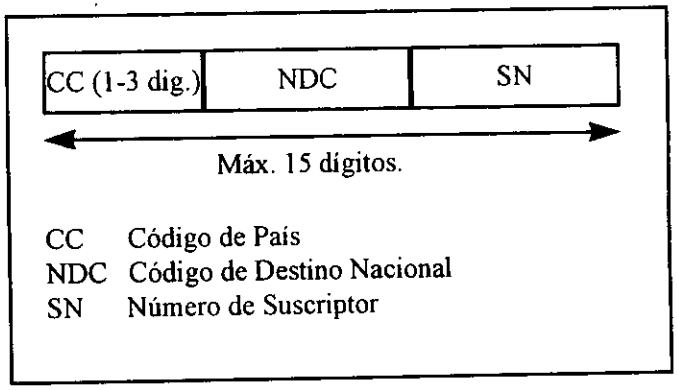


Figura 5.40 (a). Formato de una dirección E.164

En la figura 5.40(a), se resume el formato del plan de numeración E.164. Donde el número internacional es codificado en BCD (Binary Coded Decimal) y es rellenado con ceros en el lado izquierdo para resultar en un largo

constante de 15 dígitos. Hay un Código de País (CC) de uno a tres dígitos, como se estandarizó en la recomendación E.163. El resto de la dirección es un Número de Significancia Nacional (NSN). El NSN es subdividido en Código de Destino Nacional (NDC) y Número de Suscriptor (SN).

5.3.5 Enrutamiento ATM.

Una parte muy importante en ATM, son los protocolos de la Interface Nodo-Red (NNI) que se usan para enrutar peticiones ATM entre ATM switches. Dado que ATM es orientado a la conexión, una petición de conexión necesita ser enrutada desde el nodo de petición, a través de la red ATM y hasta el nodo destino.

El Forum ATM ha trabajado en la definición de un protocolo NNI Privado (P-NNI). Su meta es definir, protocolos NNI para usarse en redes privadas, o más específicamente dentro de redes que utilicen el formato de dirección ATM NSAP.

El protocolo P-NNI consiste de dos componentes :

- El primero es el protocolo de señalización P-NNI usado para avanzar una petición de conexión ATM dentro de las redes, entre la UNI origen y la UNI destino. La petición de señalización UNI es mapeada en señalización NNI en el switch origen y después la señalización NNI es mapeada a señalización UNI en el switch destino. Los protocolos P-NNI operan entre sistemas de conmutación ATM (los cuales pueden representar switches o redes enteras de switches operando como una entidad sencilla P-NNI), que son conectados por enlaces P-NNI. Los enlaces P-NNI pueden ser : físicos o virtuales. Un ejemplo típico de un enlace virtual es una ruta virtual que conecta dos nodos juntos. Dado que todos los canales virtuales, incluyendo la conexión que lleva la señalización P-NNI, serían transportados a través de todos los switches intermedios entre estos dos nodos en dicha ruta virtual, los dos nodos son adyacentes en relación a los protocolos P-NNI. El protocolo de señalización P-NNI actual, está siendo desarrollado por el Forum ATM y es una extensión de la señalización UNI que incorpora Elementos de Información (IE) adicional para parámetros relacionados con NNI, tales como Listas de Tránsito Diseñadas (DTL). La señalización P-NNI es llevada a través de enlaces NNI en el mismo canal virtual, VCI=5, el cual es usado para señalización a través de la interface UNI. El valor del VPI depende de si el enlace es físico o

virtual.

- El segundo componente del protocolo P-NNI es un protocolo de enrutamiento de circuito virtual. Este es usado para rutear peticiones de señalización a través de la red ATM. Esta ruta es también por la cual la conexión ATM es establecida, y por donde los datos van a fluir. La operación de rutear una petición de señalización a través de una red ATM, es superficialmente similar a rutear paquetes con protocolos sin conexión (tal como IP), dado que para la petición de señalización no hay una conexión previamente establecida.

El protocolo de enrutamiento P-NNI es muy complejo. Esta complejidad surge de las dos metas del protocolo: permitir una escalabilidad más grande que la de cualquier protocolo existente; y soportar enrutamiento basado en Calidad de Servicio (QOS).

Cabe mencionar que el conjunto de protocolos de P-NNI han sido desarrollados en dos fases: P-NNI fase 0 y P-NNI fase 1. La fase cero, también es conocido con el nombre de Protocolo Inter-Switch Interino (IISP). Ambos protocolos: P-NNI fase 1 y IISP, serán la interface con la señalización UNI 3.0/3.1; además soportaran las capacidades de dicha señalización.. Ninguno de estos protocolos soportará algunos aspectos de la señalización UNI 4.0, tales como: direccionamiento de grupo y negociación de parámetros de conexión ABR (Velocidad de Bit Disponible). Esta última funcionalidad será adicionada como parte de una posible especificación futura denominada P-NNI fase 2.

5.3.5.1 P-NNI Fase 1.

Una de las grandes ventajas de ATM es el soporte de conexión con una QOS garantizada. Así, un nodo que pide establecer una conexión, puede pedir cierta QOS de la red y la red debe asegurar aquella QOS por el tiempo de vida de la conexión. En UNI 3.0/3.1, los parámetros de tráfico y QOS pedidos para una conexión no pueden ser negociados en el establecimiento o tiempo de vida de dicha conexión. Esto será posible con UNI 4.0. Para entregar tal Calidad de Servicio garantizada, los ATM switches implememtan una función conocida como Control de Admisión de Conexión (CAC). La forma en que funciona CAC es la siguiente: cuando al ATM switch le llega un petición de conexión, este debe asegurarse de que la QOS pedida para dicha conexión, no afecte la QOS de las conexiones ya establecidas, el switch aceptará la conexión si tiene la capacidad

de seguir soportando las conexiones actuales (con sus propias QOS) y de dar a la conexión entrante la QOS requerida.

El protocolo de enrutamiento VC (Conexión Virtual), debe asegurarse que la petición de conexión sea enrutada a lo largo de una ruta que apunte al destino y tenga alta probabilidad de satisfacer la QOS pedida en el establecimiento de la conexión; esto es, que la ruta de la conexión cruce por ATM switches cuyo CAC local no rechace la llamada.

Para hacer lo anterior, el protocolo P-NNI utiliza un protocolo de enrutamiento de estado de la topología en el cual los nodos llevan QOS e información de alcance, tal que todos los nodos tienen información a cerca del alcance dentro de la red y los recursos de tráfico disponibles dentro de la red. Tal información es transmitida dentro de "Paquetes de Estado de la Topología P-NNI" (PTSP).

El protocolo P-NNI usa enrutamiento origen, en el cual el nodo inicial en la ruta determina la ruta entera hasta el nodo destino, esto con la idea de evitar la dificultad de hacer enrutamiento basado en QOS con un protocolo "salto por salto" (en lugar de enrutamiento origen), dado que cada nodo tendría que ejecutar un CAC local y evaluar la QOS a través de la red entera para determinar el próximo brinco.

La clave para la escalabilidad de P-NNI es su organización de red jerárquica. El protocolo P-NNI direcciones ATM de 20 bytes para identificar niveles en la jerarquía de red, con la idea de soportar un numero grande de niveles: un máximo de 104 (el número de bits en el prefijo de la dirección ATM), aunque no más que una media docena se usará, inclusive en redes globales.

El protocolo de enrutamiento ATM P-NNI fase 1, está bajo desarrollo del Forum ATM, además dado que como ya se menciono es un protocolo muy complejo no se profundizará más, debido a que no es una parte vital para los fines del trabajo de tesis que desarrollamos. Sin embargo, es preciso dejar claro que P-NNI es un protocolo muy importante para ATM, y su importancia aumenta si se pretende usar ATM a gran escala y con diversidad de servicios.

5.3.5.2 Protocolo Inter-Switch Interino

Mientras que el protocolo P-NNI fase 1 es extremadamente potente, es también muy complejo, lo cual tiene como consecuencia que su desarrollo total

tome mucho tiempo, y por lo tanto su implementación práctica demore. Desafortunadamente, sin el protocolo P-NNI no hay un estándar que permita a los usuarios construir redes de ATM switches de diversos fabricantes. Para resolver a corto plazo estos problemas, Cisco Systems Inc., propuso al Forum ATM el desarrollo de un protocolo de señalización muy simple basado en UNI, para interoperabilidad entre switches. El protocolo que se desarrolló es el P-NNI fase 0, mejor conocido como Protocolo Inter-Switch Interino (IISP).

Con el protocolo IISP, las peticiones de señalización son enrutadas entre switches usando tablas de prefijos de direcciones, configuradas dentro de cada switch ; esto evita la necesidad de un protocolo de enrutamiento VC (Conexión Virtual).Estas tablas son configuradas con los prefijos de direcciones que son alcanzables a través de cada puerto en el switch. Cuando una petición de señalización es recibida por un switch, vía un enlace IISP o UNI, el switch checa la dirección ATM destino contra la tabla de prefijos y nota el puerto con la coincidencia (byte por byte) mas grande ; y después lleva la petición de señalización a través de ese puerto usando señalización UNI. El IISP no tiene la misma escalabilidad que el protocolo P-NNI fase 1. Por ejemplo, la configuración manual de tablas de prefijos limita su aplicación a redes con únicamente un número pequeño de nodos.

Las implementaciones de IISP no serán compatibles con P-NNI fase 1, debido a que IISP usa señalización UNI y no señalización NNI. Los usuarios necesitarán mejorar sus switches cuando quieran implementar P-NNI.

El IISP no soporta enrutamiento basado en QOS, pero los nodos si pueden soportar Control de Acceso de Conexiones y se pueden configurar con rutas alternas o redundantes. A pesar de las limitaciones de IISP este sera ampliamente usado por lo siguiente : mientras que P-NNI fase 1 soporta enrutamiento basado en QOS, este es únicamente requerido para conexiones VBR y CBR, donde los sistemas finales pueden soportar una QOS específica. Los sistemas finales que piden conexiones UBR ó ABR, pueden especificar únicamente muy limitadas capacidades de QOS. Como tal, las métricas del protocolo P-NNI no se aplican a tales conexiones y deben ser enrutadas usando algún otro criterio (tal como: la ruta más corta).

La mayoría del tráfico de datos en redes ATM usará conexiones UBR ó ABR a corto y mediano plazo, dado que los protocolos de capas más altas no pueden especificar QOS (y entonces usan conexiones VBR). Dados todos estos factores,

se puede entender que IISP será ampliamente usado antes de la especificación final y desarrollo del protocolo P-NNI fase 1, aunque este último suplantará al primero a medida que aquél llegue a estar disponible.

5.4 PLANO DE ADMINISTRACIÓN

5.4.1 Interface de administración local interina (ILMI)

Como ya se había mencionado anteriormente, en el modelo de B-ISDN se definen tres planos: plano de usuario, plano de control y plano de administración. El Forum ATM ha desarrollado la Interface de Administración Local Interina (ILMI por sus siglas en inglés) basado en el Protocolo de Administración de Red Simple (SNMP), para realizar funciones del plano de administración.

Una Base de Información de Administración (MIB) especificada en la UNI, incluye suficientes "objetos administrables" para permitir el control y la configuración de nodos y terminales ATM.

Cada UNI física en un dispositivo tiene sus propios parámetros MIB, cubriendo todas las rutas y canales virtuales en la UNI. Dado que los dispositivos en ambos extremos de un enlace llevan las mismas conexiones,
porciones de las MIB`s son idénticas.

Para identificar cada ocurrencia de una MIB, puede asignarse una dirección a una UNI ATM, dicha dirección puede estar basada en un esquema privado (como la forma IEEE 802 de números binarios de 48 bits) o un número telefónico E.164. Ya sea que se trate de una dirección u otra, el único requerimiento es poner la dirección a todos ceros, indicando a la otra parte que la MIB se refiere a esta UNI.

La dirección UNI, cuando se aplica, organiza toda la información en la MIB. Los parámetros de configuración en la interface física y estadísticas de desempeño para esta son ordenadas por la dirección UNI. Sumando los VPI y VCI a la dirección crea un índice único para el uso de parámetros en canales o rutas individuales.

La ILMI supone que cada uno de los dispositivos ATM soporta al menos una interface UNI y tiene una Entidad de Administración UNI (UME) para cada UNI. Las UME´s en extremos opuestos de un enlace inter-nodal se comunican usando SNMP sobre una AAL y un VPI/VCI fijo. La dirección por default es VPI=0, VCI=16; AAL-5 seria requerida. En la figura 5.41 se muestra el contexto de ILMI.

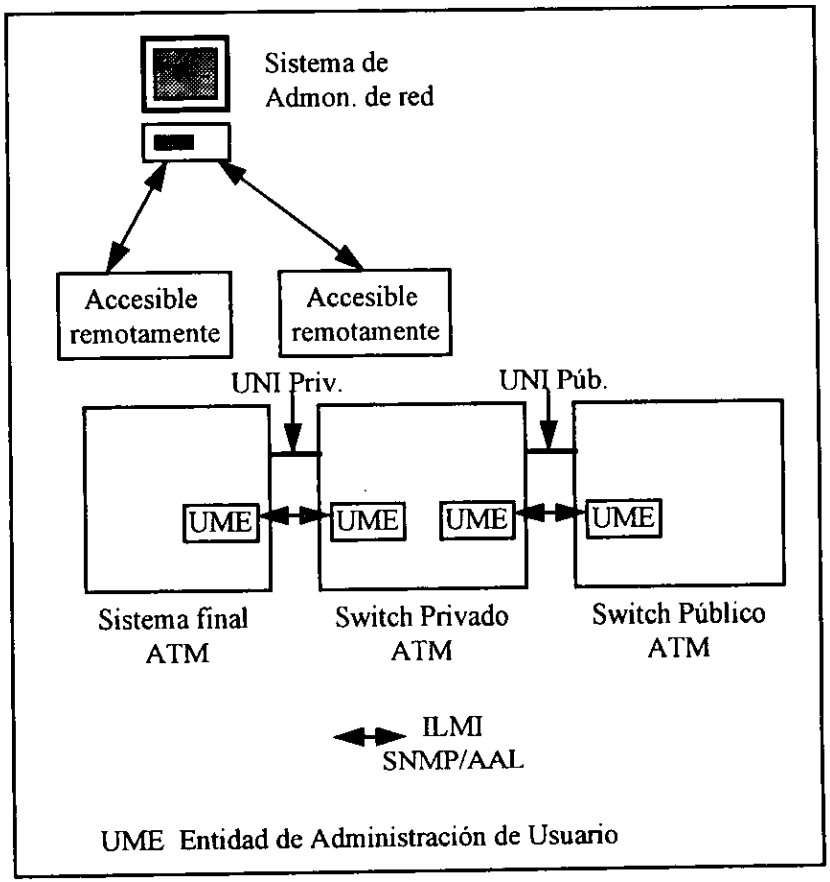


Figura 5.41 . Definición y contexto de ILMI.

Peticiones, respuestas y traps (mensajes enviados sin una petición previa) son diferenciados en el tipo de unidad de datos de protocolo (PDU) SNMP, no en el nivel de celdas ATM, de acuerdo al RFC-1157.

La información de administración definida por ILMI provee información de configuración y estado desde la UME, sin importar su UNI. Esta información detalla el estado y configuración de ambas, capa física y capa ATM en la UNI. Esta información es organizada dentro de la MIB, que contiene varios grupos de objetos administrables, como ya se había mencionado:

- Capa física
- Capa ATM
- Estadísticas de capa ATM
- VPC's y VCC's

Dentro de estos grupos, objetos administrados pueden pertenecer al sistema como un todo, una interface física, una interface de capa ATM, un canal virtual o una ruta virtual. Ejemplos de objetos definidos en la MIB UNI ATM incluyen:

- Tipo de transmisión (SONET STS-3c, DS3, etc.)
- Tipo de medio (coaxial, fibra monomodo, y más)
- Estado de operación (en servicio, fuera de servicio, y loop-back)
- Número máximo de VCC's
- Tipo de puerto UNI (privado o público)
- Celdas ATM recibidas, tiradas y transmitidas
- QOS transmitida
- Valor VPI/VCI

5.5 EMULACIÓN LAN (LANE)

5.5.1 Introducción

Muchas organizaciones están planeando migrar sus redes a ATM para satisfacer las demandas que surgen de ancho de banda para usuarios individuales y aplicaciones basadas en LAN. Aunque ATM está aun siendo desarrollada, puede usarse actualmente como una tecnología común y simple para redes LAN y WAN.

Como ya habíamos enfatizado al inicio del capítulo, existen muchas ventajas ofrecidas por ATM, entre las más sobresalientes tenemos:

- Velocidades más altas significativamente. desde 155 Mbps escalable hasta 622 Mbps ó más.

- La habilidad para transmitir voz, datos, video y tráfico multimedia con un uso del ancho de banda altamente eficiente.
- Una tecnología "internetworking" para implementación en redes privadas y redes públicas.

La cuestión para muchas organizaciones es como soportar las LAN´s Ethernet y Token Ring existentes mientras se hace una migración gradual a ATM ó se integra ATM en sólo ciertas partes de la red. Por una parte los usuarios quieren que sus aplicaciones corran transparente sobre la red, ya sea que se trate de una LAN Ethernet, LAN Token Ring ó LAN ATM. Por el otro lado, los administradores quieren formas para incrementar el desempeño de la red y asegurar interoperabilidad, en tanto que protegen la inversión existente en infraestructura LAN.

♦ **Conmutación LAN**

La implementación de **LAN switches** es la forma más económica de incrementar el ancho de banda disponible en LAN´s de medio compartido sin requerir cambios costosos adaptadores, alambrado, software de red, ó aplicaciones. Los LAN switches pueden entregar alta velocidad, conexiones LAN dedicadas a usuarios individuales y ancho de banda agregado para mejor desempeño en una red "backbone". Los LAN switches también habilitan la creación de LAN´s virtuales (VLAN´s) las cuales son agrupaciones de usuarios basadas en su función lógica más que en su ubicación física. En una red que incorpora tecnología LAN existente y ATM, es importante entender el significado de las funciones de conversión LAN a ATM. El protocolo LANE provee una opción para esta conversión.

♦ **Integración de LAN´s existentes a redes ATM**

Dos métodos pueden usarse para interconectar LAN´s sobre una red ATM. El primer método es protocolo en modo-nativo soportado sobre ATM, el cual ofrece la comunicación directa entre LAN´s operando sobre el mismo protocolo. Ruteadores multiprotocolo con interfaces ATM pueden rutear protocolos en modo-nativo sobre ATM y mover tráfico entre redes LAN sobre una red ATM. Dichos ruteadores tendrán la función de hacer que redes multiprotocolo coexistan y se integren con redes ATM nuevas. El soporte para protocolos en modo-nativo habilitaría a aplicaciones multimedia y aplicaciones sensitivas al retardo tomar ventaja de QOS de ATM. Sin embargo, nuevos estándares deben ser desarrollados para cada protocolo individualmente, ó un sólo estándar para soportar multiprotocolo. Se están haciendo esfuerzos para definir nuevos

estándares para operación de protocolo en modo-nativo sobre ATM. El protocolo IP ha recibido gran atención al respecto. La Comisión de Investigación de Ingeniería Internet (IETF por sus siglas en inglés) se ha definido IP clásica y ARP sobre ATM en el RFC 1577.

El Forum ATM ha establecido un grupo de trabajo para considerar el desarrollo de estándares de multiprotocolo sobre ATM (MPOA). Esto proveerá de un medio para extender el soporte de protocolo en modo-nativo más allá de IP.

El segundo método para interconectar redes LAN sobre una red ATM es "puenteando" a través de la tecnología LANE. LANE es un protocolo de "puenteo" de capa 2 que hace que una red ATM orientada a conexión se vea y parezca como un segmento LAN Ethernet o Token Ring sin conexión compartido. Como LANE es de capa 2, puede manejar tanto protocolos ruteables (TCP/IP, IPX y DECnet), así como protocolos no ruteables (NetBIOS y SNA-Arquitectura de Red de Sistema).

De los dos métodos ya mencionados, LANE ofrece varias ventajas. Con LANE, los usuarios pueden tomar ventaja de las altas velocidades soportadas por ATM y accesar a dispositivos ATM sin sustituir la inversión existente en hardware LAN, software, y aplicaciones. Ethernet, Token Ring, y estaciones finales ATM continuaran comunicandose como si estas estuvieran en la misma LAN usando procedimientos estándar, debido a que el backbone ATM es transparente al usuario. El protocolo LANE define como estaciones finales se comunican con otra a través de la red ATM, y como servidores ATM conectados se comunican con dispositivos en LAN's Ethernet y Token Ring.

5.5.2 Protocolo LANE

5.5.2.1 Necesidades Actuales

Los sistemas conectados directamente a una LAN "heredada" implementa la capa MAC apropiada a ese tipo de LAN. Los sistemas finales conectados directamente a una red ATM implementan protocolos ATM y AAL. Así, hay tres áreas de compatibilidad a considerar:

- Interacción entre un sistema final en una red ATM y un sistema final en una LAN heredada (Ethernet o Token Ring).

- Interacción entre un sistema final en una LAN heredada y un sistema final en otra LAN heredada del mismo tipo, por ejemplo Ethernet.
- Interacción entre un sistema final en una LAN heredada y un sistema final en otra LAN heredada de diferente tipo (por ejemplo una red IEEE 802.5 y una red IEEE 802.3).

Con LANE se satisfacen dos de los tres requerimientos anteriores:

- La forma en la cual sistemas finales en dos LAN's del mismo tipo (misma capa MAC) pueden intercambiar tramas MAC a través de la red ATM.
- La forma en la cual un sistema final en una LAN puede interoperar con un sistema final emulando el mismo tipo de LAN y conectado directamente a un switch ATM.

La especificación no dice nada sobre la interoperabilidad entre sistemas en diferentes redes LAN con protocolos MAC diferentes. Esta conectividad puede ser conseguida únicamente a través de un ruteador con ATM que actúe como cliente en cada LAN emulada. Así LANE para FDDI no ha sido definida; los paquetes FDDI deben ser convertidos a Ethernet o Token Ring antes de pasar por un servicio LANE. En la figura se tiene una configuración que puede ser construida usando LANE.

5.5.2.2 Arquitectura de Protocolo

En la figura 4.42 se indica la arquitectura de protocolo involucrada en una emulación LAN ATM. Allí, se ilustra la interacción de un sistema (servidor ATM, por ejemplo) ATM conectado con un sistema conectado a una LAN heredada. Como puede verse el sistema final conectado a la LAN heredada no es afectado: este es capaz de utilizar protocolos ordinarios, incluyendo el protocolo MAC específico para esta LAN y LLC corriendo sobre MAC. También este sistema corre TCP/IP sobre LLC, y a su vez varios protocolos de aplicación de TCP/IP funcionan como si no hubiera red ATM.

Como puede verse en la figura 5.42, se tiene un switch LAN que debe tener la capacidad de convertir tramas MAC en celdas ATM; y celdas ATM en tramas MAC. Esta es una de las funciones clave de LANE. La figura 4.52 se muestra el caso en el cual un host en una LAN heredada esta intercambiando datos con un servidor conectado directamente a una red ATM. Para lograr este intercambio, el host ATM debe incluir una capa LANE que acepte tramas MAC de AAL y

pase el contenido hacia arriba a la capa LLC. Entonces el host esta realmente emulando una LAN dado que este puede recibir y transmitir tramas MAC en el mismo formato como la LAN heredada distante. Desde el punto de vista de los sistemas finales en la LAN heredada, el host ATM es sólo otro sistema final con una dirección MAC. El proceso LANE es transparente para los sistemas existentes implementando LLC y MAC.

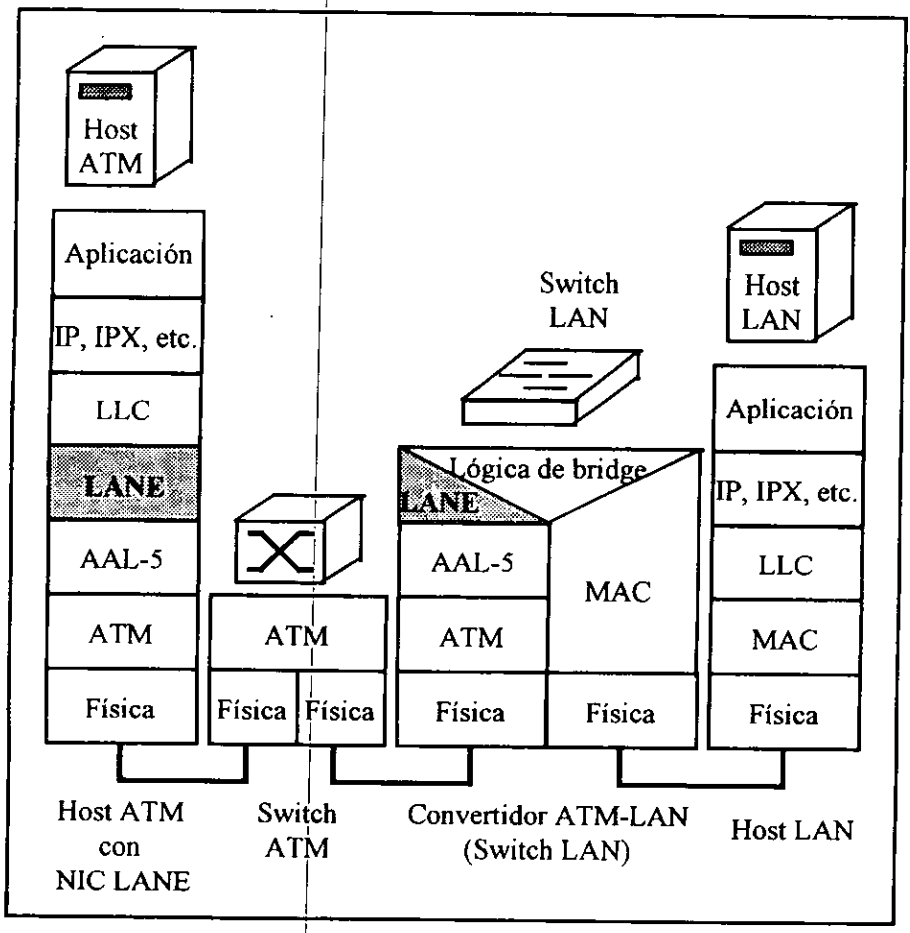


Figura 5.42. Arquitectura del protocolo LANE.

5.5.2.3 LAN's Emuladas

Una LAN emulada soporta un protocolo MAC sencillo, de los cuales están

definidos dos: Ethernet/IEEE 802.3 y IEEE 802.5 (Token Ring). Una LAN emulada de alguna combinación de los siguientes:

- Sistemas finales en una o más LAN´s heredadas.
- Sistemas finales conectados directamente a un switch ATM

Cada sistema final en una LAN emulada debe tener una dirección MAC única. El intercambio de datos entre sistemas finales en la misma LAN emulada involucra el uso del protocolo MAC y es transparente a las capas superiores. Para LLC parece que todos los sistemas finales en una LAN emulada están en la misma LAN de medio compartido. La comunicación entre sistemas finales en diferentes LAN´s emuladas es posible únicamente a través de ruteadores o "puentes". Los "puentes" o ruteadores tienen que reensamblar las celdas en paquetes, y dividir los paquetes en celdas para enviarlas a otra LAN emulada.

5.5.3 Componentes LANE

LANE sigue un modelo cliente/servidor, con múltiples clientes conectándose a componentes de emulación LAN. Los clientes son típicamente implementados en dispositivos tales como adaptadores o LAN switches, en tanto que los clientes LANE y Servidores de Emulación LAN (LES) pueden ser implementados juntos en un ruteador, switch LAN o ATM. Los servidores LANE también pueden ser distribuidos en diferentes ruteadores, switches o Hosts a través de la red ATM.

LANE define tres tipos diferentes de componentes: el Servidor de Emulación LAN (LES), el Servidor de Broadcast y Desconocido (BUS), y el Servidor de Configuración de Emulación LAN (LECS).

Estos servidores proveen los siguientes servicios:

- Asociar direcciones MAC a direcciones ATM
- Ejecutar transferencia de datos "unicast" y distribución de datos "multi/broadcast" entre clientes LANE en las LAN emuladas (ELAN´s).
- Mantener la relación entre LAN emuladas y VLAN´s.

5.5.3.1 Cliente de Emulación LAN (LEC)

Un LEC provee servicios de resolución de dirección y entrega de datos. Los

adaptadores ATM, ruteadores y switches LAN con interfaces ATM soportaran LEC's para proveer conectividad a un ambiente LAN ATM.

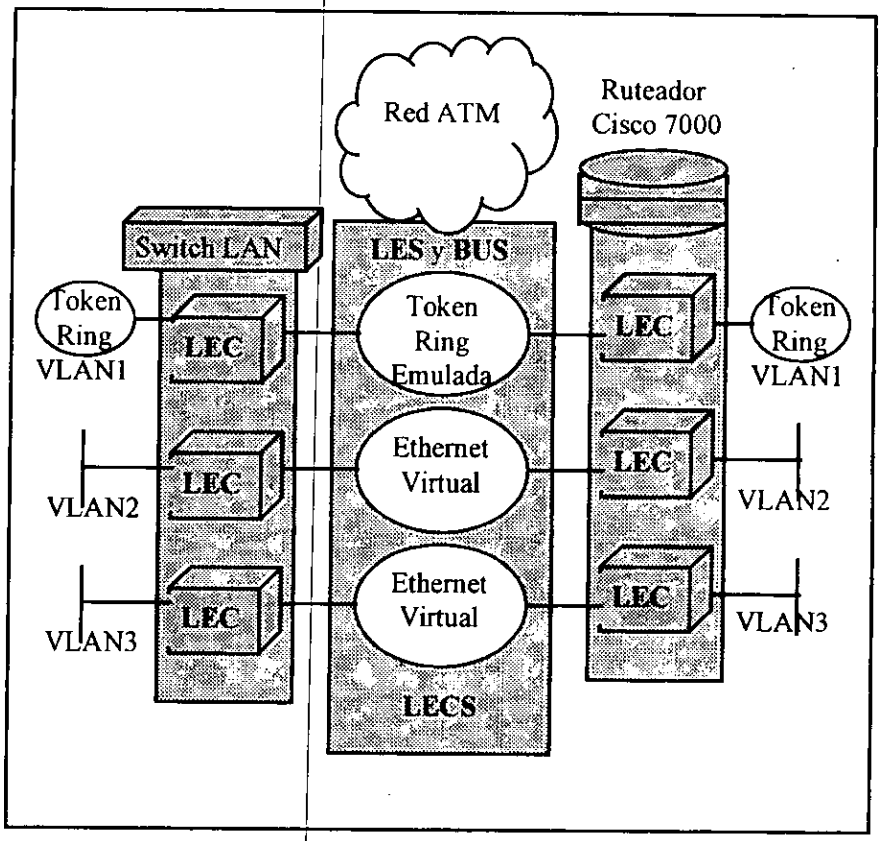


Figura 5.43. Componentes de LANE.

Un LEC provee una interface estándar Ethernet o Token Ring a cualquier entidad de capas más altas, tal como la capa 3 IP y protocolos IPX. Cada adaptador ATM, ruteador, o switch LAN puede soportar instancias de un LEC, con un LEC separado para cada ELAN.

5.5.3.2 Servidor de Emulación LAN (LES)

El LES provee servicios de resolución de dirección que asocian direcciones MAC Ethernet o Token Ring con direcciones ATM. El LES por si mismo está definido por una dirección ATM única.

Los LEC's se comunican directamente con otro únicamente cuando ellos están conectados al mismo LES. Sin embargo, múltiples LES's pueden existir en una misma LAN ATM física, donde cada LES soporta una LAN emulada diferente.

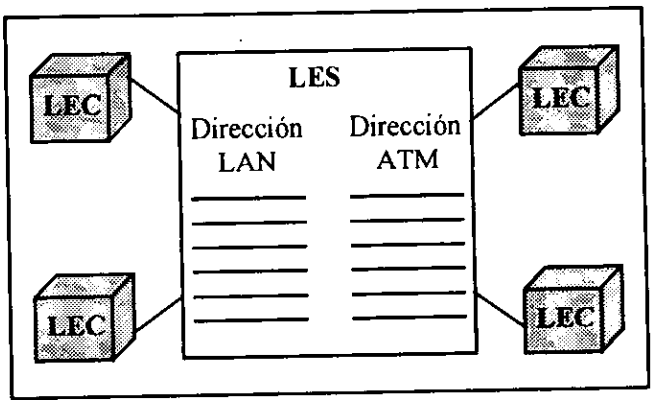


Figura 5.44. Resolución de dirección con LES.

5.5.3.3 Servidor de Broadcast y Desconocido (BUS)

El BUS recibe todos los paquetes broadcast y multicast y transmite estos mensajes a cada una de las LAN emuladas. Los paquetes multicast son importantes para aplicaciones tales como aprendizaje a distancia y para protocolos tales como IPX y NetBIOS que dependen mucho de paquetes multicast. Un LEC está asociado con un solo BUS para cada LAN emulada. Cada BUS está identificado por una dirección ATM única, la cuál, el LES asocia con una dirección MAC broadcast.

5.5.3.4 Servidor de Configuración de Emulación LAN (LECS)

El LECS mantiene información de configuración a cerca de la red ATM y suple la dirección del LES al LEC cuando este es inicializado. Con esta

información. Con esta información, los LEC´s pueden ejecutar su propia configuración y unirse a redes automáticamente. El LECS también habilita a los administradores de red para controlar cual LAN´s físicas son combinadas para formar VLAN´s.

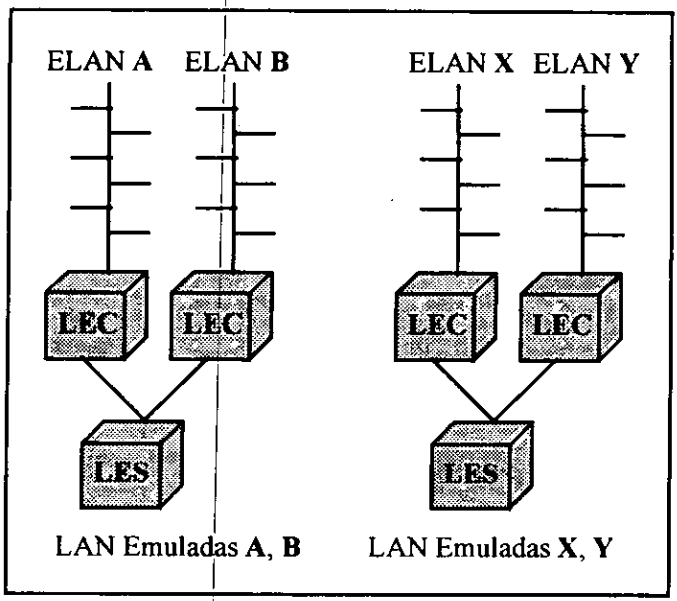


Figura 5.45. Un LES soporta más que una LAN emulada.

El LECS asigna clientes LANE individuales para emular LAN´s a través del LES. Un LECS sirve a todas las LAN´s emuladas dentro de un dominio administrativo.

5.5.4 Comunicación entre componentes LANE

Los componentes LANE se comunican con otros usando varios tipos de VCC´s. El LECS mantiene VCC´s separados para transmisión de datos y control de tráfico. Las conexiones de datos son definidas como sigue:

- VCC Directo de Datos, es una conexión bidireccional punto a punto entre un par de LEC´s para intercambio directo de datos. Una malla de estas conexiones existirá entre los LEC´s en una LAN emulada.

- VCC para Envío de Multicast, es una conexión bidireccional del LEC al BUS.
- VCC Hacia Multicast, es una conexión punto a multipunto unidireccional del BUS al LEC usada para comunicación broadcast y multicast.

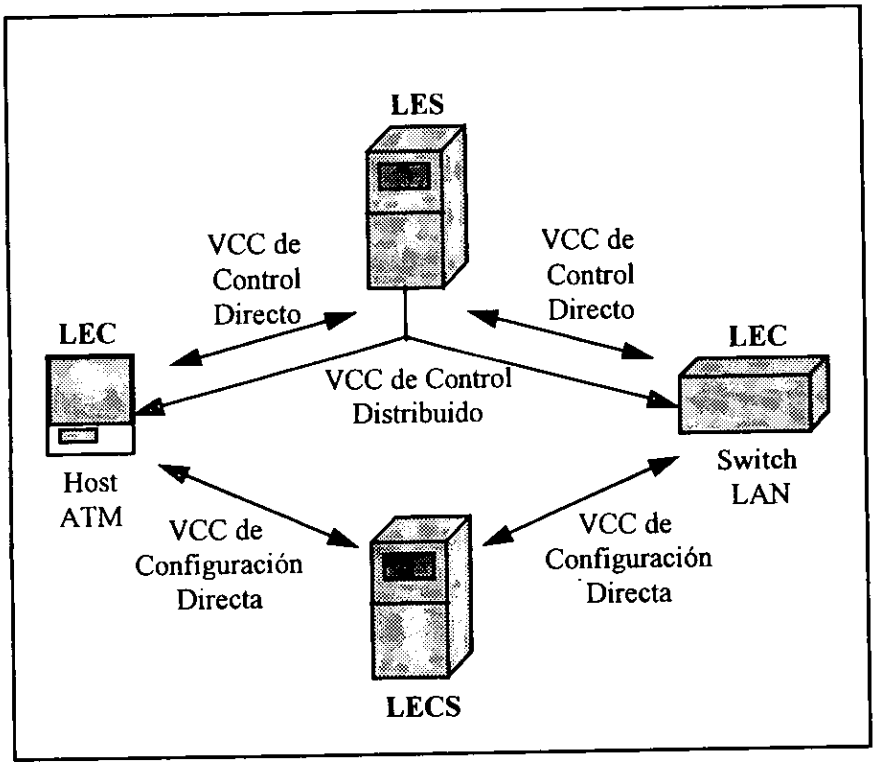


Figura 5.46. Comunicación entre componentes LANE.

Respecto de las conexiones de control tenemos:

- VCC Directo de Configuración, es una conexión punto a punto bidireccional del LEC al LECS.
- VCC Directo de Control, es una conexión punto a punto bidireccional del LES al LEC para distribución de tramas de control.
- VCC Distribuido de Control, es una conexión unidireccional, obligada desde el LES hacia el LEC que soporta peticiones broadcast ARP LANE.

5.5.5 Operación de LANE

La forma de operación del protocolo LANE es la siguiente:

♦ **Inicialización**

Para unirse a una LAN emulada, un cliente debe empezar por obtener la dirección ATM del LES para esa LAN emulada. La manera de hacerlo es establecer un VCC al LECS.

Hay tres posibles técnicas mediante las cuales un cliente puede descubrir la dirección ATM del LECS, de tal forma que el cliente pueda ejecutar la inicialización:

1. El cliente puede usar un procedimiento de administración de red definido como parte de la Interface de Administración Local Interina (ILMI) del Forum ATM. Este procedimiento toma lugar entre el cliente y el software ILMI en el switch ATM asociado. Si el software ILMI tiene la dirección del LECS, para la LAN emulada pedida, este provee esa dirección al cliente. El cliente entonces establece un VCC al LECS.
2. Si el procedimiento ILMI falla, el cliente trae una dirección predefinida listada en la especificación, denomina "dirección bien-conocida". Esta dirección se supone debe corresponder a un LECS en cualquier red ATM que cumpla con la especificación del Forum ATM. El cliente utiliza esta dirección para establecer un VCC al LECS.
3. Si el procedimiento anterior también falla, el cliente trae el VPI/VCI "bien-conocido" definido en la especificación del Forum ATM. Cuando la red es configurada, el administrador de la red puede establecer esta ruta virtual/canal virtual permanente.

♦ **Configuración**

Una vez que una conexión es establecida entre el cliente y el LECS, el cliente puede establecer un dialogo con el LECS. Basado en sus propias políticas, base de datos de configuración, e información provista por el cliente, el LECS asigna el cliente a un servicio de LAN emulada en particular, dándole al cliente la dirección ATM del LES. El LES regresa al cliente información acerca de la LAN emulada, incluyendo el protocolo MAC, máximo tamaño de trama, y el nombre de la LAN emulada. El nombre puede ser definido por el administrador de configuración, y tendrá significado en la definición de los grupos de trabajo lógicos.

♦ **Unión a una LAN Emulada**

Hasta aquí, el cliente tiene la información para unirse a una LAN emulada. El cliente ahora procede a establecer una conexión de control al LES, y emitirá un JOIN REQUEST (Petición de Unión) al LES, la cual incluye la dirección ATM del cliente, su dirección MAC, tipo de LAN, tamaño de trama máximo, un identificador de cliente, y una indicación "proxy". La última característica indica que este cliente corresponde a un sistema final conectado directamente a un switch ATM ó es un convertidor LAN a ATM (LAN switch con interface ATM, por ejemplo) soportando sistemas finales en una LAN heredada. Si el LES está preparado para aceptar esta cliente, entonces el LES regresa un JOIN RESPONSE (Respuesta de Unión) indicando aceptación. Puede darse el caso, de que el LES regrese un respuesta de indicación de rechazo.

♦ **Registro e Inicialización en el BUS**

Ya que el cliente se unió a una LAN emulada, este realiza un procedimiento de registro. Si el cliente es un proxy para un número de sistemas finales en una LAN heredada, este envía una lista de todas las direcciones MAC en la LAN heredada que van a ser parte de esta LAN emulada al LES. Después el cliente envía una petición al LES para la dirección ATM del BUS. Esta dirección funciona como la dirección broadcast para la LAN emulada y es usada cuando una trama MAC tiene que ser un broadcast a todas las estaciones en la LAN emulada. El cliente entonces establece una conexión de datos al BUS.

♦ **Transferencia de Datos**

Una vez que el cliente está registrado, este es capaz de enviar y recibir tramas MAC. Considerando el envío de tramas MAC, si un sistema final esta conectado a una switch ATM, el sistema final genera sus propias tramas MAC para transmisión a otros sistemas finales en la LAN emulada. En el caso de un cliente proxy, este funciona como un "puente" que recibe tramas MAC desde los sistemas finales en su LAN heredada y entonces transmite aquellas tramas MAC. En ambos casos, la trama MAC saliente debe ser segmentada en celdas ATM y transmitidas sobre un canal virtual. Hay tres casos que se deben considerar:

1. Si el cliente sabe la dirección MAC de una trama unicast, este verifica si se tiene una conexión de datos virtual ya establecida al cliente destino, si es así se envía la trama sobre esa conexión; si no, entonces se utiliza señalización ATM para establecer la conexión y después enviar la trama.
2. Si la dirección es desconocida, el cliente que envía ejecuta dos acciones. Primero, el cliente envía la trama al BUS sobre la conexión de datos que este mantiene con el BUS. El BUS puede hacer dos cosas: que transmita la trama a

la dirección MAC intentada, o si no, que haga broadcast con la trama a todos los destinos MAC en la LAN emulada. Si se hace el último caso, el destino reconocerá su dirección MAC y aceptará la trama. Segundo, el cliente intenta aprender la dirección ATM para esta dirección MAC para futura referencia. Esto lo hace mediante el envío de un comando LE_ARP REQUEST (Petición de Protocolo de Resolución de Dirección de Emulación LAN) al LES; el comando incluye la dirección MAC para la cual un dirección ATM se requiere. Si el LES sabe la dirección ATM, este regresa la dirección al cliente en un LE_ARP RESPONSE. De otro modo, el LES mantiene la petición mientras intenta aprender la dirección ATM. El LES envía su propio LE_ARP REQUEST a todos los clientes en la LAN emulada. El cliente que tenga la dirección MAC en cuestión regresará su dirección ATM al LES, el cual entonces enviará la dirección al cliente que hizo la petición original.

3. Finalmente, si la trama MAC es una trama broadcat o multicast, el cliente que desea transmitir envía la trama al BUS sobre la conexión de datos virtual que dicho cliente tiene hacia el BUS. El BUS entonces copia la trama y la envía sobre las conexiones de datos virtual a todos los clientes en esa LAN emulada.

5.5.6 Formatos de la Trama LANE

LANE puede usar dos tipos de formatos de trama: el formato de trama de datos usado sobre conexiones de datos entre clientes y entre un cliente y el BUS, y formatos de trama de control sobre conexiones entre clientes y el LES y LECS. La figura 5.48 muestra los formatos de la trama de datos. Un formato esta definido para una LAN emulada IEEE 802.3 y uno para una LAN emulada IEEE 802.5; debe tenerse presente que todos los sistemas finales en un LAN emulada deben usar el mismo protocolo MAC.

En cada caso, el formato es derivado de un formato de una trama MAC. Si consideramos primero el caso de IEEE 802.3. Cuando un cliente recibe una Unidad de Datos de Protocolo (PDU) LLC de la próxima capa más alta (Fig. 5.48), este construye una trama MAC para transmisión. Esta trama tiene el formato de una trama MAC ordinaria, con las siguientes excepciones. Primero, el campo de Secuencia de Chequeo de Trama (FCS) es omitido, esto elimina encabezadores innecesarios. Segundo, un encabezador de Emulación LAN (LE) es agregado. Este encabezador de 16 bits contiene el identificador del cliente. Cuando esta trama es recibida, por el cliente destino, el encabezador LE se quita . Si el cliente destino es un sistema ATM, este quita los campos MAC restantes y

pasa la información LLC hacia arriba. Si el cliente destino es un convertidor ATM a LAN conectado a una LAN IEEE 802.3, este quita el encabezador LE, agrega un campo FCS a la trama MAC y transmite la trama MAC en la LAN.

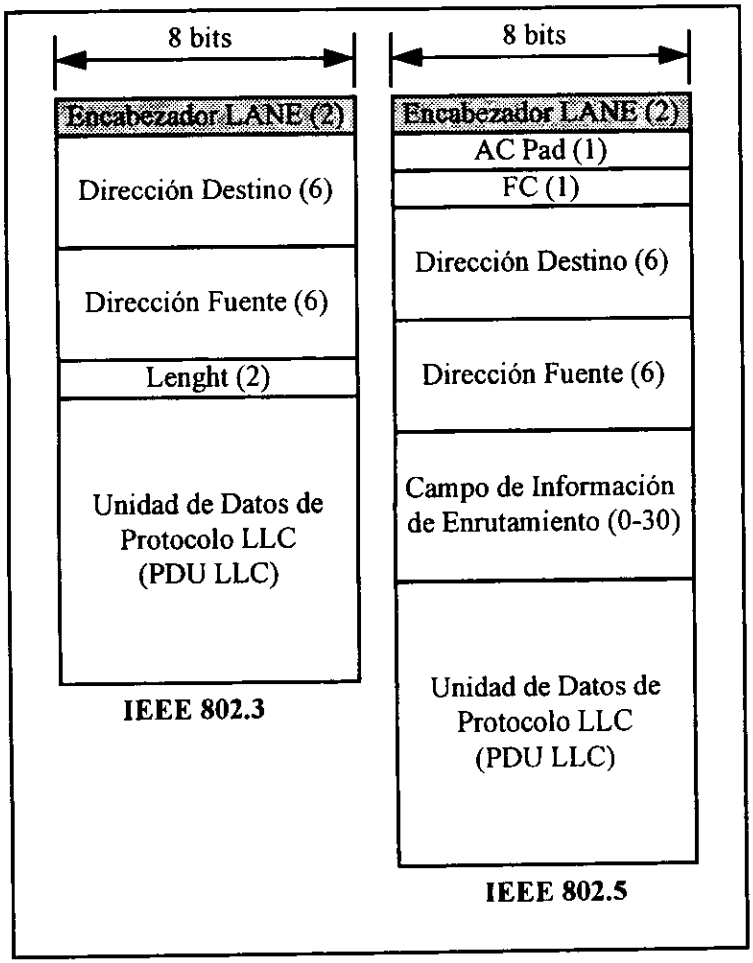


Figura 5.48. Formatos de la trama de datos LANE.

La operación para la trama MAC IEEE 802.5 es similar. También un encabezador LE es agregado. En este caso, los últimos tres campos de la trama se quitan: FCS, Delimitador de Fin (DE), y Estado de la Trama (FS). Si la trama es transmitida a una LAN Token Ring, los campos son restaurados.

En la figura 5.49 se tiene el formato de trama de control. Este consiste de los siguientes campos:

- Marker: puesto siempre a "FF00", indicando trama de control.

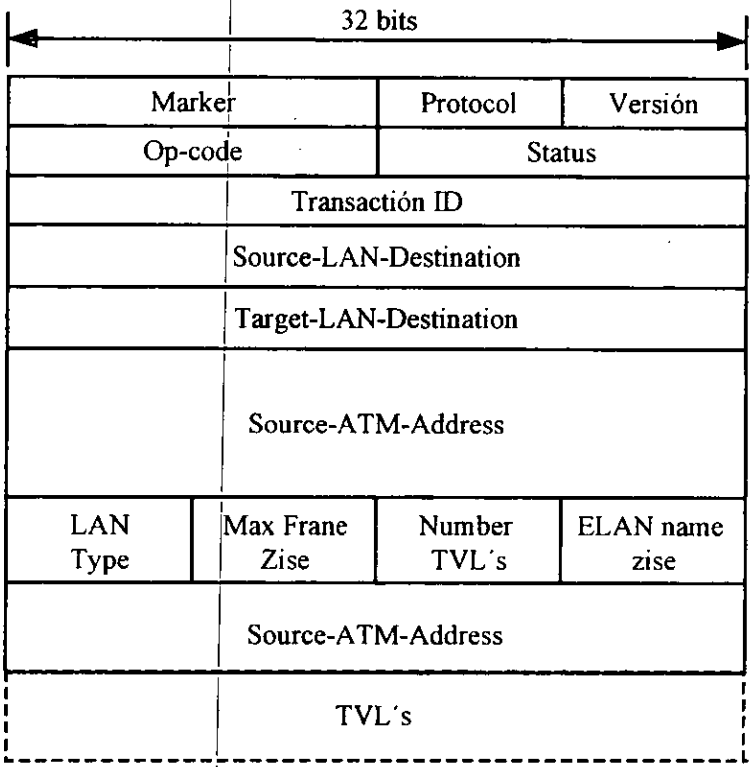


Figura 5.49. Trama de Control LANE.

- Protocol: siempre puesto a "01", indicando protocolo de Emulación LAN ATM.
- Versión: siempre puesto a "01", indicando versión 1.
- Op-code: tipo de trama de control; por ejemplo LE_CONFIGURE REQUEST y LE_ARP REQUEST.
- Status: puesto a cero en peticiones; usado en respuestas; ejemplo: parámetros de petición inválidos; direcciones ATM duplicadas; LAN destino invalida.

- Transaction ID: valor arbitrario asignado por el que hace la petición y usado por el que responde, tal que el que hace una petición pueda discriminar entre respuestas a diferentes peticiones salientes.
- Requester-LECID: identificador del solicitante.
- Flags: modificadores para ciertas respuestas.
- Source-LAN destination: LAN origen
- Target-LAN destination: LAN destino
- Source-ATM-address: dirección ATM del transmisor
- LAN Type: IEEE 802.3 o IEEE 802.5
- Max Frame Size: tamaño de trama máximo permitido en esta LAN emulada o el tamaño máximo de trama que el cliente aceptará.
- Number TLVs: numero de registros de valor-largo-tipo.
- ELAN name size: número de bytes del campo de nombre de ELAN.
- Target-ATM-address: dirección ATM de receptor.
- ELAN name: nombre asignado a esta LAN emulada.
- TLVs: una serie de parámetros que especifican a un código dado, cada uno consiste de un tipo (identifica al parámetro), largo (largo del valor en bytes) y valor (valor de parámetro).

5.5.7 Desventajas de LANE.

Las redes LANE son suceptibles a las mismas limitaciones de desempeño y escalabilidad inherentes que tiene las redes puenteadas tradicionales. La conectividad entre VLAN's aún requiere ruteadores tradicionales, los cuales pueden introducir cuellos de botella. Aun los ruteadores más rápidos, capaces de manejar 500,000 paquetes por segundo, ofrecen únicamente una fracción de la velocidad que ofrecen los ATM switches. A medida que el número de Hosts ATM conectados dentro de cada LAN emulada aumenta, el número de switches ATM crece, los ruteadores convencionales no serán capaces de soportar este crecimiento.

Estos ruteadores también introducen latencia: aún si la fuente y el destino estan conectados a ATM, la fuente tiene que establecer un circuito virtual (VC) ATM al ruteador, el cual establece otro circuito al destino.

La escalabilidad también puede ser un problema. La versión actual de LANE no permite que tráfico de múltiples LAN's virtuales compartan el mismo circuito virtual. Esto limita la escalabilidad debido a que a medida que el

número de LAN´s virtuales crece, el número de circuitos virtuales crece también y los switches no pueden soportar un numero infinito de circuitos virtuales. El Forum ATM está mejorando esta característica en LANE 2.0.

Como ya se vio, LANE efectivamente esconde los protocolos de la capa de red y más altos, de la fábrica ATM, lo cual introduce un nuevo conjunto de problemas. Uno es un overhead del protocolo adicional. Por ejemplo IP tiene que realizar pasos extra para encontar la dirección ATM destino. Estos pasos resultan en alta cantidad de tráfico broadcast. Dado que cada broadcast en un LAN emulada debe escuchar cualquier broadcast, esto desperdicia ciclos de reloj en todas las máquinas. Además el proceso consume ancho de banda en la red.

Dos problemas surgen del mapeo ATM a MAC:

- Primero, las aplicaciones que corren sobre una red LANE no pueden tomar ventaja de los atributos multimedia y QOS de ATM.
- Segundo, hay un impacto de desempeño que viene de las limitaciones de tamaño de trama máximo de LANE. Todos los dispositivos en una LAN emulada deben usar un mismo tamaño de trama, llamado Unidad de Transmisión Máximo (MTU). Las MTU´s en Ethernet son de 1500 bytes, pero los dispositivos conectados directamente a ATM pueden manejar MTU´s mucho más grandes, lo cual puede significar mucho mejor throughput. Pero en una LAN emulada con Ethernet y Host ATM, los dispositivos ATM deben usar la MTU Ethernet más pequeña.

El IETF ha definido especificaciones (IP sobre ATM) que resuelven algunos de los problemas anteriores. Lo que significa que redes IP pueden correr sobre ATM sin requerir software de LANE. Los RFC´s (Request For Coment) 1577 (IP clásico sobre ATM) Y 1483 (encapsulación multiprotocolo sobre AAL) definen formas de mapear directamente redes IP en la fábrica ATM.

5.5.8 LANE y LAN´s Virtuales (VLAN´s)

LANE es usado por vendedores para proveer un servicio de LAN virtual en backbones ATM. Tales LAN´s virtuales son implementadas en redes conmutadas que consisten de una combinación de LAN switches, sistemas finales ATM (típicamente servidores, usando Tarjetas Interface de Red / NIC) y ruteadores con interfaces ATM (ruteadores ATM), todos conectados a una ELAN. La ELAN parece una LAN normal en todo, excepto por el ancho de banda, según los sistemas finales estén conectados a los puertos LAN en un

switch LAN, o los protocolos de capas más altas operen dentro de host ó ruteadores ATM. Esta operación no difiere de ninguna manera desde el punto de vista de administración de la red, sin embargo, construir VLAN´s con LANE tiene ventajas significativas.

En particular, a través de la administración de la red y el uso de mecanismos tales como LECS, el administrador de la red puede establecer múltiples ELAN´s diferentes a través de un backbone ATM y entonces asignar puertos de un switch LAN o hosts ATM a diferentes ELAN´s, independientes de la ubicación física de los dispositivos. Esto es, a diferencia de las redes comunes donde la ubicación física de un dispositivo generalmente asigna el segmento LAN físico al cual el dispositivo puede ser conectado. Hoy, los usuarios ubicados físicamente juntos, deben ser puestos en la misma LAN. Esto fue aceptable en el pasado, donde los grupos de trabajo lógico, se hacían coincidir con la ubicación física de los dispositivos (servidores, clientes, etc.) necesarios para ese grupo de trabajo. El concepto de VLAN significa que personas que pertenecen a un grupo de trabajo lógico, no son restringidas a permanecer a una localidad física.

Los hosts que necesiten ser miembros de múltiples VLAN´s (por ejemplo, debido a que ellos pueden ser servidores que soporten aplicaciones comunes) pueden soportar múltiples LEC´s en sus NIC´s ATM y así actuar como un host en varias ELAN´s. Típicamente un puerto en un LAN switch, sería asignado a una sola ELAN.

La construcción de VLAN´s sobre LANE les dará a los administradores de red la habilidad de crear fácil y dinámicamente, además de reconfigurar dichas VLAN´s, para adaptar la red al flujo de trabajo, más que obligar a la organización a adaptar su trabajo a la topología de una red física.

Permitiendo la reconfiguración lógica centralizada de sistemas finales, sin requerir la reconfiguración de la red física, puede también ayudar a reducir el costo de "movimientos, adiciones y cambios", los cuales constituyen una proporción significativa del costo de soporte de la red, dado el dinamismo incrementado de los grupos de trabajo. Por ejemplo un nodo puede ser movido físicamente, pero aun el miembro en ese nodo puede seguir perteneciendo a la misma VLAN. De manera análoga, un nodo puede hacerse un miembro de una nueva VLAN a través de un cambio de su membresía en la ELAN, sin requerir ningún cambio físico en la red. En el último caso, dependiendo del protocolo, el nodo puede necesitar cambiar su dirección de capa de red (por ejemplo IP).

Estos beneficios potenciales de las VLAN´s promoverán un amplio desarrollo de LANE. Sin embargo las limitaciones de LANE también deben ser entendidas. LANE es en esencia un estándar de "puenteo" LAN. Como tal, como con las LAN´s "puenteadas" físicamente, las ELAN´s son susceptibles a fenómenos como tormentas de broadcast. Estos factores tienden a limitar la aplicabilidad de las ELAN´s a grupos pequeños, donde las VLAN´s también ofrecen las ventajas más sobresalientes. Esto significa que una red corporativa grande es propensa a soportar un numero grande de VLAN´s (ELAN´s).

Esto implica inmediatamente la necesidad de un medio que interconecte todas estas ELAN´s (para interconectar ELAN Token Ring y Ethernet, por ejemplo) entre ellas mismas y con redes existentes LAN y WAN. La forma más común mediante la cual esto puede ser hecho, es a través de ruteadores ATM. Así como los ruteadores convencionales conectan LAN´s físicas juntas, hoy; los ruteadores ATM interconectarán VLAN´s. Estos harán el soporte de interfaces ATM nativas de alto desempeño e implementaran LANE tal que el ruteador soportará múltiples LEC´s en cada interface ATM física nativa, una para cada ELAN que este interconecte.

Las VLAN´s ofrecen beneficios de costo y desempeño significativo, para la mayoría de las LAN´s instaladas hoy. Estos beneficios son palpables a medida que los administradores de red migran sus redes instaladas a una arquitectura de red conmutada. En tanto que las VLAN´s son parte integral de la arquitectura ATM, el concepto y mucha de la tecnología ha sido diseñada en LAN switches que ofrecen beneficios similares a través de backbones LAN compartidos. Además la aplicación de los usuarios finales no necesita ser cambiada para gozar de estos beneficios.

Las VLAN´s como parte de la arquitectura de conmutación, son invisibles a los usuarios finales. Las VLAN´s son más que un hub de medio compartido, enrutamiento, "conmutación" o solución de administración de red; las VLAN´s son la combinación de todos estos componentes que proveen una segmentación potente, y administración eficiente a través de la red.

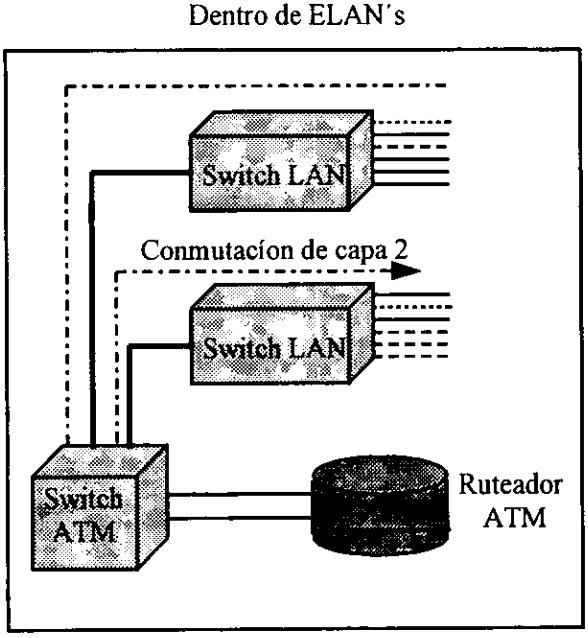


Figura 5.50a. Operación de VLAN's.

Los sistemas finales reconocerán, cuando un destino deseado está fuera la VLAN (ELAN) del nodo. En el caso de un nodo implementado IP, por ejemplo, típicamente cada VLAN será asociada con un número de subred IP único. Por lo tanto un nodo en una ELAN ejecutará un proceso sobre la dirección IP destino para determinar que el nodo no está en la subred propia del nodo fuente (por lo tanto la ELAN). El nodo entonces llevará el paquete, usando protocolos LANE, su ruteador por default; este ruteador también será miembro de la ELAN, y por lo tanto será alcanzable a través de la ELAN. Si el nodo destino está en la misma subred - por consiguiente en la VLAN - una conectividad directa será posible, por supuesto sin requerir involucrar un ruteador.

Una vez que el paquete alcance el ruteador, este consultará sus propias tablas de próximo brinco para determinar a donde llevará el paquete. Si estas tablas indican que el destino es alcanzable a través de otra ELAN, de la cual el ruteador es miembro, el ruteador entonces llevará el paquete a esa ELAN, posiblemente sobre la misma interface física sobre la cual el paquete fue recibido primero, pero ahora en una nueva ELAN. Puede verse que el procesamiento de protocolos de capas más altas dentro del ruteador no es afectado por el hecho de que el

ruteador está ahora negociando con LAN's emuladas y no con LAN's fisicas. Esta es otra característica de LANE, el hecho de esconder las complejidades de la red ATM.

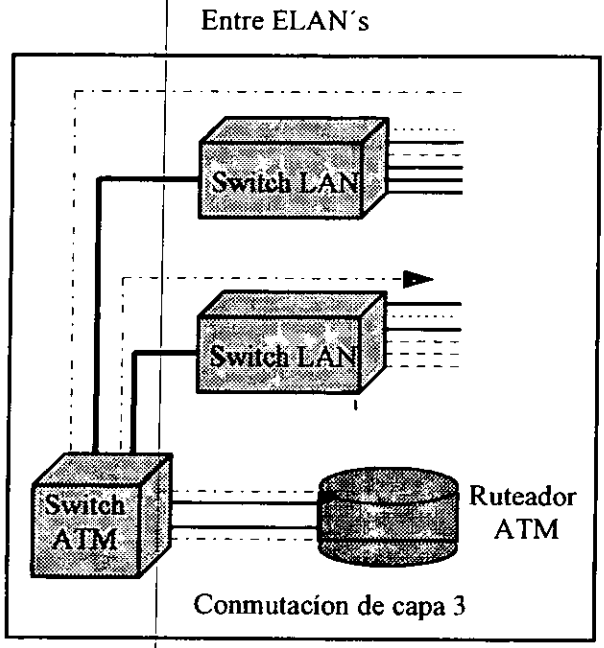


Figura 4.50b. Operación de VLAN's.

Una desventaja clara de este planteamiento, sin embargo, es que el ruteador ATM puede llegar a ser un "cuello de botella" dado que todo el tráfico inter-ELAN deberá pasar por el ruteador. LANE por si mismo tiene otra limitación. Por definición, la función de LANE es esconder las propiedades de ATM de los protocolos de capas más altas. Esto es bueno a corto y mediano plazo, dado que esto excluye la necesidad de hacer cambios en estos protocolos. Por otro lado, LANE también impide que esos protocolos hagan uso de los beneficios únicos de ATM, específicamente de las características de QOS de ATM. LANE esta definido para usar únicamente conexiones UBR y ABR; en un futuro, protocolos de capas más altas pueden tener la necesidad real de utilizar esas propiedades (esto es, uso de conexiones VBR). Por último es necesario notar que LANE no es el único medio para soportar VLAN's.

5.6 IP SOBRE ATM

5.6.1 Introducción

IP sobre ATM (RFC 1577) utiliza la AAL-5 de ATM para llevar datagramas IP, y así transferirlos a través de la red ATM. Viéndolo de una manera 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 AAL-5. Entonces el emisor puede pasar un datagrama completo IP hacia AAL-5 para entregarlo a través de circuito. Con AAL-5 el datagrama IP es dividido y transportado en celdas en la red ATM. En el lado receptor, AAL-5 reensambla el datagrama, y utiliza la información del "trailer" que la información recibida del datagrama IP es correcta.

Dentro del campo de información de AAL-5 se pueden transportar hasta 65,000 octetos en un solo paquete. Si TCP/IP restringe el tamaño de los datagramas que pueden enviarse en una red ATM. El estándar impone un límite de 9,180 octetos por datagrama. Esto es IP impone una Unidad de Transferencia Máxima (MTU) de 9,180 octetos en redes ATM. Es decir, AAL-5 acepta transfiere y entrega datagramas de 9,180 octetos.

5.6.2 Formato del paquete IP en AAL-5

Dado que AAL-5 no incluye un campo de tipo, de tal forma que una trama AAL-5 no es autoidentificable. La forma sencilla de encapsulación supuesta en la introducción, no es suficiente. Y en realidad puede haber dos posibilidades:

- Que las dos computadoras en los dos extremos del circuito virtual acuerden a priori que el circuito debe utilizarse para un protocolo específico. Es decir, el circuito no será únicamente para enviar datagramas IP.
- Las dos computadoras en los dos extremos del circuito virtual acuerdan a priori que algunos octetos del área de datos serán reservados para utilizarse como un campo de tipo.

En el caso en que las computadoras acuerdan un protocolo de alto nivel para un circuito dado, tiene la ventaja de no necesitar información adicional en un paquete. Así, si las computadoras acuerdan transferir IP, un emisor puede transferir cada datagrama de manera directa hacia AAL-5; no se necesita enviar información adicional, aparte del datagrama y el "trailer" AAL-5. La

desventaja, es que se debe tener un circuito virtual para cada protocolo de alto nivel (IP, IPX).

En el segundo caso, dos computadoras utilizan un circuito virtual para varios protocolos lo cual tiene la desventaja de que cada paquete debe tener un campo que identifique el tipo de protocolo. También se tiene la desventaja de que todos los protocolos viajan con el mismo retardo y la misma prioridad.

TCP/IP especifica que las computadoras pueden seleccionar entre los dos métodos de AAL-5. Tanto el emisor como el receptor deben acordar como utilizar el circuito. TCP/IP sugiere que cuando las computadoras eligen incluir un campo de tipo en el paquete, estas deben utilizar el encabezador IEEE 802.2 (Control de Enlace Lógico/LLC) seguido por un encabezador de Punto de Conexión a la Subred (SNAP). La figura 5.51 ilustra la información LLC/SNAP prefijada para un datagrama antes de ser enviado hacia un circuito virtual ATM. En dicha figura también se muestra el formato completo del paquete utilizado para enviar un datagrama IP sobre AAL-5. El encabezado LLC/SNAP de 8 octetos identifica el contenido como un datagrama IP.

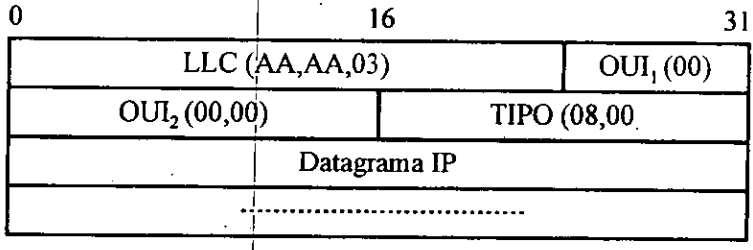


Figura 5.51. Formato del paquete utilizado para llevar IP en AAL-5.

En el formato anterior, LLC consiste de 3 octetos que contienen el valor hexadecimal AA.AA.03. El encabezado SNAP consiste de 5 octetos: 3 que contienen un Identificador Único Organizacional (OUI), y 2 para el tipo. El campo OUI identifica una organización que administra los valores del campo de Tipo, y el campo Tipo identifica el tipo de paquete. Para un datagrama IP, el campo OUI contiene 00.00.00 que identifica la organización responsable de los estándares Ethernet, y el campo de Tipo contiene 08.00, el valor utilizado cuando se encapsula IP en una trama Ethernet. El software en el host emisor debe prefijar el encabezador LLC/SNAP para cada paquete antes de enviarlo hacia

AAL-5, el software en el host de recepción debe analizar el encabezador para determinar como manejar el paquete.

5.6.3 Direcciones IP en una red ATM

La asignación de direcciones IP en una red ATM es más complicado que la encapsulación de IP en celdas ATM. 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 una parte, como las direcciones físicas de ATM son más grandes que las direcciones IP , una dirección física ATM no puede codificarse dentro de una dirección IP. Así, IP no puede utilizar la asignación de direcciones estáticas para redes ATM. Por otro lado, el hardware ATM no soporta el broadcast como tal. Por lo tanto, IP no puede utilizar el ARP convencional para asignar direcciones en redes ATM.

Los circuitos virtuales permanentes complican más la asignación de direcciones. Debido a que un administrador configura manualmente cada PVC, un host sólo conoce el VPI/VCI. El software en el host no conoce la dirección IP ni la dirección de hardware del extremo remoto. Un mecanismo de asignación de direcciones IP debe proporcionar la identificación de una computadora remota conectada a un PVC así como la creación dinámica de SVC's para destinos conocidos.

Las tecnologías de conmutación orientadas a la conexión requieren dos niveles de asignación. Primero, cuando crean un circuito virtual sobre el que serán enviados los datagramas, las direcciones IP de los destinos deberán transformarse en direcciones de los puntos extremos ATM. Las direcciones de los puntos extremos se usan para crear un circuito virtual. 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 a una red ATM: el primer direccionamiento es necesario sólo cuando un host crea un SVC.

5.6.4 Concepto de Subred IP Lógica.

Aunque ningún protocolo ha sido propuesto para resolver el caso general de

asignación de direcciones para redes ATM extensas, un protocolo se perfila como una solución restringida. La restricción radica en que el grupo de computadoras utilizan una red ATM en lugar de una red física única (a menudo local). El grupo forma una Subred IP Lógica (LIS). Varias subredes IP lógicas pueden definirse entre un conjunto de computadoras conectadas al mismo hardware de red ATM. Por ejemplo, la figura 5.52 ilustra 8 computadoras conectadas a una red ATM dividida en dos LIS.

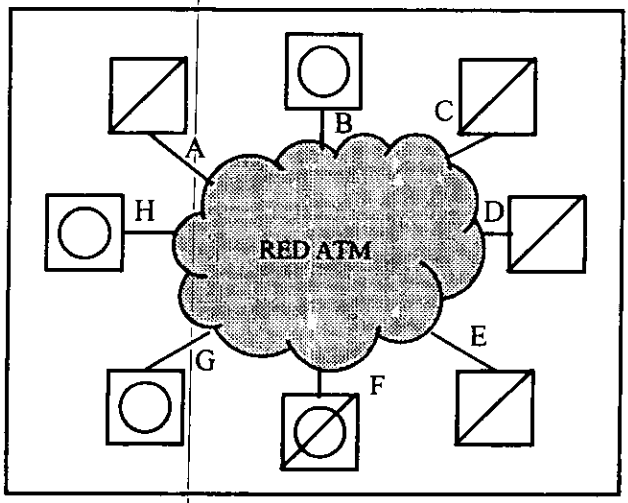


Figura 5.52. Computadoras conectadas a una red ATM que participan en dos subredes IP lógicas.

En la figura se ven que todas las computadoras están conectadas a una red física ATM. Las computadoras A, B. C, D y F participan en una LIS, mientras que las computadoras B, F, G y H participan en otra LIS. Cada LIS funciona como una LAN separada. Las computadoras participan en la LIS estableciendo circuitos virtuales con el fin de intercambiar datagramas. Todas las computadoras en una LIS comparten un sólo prefijo de red IP y este prefijo difiere de los utilizados en otras subredes lógicas. Todas las computadoras deben utilizar la misma MTU en todos los circuitos virtuales que comprenden la LIS. Finalmente, aunque el hardware ATM proporciona la conectividad potencial, una computadora en una LIS no debe comunicarse en forma directa con otra computadora en otra LIS. De hecho, todas las comunicaciones lógicas entre sus redes deben proceder a través de un ruteador que participe entre varias subredes lógicas. En la figura el dipositivo F puede ser un ruteador IP entre las dos

subredes IP lógicas dado que participa en ambas.

5.6.5 Gestión de conexiones

Un host debe mantener un registro de circuitos abiertos conforme estos son utilizados. La administración de circuitos se da en el software de interface de red más allá de IP. Cuando un host necesita enviar un datagrama, se vale del ruteo IP convencional para encontrar la dirección del próximo salto apropiado N (una dirección IP), y lo pasa hacia la interface red. La interface de red examina la tabla de circuitos abiertos. Si hay un circuito abierto para N, el host emplea AAL-5 para enviar el datagrama. Si no hay un circuito virtual abierto hacia N, antes de que el host puede enviar el datagrama deberá localizar una computadora con dirección N, crean un circuito y añadir un circuito a su tabla.

El concepto de LIS restringe el ruteo IP. En una tabla de ruteo configurada adecuadamente, la dirección del próximo salto para cada destino debe ser una IP con la misma subred lógica que el emisor. La restricción viene del hecho de cada dirección del próximo salto en la tabla de ruteo debe ser un ruteador conectado con la LAN.

Una de las razones para tener subredes lógicas proviene de las restricciones del hardware y el software. Un host no puede mantener un número extenso de circuitos virtuales abiertos al mismo tiempo, ya que cada circuito requiere recursos en el hardware ATM y en el sistema operativo. Si se crean LIS, se limita el número máximo de circuitos abiertos simultáneamente al número de computadoras en la LIS.

Cuando un host crea un circuito virtual para una computadora en su LIS, el host debe justificar una dirección ATM de hardware para el destino. El problema es que el host transforme la dirección del próximo salto en la dirección de hardware ATM apropiada. El host no puede hacer una solicitud a todas las computadoras en la LIS por que ATM no ofrece un hardware de broadcast, en lugar de ello, contacta un servidor para obtener la transformación. La comunicación entre el host y el servidor utiliza ATMARP, una variante del protocolo ARP.

Como con un ARP convencional, un host forma una solicitud que incluye las direcciones de hardware y las direcciones IP y ATM del emisor, 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 LIS. Si el servidor conoce la dirección de hardware ATM, envia una respuesta ATMARP. De otro forma, el servidor envía una respuesta ATMARP negativa.

5.6.7 Formato del paquete ATMARP

En la figura 4.53 se tiene el formato del paquete ATMARP. Este difiere ligeramente del paquete ARP convencional. El cambio más notorio es que el paquete ATMARP comprende los campos de longitud y dirección adicional para adaptarse a las direcciones ATM. El cambio se debe a que han sido propuestas varias formas para direcciones ATM, y que no se sabe cual de ellas quede como estándar. Los formatos de direcciones propuestas para ATM ya se mencionaron en una sección anterior. Las compañías telefónicas que ofrecen redes públicas ATM se valen de un formato de 8 octetos donde la dirección es un número E.164. por otro lado, el Forum ATM permite que cada computadora conectada a una red ATM privada sea asignada a 20 octetos una dirección de Punto de Acceso al Servicio de Red (NSAP). Como tal, se necesita una dirección jerarquizada de dos niveles para especificar una dirección, E.164 para una localidad remota y una dirección NSAP de un host en un conmutador local.

Con el fin de 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. En la figura ATMARP comienza con campos de tamaños fijos que especifican longitudes de dirección. El primero de los dos campos sigue el mismo formato que un ARP convencional. El campo Tipo de Hardware (Hardware Type) contiene el valor hexadecimal 0x0013 para ATM, y el campo Tipo de Protocolo (Protocol Type) contiene el valor 0x0800 para IP.

Dado que el formato de las direcciones fuente y destino pueden diferir, cada dirección ATM requiere un campo de longitud. El campo SEND HLEN especifica la longitud de la dirección ATM del emisor y el campo SEND HLEN2 especifica la longitud de la subdirección ATM del emisor. Los campos TAR LEN y TAR LEN2 especifica la longitud de la dirección ATM del destino y de su subdirección. Los campos SEND PLEN y TAR PLEN especifican la longitud de las direcciones de protocolo emisor y receptor.

Tipo de Hardware (0x0013)		Tipo de Protocolo (0x0800)	
SEND. HLEN (2	SEND. HLEN2 (	Operación	
SEND. PLEN (4	TAR. HLEN (0	TAR. HLEN2 (0	TAR. PLEN2 (4
Dirección ATM del Emisor (octetos 0-3)			
Dirección ATM del Emisor (octetos 4-7)			
Dirección ATM del Emisor (octetos8-11)			
Dirección ATM del Emisor (octetos 12-15)			
Dirección ATM del Emisor (octetos 16-19)			
Dirección del Protocolo del Emisor			
Dirección ATM del Destino (octetos 0-3)			
Dirección ATM del Destino (octetos 4-7)			
Dirección ATM del Destino (octetos 8-11)			
Dirección ATM del Destino (octetos 12-15)			
Dirección ATM del Destino (octetos 16-19)			
Dirección del Protocolo del Destino			

Figura 5.53. Formato del paquete ATMARP en el que se utilizan 20 octetos para las direcciones, como lo recomienda el Forum ATM.

Aparte de los campos de longitud, en el encabezador de ATMARP se tienen 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 los mismo, pero para el destino.

5.6.7.1 Formatos de los campos de longitud de la dirección ATM

Dado que ATMARP esta diseñado para utilizarse con direcciones 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 y longitud en un campo de 8 bits.

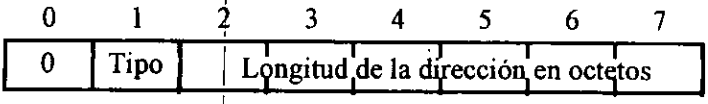


Figura 5.54. Codificación de un tipo de dirección ATM en un campo de 8 octetos.

Con un sólo bit se codifica el tipo de dirección ATM pues sólo se dispone de dos formas posibles. Si el bit 1 se pone a cero, la dirección tiene el formato NSAP recomendado por el Forum ATM. Si el bit se pone 1 se pone al valor de uno, la dirección está en el formato E.164. Como cada campo de longitud de dirección ATM en un paquete ATMARP tiene la forma mostrada en la figura 5.54, un sólo paquete puede contener varios tipos de direcciones ATM.

Código	Significado
1	Solicitud ATMARP
2	Respuesta ATMARP
8	Solicitud ATMARP inversa
9	Respuesta ATMARP inversa
10	Acuse de recibo negativo ATMARP

Tabla 5.10. Valores que puede tomar el campo de operación.

5.6.7.2 Campo de Operación en el paquete ATMARP

Con el paquete ATMARP se solicita una asignación de dirección y también se solicita una asignación de dirección inversa. Cuando una computadora envía un paquete ATMARP, debe poner el campo de Operación a uno de los siguientes códigos de la Tabla 5.10, para especificar el tipo de asignación.

5.6.8 Operación de ATMARP

Dado que el hardware ATM soporta dos tipos de circuitos virtuales, se tienen dos casos: para un PVC y para un SVC.

- **Circuitos virtuales permanentes**
  Dado que los PVC's son configurados por el administrador de la red, los hosts no participan en la configuración del PVC. Un host comienza la operación

con el PVC ya instalado en su lugar, y no recibe ninguna información acerca de las direcciones de los puntos extremos remotos. A menos que la información haya sido configurada en el host (almacenada en disco duro), el host no tiene conocimiento de las direcciones IP o las direcciones ATM de la computadora a la que se conecta un PVC.

El protocolo ATMARP inverso, es el que resuelve el problema de encontrar una dirección cuando se emplea un PVC. Para utilizar el protocolo, una computadora debe conocer cada uno de los PVC´s que han sido configurados. Para determinar las direcciones IP y ATM de un punto extremo remoto, una computadora envía un paquete de Solicitud Inversa ATMARP, con el campo de operación puesto en 8. Cada vez que llega una solicitud en un PVC el receptor genere una Respuesta Inversa ATMARP en el campo de operación puesto en 9. Tanto la Solicitud como la Respuesta, contienen la dirección IP del emisor y la dirección ATM. Así, una computadora ubicada en cada extremo de la conexión aprende la asignación para la computadora ubicada en el otro extremo.

- **Circuitos Virtuales Conmutados**

Dentro de una LIS las computadoras crean SVC´s en función de la demanda. Cuando una computadora X desea enviar un datagrama a una computadora Y, y no existe en ese momento un circuito a Y. La computadora X utiliza la señalización ATM para crear el circuito necesario. Así, X comienza con la dirección IP de Y, la cual debe ser trasformada en una dirección ATM equivalente. Se dice que cada LIS tienen un servidor ATMARP y todas las computadoras en una LIS deben ser configuradas de tal forma que tengan conocimiento acerca de como alcanzar el servidor (es decir, una computadora puede tener un PVC al servidor, ó la dirección ATM del servidor almacenada en disco). Un servidor no forma conexiones hacia otras computadoras, el sólo espera que las computadoras en la LIS se pongan en contacto. Para transformar la dirección IP de Y en dirección ATM, la computadora X forma un paquete de Solicitud ATMARP y lo envía sobre la conexión hacia el servidor. El campo de Operación en un paquete contiene 1, y el campo de dirección de protocolo destino contiene Y (protocolo de Y).

El servidor ATMARP mantiene una base de datos de las transformaciones de direcciones IP en direcciones ATM. Si el servidor conoce las direcciones ATM de Y, el protocolo ATMARP opera de manera similar a Proxy ARP. El servidor forma una Respuesta ATMARP, con el campo de Operación puesto en 2 y llenar la dirección ATM que corresponda a la dirección IP del destino. Como en un

ARP convencional, el servidor intercambia las entradas del emisor y destino antes de regresar la respuesta a la computadora que envió la solicitud.

Si el servidor no contiene la dirección ATM que corresponde a la dirección IP de destino en una solicitud. ATMARP difiere de ARP. En lugar de ignorar la solicitud, el servidor devuelve un acuse de recibo negativo (un paquete ATMARP con el campo de Operación en 10). Un acuse de recibo negativo distingue entre direcciones para las que un servidor no tiene una asignación y un servidor con falla de funcionamiento. De tal manera que cuando un host envía una solicitud a un servidor ATMARP, determina un de tres posibilidades: la dirección ATM del destino, si el destino no está actualmente disponible en la LIS o si el servidor actualmente no está respondiendo.

♦ **Registro de direcciones IP en el servidor ATMARP.**

Un servidor ATM elabora y mantiene automáticamente su base de datos de asignaciones. Para hacerlo utiliza ATMARP Inverso. Cada vez que un host o un primer ruteador abre un circuito virtual hacia el servidor ATMARP, el servidor inmediatamente envía un paquete de Solicitud Inversa ATMARP. El host o el ruteador deben responder enviando un paquete de Respuesta Inversa ATMARP, el servidor extrae las direcciones IP y ATM del emisor y almacena la asignación en su base de datos. Así, cada computadora en una LIS debe establecer una conexión hacia el servidor ATMARP, aun cuando la computadora no consulte las asignaciones.

♦ **Permanencia de asignaciones en el servidor ATMARP.**

La asignación obtenida por ATMARP debe ser cronometrada y eliminada si es necesario. Una vez que una computadora registra sus asignaciones con un servidor ATMARP, el servidor conserva la entrada de la información por un mínimo de 20 minutos. Después el servidor examina la entrada de la información, si no existe un circuito hacia la computadora que envió la entrada de información, el servidor borra la entrada. En cambio si la computadora que envió la entrada mantiene un circuito virtual abierto, el servidor revalidará la entrada. El servidor envía una Solicitud ATMARP y espera una Respuesta. Si la Respuesta verifica la información en la entrada, el servidor espera otros 20 minutos. Si la Respuesta Inversa ATMARP no concuerda con la información de la entrada, el servidor borra la entrada y cierra el circuito.

Por otra parte, un host o un ruteador deben también utilizar temporizadores para invalidar la información obtenida desde un servidor ATMARP. Un host o

ruteador puede tomar una asignación obtenida de un servidor ATMARP por un máximo de 15 minutos. Cuando se alcanza los 15 minutos, la entrada debe ser revalidada o removida. Si una asignación de dirección expira, y el host no tiene un circuito virtual abierto para el destino, el host retirara la entrada de su memoria intermedia ARP. Si un host tiene un circuito virtual abierto hacia el destino, el host intentará revalidar la asignación de direcciones. La finalización de tiempo de validez de una asignación de direcciones puede retrasar el tráfico debido a que:

- Un host o ruteador debe dejar de enviar datos a cualquier destino para el que la asignación de direcciones ha expirado hasta que la asignación pueda revalidarse.

El método que un host emplea para revalidar una asignación depende del tipo de circuito que se este utilizando. Si el host puede alcanzar el destino con un PVC, el host envía una Solicitud Inversa ATMARP en el circuito y espera una Respuesta. Si el host tiene un SVC abierto hacia el destino, el host envía una Solicitud ATMARP hacia el servidor ATMARP.

- **Ventajas y desventajas de IP sobre ATM.**

Mapeando IP a ATM elimina algunas de las limitaciones de LANE. Por ejemplo este elimina el overhead de protocolo resultante de la translación de dirección. Con IP sobre ATM, peticiones de ARP son llevadas directamente al serviodr de ARP, el cual contesta con la dirección ATM. Con esto la estación originante puede establecer una conexión ATM al destino. De esta forma se reducen el número de pasos necesarios para establecer una conexión, minimizando el tráfico broadcast y mejorando la latencia. Otra ventaja de mapear IP directamente sobre ATM, es la habilidad de usar grandes MTU's debido a que los dispositivos de la capa de red entienden como manejar la fragmentación IP.

Una desventaja significativa del RFC 1577 es que como LANE, necesita un ruteador convencional para interconectar difrentes subredes, por lo tanto los problemas de throughput y latencia aun permanecen. El IETF esta desarrollando el Protocolo de Enrutamiento de Próximo Brinco (NHRP), el cual ayudará a resolver este problema. Otra limitación es que estos RFC's (a abril de 1996) no definen el manejo de broadcast o multicast.

Como su propio nombre lo indica, solo está definido el manejo de IP sobre ATM. Hay aun la necesidad de una forma para manejar el ruteo de otros

protocolos de capa de red.

5.7. MULTIPROTOCOLO SOBRE ATM.

5.7.1 Introducción

Mucho se ha dicho de ATM: alta velocidad, escalabilidad y la posibilidad de crear redes virtuales, sin embargo esto no es suficiente. Dado que como ya también se vio (con LANE e IP sobre ATM), existe la necesidad de un mecanismo para integrar las redes multiprotocolo de hoy con ATM, un esquema que permita a los administradores de red que puedan construir redes escalables y administrables, sin requerir un cambio que deseche Ethernet, Token Ring e infraestructuras TCP/IP en su totalidad.

En el Forum ATM está bajo desarrollo (abril de 1996) una solución llamada Multiprotocolo Sobre ATM (MPOA por sus siglas en inglés). En esencia MPOA expande los equemas como LANE (del Forum ATM); así como IP sobre ATM, Protocolo de Enrutamiento de Próximo Brinco (NHPR), y Servidor de Resolución de Dirección Multicast (MARS) estos tres últimos conceptos desarrollados por el IETF. Lo que hace diferente a MPOA es su habilidad para integrar estas soluciones como un todo. MPOA introduce un nuevo concepto: Ruteadores Virtuales.

Hay tres cosas que MPOA resuelve:

- Este define una forma de alto desempeño y baja latencia para llevar IP y otros protocolos a través de una fábrica de conmutación ATM.

- También da la posibilidad a los administradores de red construir redes virtuales, de tal forma que los usuarios puedan ser agrupados juntos como parte de una red virtual sin importar donde se localizan fisicamente en la red, aún si ellos no están conectados directamente a ATM.

- MPOA permite que el tráfico sea llevado directamente a su destino sobre un circuito virtual de un solo brinco. Mediante el mapeo directo de los protocolos de la capa de red a ATM, MPOA reduce tráfico broadcast y overhead sobre la red; y soporta Unidades de Protocolo Máxima (MPU's) máxima. Finalmente MPOA permite a las aplicaciones utilizar las aplicaciones de QOS de ATM.

5.7.2 Arquitectura MPOA.

La arquitectura MPOA comprende los siguientes componentes:

- ***Edge devices***. Algunas veces referidos como switches multicapa, los "edge devices" son switches inteligentes que usan ya sea la dirección de capa de red o su dirección de la capa MAC para llevar paquetes entre segmentos de LAN´s heredadas e interfaces ATM.

- ***Host ATM-conectados.*** Estos son Hosts con tarjetas ATM que implementan MPOA como parte de sus "drivers". MPOA permite a los Host con tarjetas ATM comunicarse eficientemente con otro host con tarjeta ATM o con LAN´s heredadas conectadas mediante un "edge device".

- ***Servidores de rutas.*** No son dispositivos físicos como tales, los servidores de rutas son una colección de funciones que hacen posible a las subredes de la capa de red ser mapeadas en ATM. Los servidores de rutas pueden ser implementados como productos aislados, o ellos pueden consistir de software agregado a ruteadores existentes o switches.

5.7.3 Servicio de ruteo

En esencia, los servidores d rutas asumen las funciones del BUS, LES en LANE. Los servidores de rutas mantienen información de direcciones ATM, direcciones MAC y direcciones de la capa de red, la cual es usada para establecer circuitos virtuales directos entre dos dispositivos finales cualesquiera ("edge devices" o Hosts conectados a ATM) que quieren comunicarse uno con otro. Para comunicarse información de enrutamineto con ruteadores convencionales, los servidores de rutas corren protocolos como RIP (Protocolo de Información de Enrutamiento), OSPF y IPNNI (Interface Red a Red Privada Integrada).

En lugar de LAN´s emuladas, MPOA define grupos de direcciones o subredes virtuales. Estas denotan ambos, un protocolo de capa 3 y una rango de direcciones. En otras palabras, las subredes virtuales definen un grupo de hosts unidos y un protocolo particular que los une. Por ejemplo una subred virtual puede consistir de una subred IP, lo que significa los dispositivos IP asociados, más el protocolo IP.

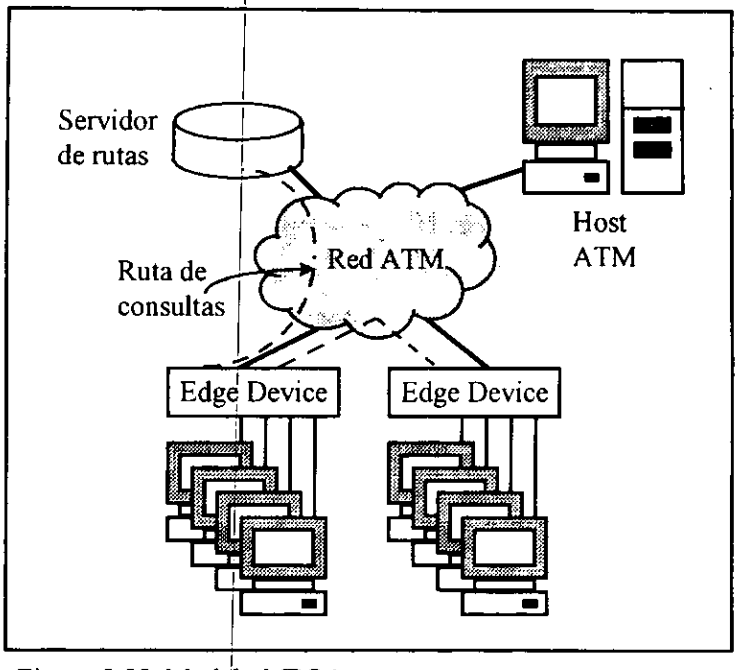


Figura 5.55. Modelo MPOA.

El Grupo de Trabajo MPOA a acordado que el tráfico de sus subredes virtuales sea compatible con LANE. Esto significa que los adaptadores (ATM cards) y los "edge devices" que incorporen software de LANE podrán comunicarse con dispositivos MPOA si ellos están dentro del mismo grupo de direcciones, por ejemplo si todos los dispositivos caen dentro de la misma subred IP.

Permitir a hosts comunicarse con otros dispositivos en otros grupos de direcciones, requiere más que lo anterior. En particular, las tarjetas y switches deben soportar MPOA más que sólo LANE y un servidor de rutas debe estar presente. "Edge devices" con LANE únicamente, pueden comunicarse con otros grupos de direcciones MPOA solamente a través de un ruteador ó "gateway" que soporte LANE y MPOA.

5.7.4 Ruteadores Virtuales

Un aspecto clave del modelo MPOA es su ya mencionado ruteador virtual, el cual es un conjunto de dispositivos MPOA operando sobre una fábrica ATM que colectivamente proveen la funcionalidad de un ruteador multiprotocolo, figura 5.55. Dado que los "edge devices" aceptan datos de un subred conectada, ellos son análogos a las tarjetas interface del ruteador. La fábrica de conmutación ATM puede ser vista como el backplane del ruteador, enlazando los "edge devices". El servidor de rutas es análogo al procesador de control

El modelo MPOA distribuye el enrutamiento entre dispositivos "edge devices", los cuales llevan paquetes, los servidores de rutas, los cuales suplen información de enrutamiento. El tráfico entre VLAN´s no va a través del servidor de rutas.

La idea de ruteo virtual hace posible entregar funciones de enrutamiento más eficientemente de lo que lo hacen los ruteadores de hoy: los "edge devices" no tienen que ser tan inteligentes como los ruteadores para IP sobre ATM. Las dos cosas anteriormente mencionadas hacen más eficiente la escalabilidad dado que agregar capacidad para llevar paquetes solo significa agregar switches, y agregar capacidades de ruteo adicional solo significa agregar software al servidor de rutas. La administración se facilita: la arquitectura del ruteador virtual como un todo, comprende múltiples switches y servidores de rutas, que pueden ser administrados como un ruteador sencillo. Finalmente, el enrutamiento virtual permite la creación de subredes virtuales, dado que los grupos de direcciones pueden contener hosts que pueden caer dentro de cualquier lugar en la red..

El modelo MPOA básicamente divide la funcionalidad de enrutamiento entre el servidor de rutas y los "edge devices", la estandarización de este protocolo significa que los "edge devices" de un fabricante será capaz de trabajar con los servidores de rutas de otro. Aunque, ambos: "edge devices" y servidor de rutas pudieran estar en la misma caja.

5.7.5 Operación de MPOA.

Los "edge devices" examinan la dirección destino del paquete recibido en segmentos de LAN heredados, y deciden como llevar estos paquetes. Si el paquete no necesita salir del grupo de direcciones MPOA, el trabajo del "edge

device" esta hecho: este solo puentea el paquete, usando LANE para resolver la dirección ATM y establecer el circuito virtual al destino.

Si el paquete debe ser ruteado, el "edge device" lo examina para determinar la dirección destino de la capa de red del "edge device" y ve la correspondiente dirección ATM a esa dirección de capa de red. El "edge device" entonces establece un circuito virtual directo al destino apropiado.

El " edge device" (ED) obtiene la dirección ATM ya sea de su servidor de rutas o de su memoria cache. El servidor de rutas sabe, o puede usar varios protocolos de enrutamiento para descubrir, la dirección ATM de cualquier dispositivo en la red. Sin embargo, la meta del diseño es minimizar el número de veces que el DE debe visitar el servidor de rutas para recuperar esta información. Para este fin, el DE mantiene su propia cache de direcciones.

No hay un punto en el proceso en el que el paquete deba ser llevado a un ruteador estándar. En lugar de ello, la conmutación de paquetes es manejada por el ED, mientras que el servidor de rutas ejecuta resolución de enrutamiento y dirección. Se espera que esta arquitectura elimine los cuellos de botella en escalabilidad y desempeño, mencionados anteriormente.

Si el servidor de rutas local no conoce la dirección ATM apropiada, este puede propagar la pregunta a otros servidores de rutas. La dirección ATM que el ruteador provee es la dirección del host destino (si el host está conectado a ATM) ó la dirección del DE al cual el host no-ATM está conectado.

Una de las preocupaciones del Grupo de Trabajo MPOA, es que MPOA pudiera interoperar con arquitecturas ruteadas. El ruteador virtual MPOA entero (incluyendo ED's, servidores de rutas, e infraestructura ATM) está diseñado para trabajar con los ruteadores existentes usando los protocolos de los ruteadores de hoy. Esto hará posible que los administradores de red usen MPOA en conjunción con, más que en remplazo de sus redes ruteadas.

CAPITULO 6

INTEGRACION DE LAN SWITCHES EN ATM

6.1 INTRODUCCIÓN

Hasta ahora hemos analizado las tecnologías de redes LAN más populares: Ethernet, Token Ring, FDDI y Fast Ethernet; también llamadas redes LAN heredadas. Por otra parte también se trató el tema de la arquitectura de red TCP/IP, lo cual es el conjunto de protocolos más utilizado a nivel mundial, sin embargo no es el único.

En el capítulo 4 se enfoco al tema de LAN switches, se vieron sus ventajas y la necesidad de utilizarse en conjunto con los ruteadores. El capítulo anterior fue dedicado a enumerar las características más sobresalientes de ATM, su operación, los problemas que resuelve y las opciones que hay para integrar ATM como backbone de redes corporativas, sin que haya necesidad de un cambio en las aplicaciones de datos.

En el presente capítulo se detalla el funcionamiento de LAN switches cuando tienen instalada una ó más interfaces ATM, también se describen cada uno de los componentes necesarios para una red conmutada. Además se enumeran las características principales que se deben tomar en cuenta en un LAN switch cuando este será conectado a una red ATM, las características de un ATM switch para que satisfaga las necesidades (voz, datos y video: juntos) del usuario y lo más sobresaliente de un ruteador conectado a ATM.

6.1.1 LAN "switching" y ATM.

Ambos, LAN "switching" y ATM ofrecen incremento substancial en el ancho de banda de la red. LAN "switching" da un ancho de banda dedicado a cada conexión, en lugar del ancho de banda compartido de las LAN's tradicionales. ATM tiene un amplio rango de aplicaciones, incluyendo redes WAN y promete traer soluciones de alta velocidad.

ATM y LAN "switching" pueden ser complementarios. Las dos tecnologías pueden ser usadas juntas para resolver problemas de ancho de banda para pequeños campus ó grandes empresas.

Los principales beneficios de los productos LAN "switching" son: el mejoramiento de la compatibilidad y el throughput con conexiones LAN existentes. Para aplicaciones que requieren acceso a velocidad completa (full speed) a recursos de cómputo, una conexión de un LAN switch provee desempeño significativamente más grande que las LAN's convencionales de medio compartido. LAN "switching" es atractivo como una solución a corto plazo, dado que las Workstations pueden ser conectadas al puerto de un LAN switch sin necesidad de que sea mejorada con una NIC (tarjeta de red) cara. Los usuarios Ethernet existentes pueden ser conectados con sus NIC's y alambrado existentes, a diferencia de que si se quieren conectar a FDDI, 100Base-T, o ATM tienen que comprar nuevas NIC's, y en algunos casos nuevo alambrado. Mediante la posposición del cambio a una nueva tecnología completamente al escritorio, la inversión existente es preservada. Otro beneficio adicional de LAN switching es la posibilidad de crear VLAN's.

En tanto que el mercado de LAN switching está en su apogeo hoy, el mercado para productos ATM comienza a tomar fuerza. ATM está empezando a reemplazar backbones de FDDI y algunos backbones bridge/ruteador colapsados. Habrá un incremento en la demanda de los backbones ATM a medida que los LAN switches con muchos puertos puedan generar una gran cantidad de tráfico, algunas veces excediendo las velocidades tales como 100 Mbps. de FDDI.

ATM al escritorio está aún limitado ha aplicaciones de muy alto desempeño. Hay pocas aplicaciones compatibles con ATM y las Interfaces de Programación de Aplicación (API's) necesarias están siendo escritas. Por ahora, ATM está apareciendo principalmente en los backbones, mientras LAN switching domina en conectividad al escritorio y grupos de trabajo.

6.1.2 Integración de Redes Compartidas y Conmutadas.

El cambio de LAN's conmutadas a LAN's compartidas no tiene por que ser abrupto. Dado que no todos los usuarios necesitan una conexión de 10 Mbps. dedicada, y aún pocos necesitan una conexión de alta velocidad, las redes compartidas coexistirán con LAN switching y ATM. LAN switching y ATM

pueden complementarse una con otra para formar una solución híbrida para redes escalables de alto desempeño.

Los LAN switches pueden ser usados para resolver problemas de ancho de banda a medida que estos surjan. Se pueden emplear LAN switches en etapas, gradualmente remplazando hubs de medio compartido, los cuales pueden ser movidos a áreas de ancho de banda más bajo. Los usuarios que estén satisfechos con una LAN de medio compartido de 10 Mbps., pueden permanecer en una LAN de medio compartido, los cuales pueden ser conectados directamente a un puerto Ethernet conmutado.

Usuarios potentes o servidores pueden ser conectados directamente a un puerto de 10 Mbps. en el LAN switch, para ancho de banda dedicado. Los servidores pueden también ser conectados con enlaces de alta velocidad, tales como: Fast Ethernet o FDDI.

Los ATM switches pueden ser integrados con LAN´s de medio compartido o con LAN´s conmutadas para proveer backbones de alta velocidad, no sin antes hacer adaptaciones al tráfico LAN para correr sobre ATM, como ya se había hecho notar en el capítulo anterior.

6.2 COMPONENTES DE UNA RED CONMUTADA

Una red conmutada esta compuesta de tres componentes fundamentales:

- Plataformas de conmutación.
- Una infraestructura de software común.
- Aplicaciones y herramientas de administración.

Nuestro trabajo está enfocado principalmente al primer punto: plataformas de conmutación, dado que ahí es donde encontramos a los LAN switches y ATM switches.

Sin embargo, es importante notar que el software está directamente relacionado con las plataformas de conmutación, además para estar preparado para resolver fallas en la red y tener información con la finalidad de escalarla, es indispensable un buen sistema de administración de red.

6.2.1 Elementos de una plataforma de conmutación

Existe una arquitectura para redes conmutadas propuesta por Cisco Systems, Inc. llamada CiscoFusion, en la cual se dice que los elementos fundamentales para este tipo de redes son:

- LAN switches.
- ATM switches.
- Ruteadores.

A continuación se describen cada uno de estos elementos, y su función dentro de una red conmutada:

1. LAN switches

Los LAN switches más populares son los Ethernet LAN switch (también existen FDDI LAN switch y Token Ring LAN switch) los cuales son actualmente un tipo de BRIDGE multipuerto. Los Bridges ofrecen la característica de limitar el dominio de colisiones. Los LAN switch hacen lo mismo, pero además son mucho más rápidos. Los LAN switches mueven paquetes tan rápido, que pareciera que efectúan varias "conversaciones" al mismo tiempo. Cuando el LAN switch tiene un puerto de ATM, debe tener cargado el software de LANE (LAN Emulation) de tal forma que cada uno de sus puertos Ethernet pueden ser un LEC (Cliente de LANE), lo que significa que cada puerto correspondería a una LAN emulada.

Los tipos de Ethernet LAN switch en el mercado pueden ser clasificados de la siguiente manera:

- **LAN switch de grupo de trabajo.** La idea de utilizar un LAN switch de este tipo es incrementar el ancho de banda para un grupo de trabajo pequeño, típicamente un servidor y sus clientes. Dado que estos switches tienen capacidad para 4000 direcciones MAC en sus tablas de direcciones, pueden ser usados como LAN switch de segmento. Un ejemplo de este tipo de switch es el HP AdvancedStack Switch 200.

- **LAN switch de segmento.** Los switches de segmento son para interconectar grupos de trabajo, switches de grupo de trabajo ó hubs de medio compartido. Estos switches tienen tablas de direcciones más grandes, son más flexibles en la configuración de sus puertos y soportan velocidades de throughput más altas. El HP AdvancedStack Switch 2000 y el LANplex 2500 de 3Com son un LAN switch de segmento.

- **LAN switch de backbone.** Este tipo de LAN switch es usado para interconectar un sitio grande y proveer conectivididad para sitios remotos. El switch de backbone es altamente modular y tiene conexiones FDDI, Fast Ethernet y/o ATM. Algunas veces tienen funciones de enrutamiento básicas. Ejemplos de esto switches son: LANplex 2500, CELLplex 7000, LANplex 6000 todos de 3Com. Cisco Systems Inc., tiene su familia de LAN switches Catalyst con varios modelos que dependen de su funcionalidad.

Las características más sobresalientes que deben ser tomadas en cuenta cuando se elige un LAN switch para ser conectado a ATM y en general para cualquier LAN switch son:

- Interfaces ATM que cumplan con estándares (STM-1 por ejemplo).
- Soporte de IISP (Protocolo Inter-Switch Interino) y P-NNI (protocolo Interfaz Nodo-Red Privado).
- Soporte de LANE 1.0 y posibilidad de soportar 2.0.
- Soporte de VLAN´s.
- Posibilidad de ser "edge devices" en una arquitectura MPOA en un futuro.
- Soporte del protocolo Inter-Swictch Link o 802.10 para manejo de VLAN´s.
- Soporte de interfaces 10Base-T, 100Base-T y FDDI, dependiendo de las necesidades.
- Ancho de banda en su backplane acorde a su aplicación.
- Posibilidad de administrarlo vía SNMP, vía consola, manejo de TFTP para descarga de software.
- Observar detenidamente características de valor-agregado que cada fabricante pone en sus LAN switch (fuentes de potencia redundantes, por ejemplo.)

2. ATM switches

Dentro de un red conmutada, la función de los ATM switches es de ser el backbone de la red y proveer conexiones ATM a servidores de muy alto desempeño, pero también llevar otros tipos de tráfico tales como voz y vi deo, con la finalidad de consolidar la red, para tener un mejor manejo del ancho de banda, escalabilidad y disminución de los gastos de operación. Aunque todos los ATM switches conmuten celdas, estos difieren marcadamente en cuanto a sus capacidades, interfaces y servicios soportados, redundancia, software ATM interworking y la sofisticación de la administración de tráfico.

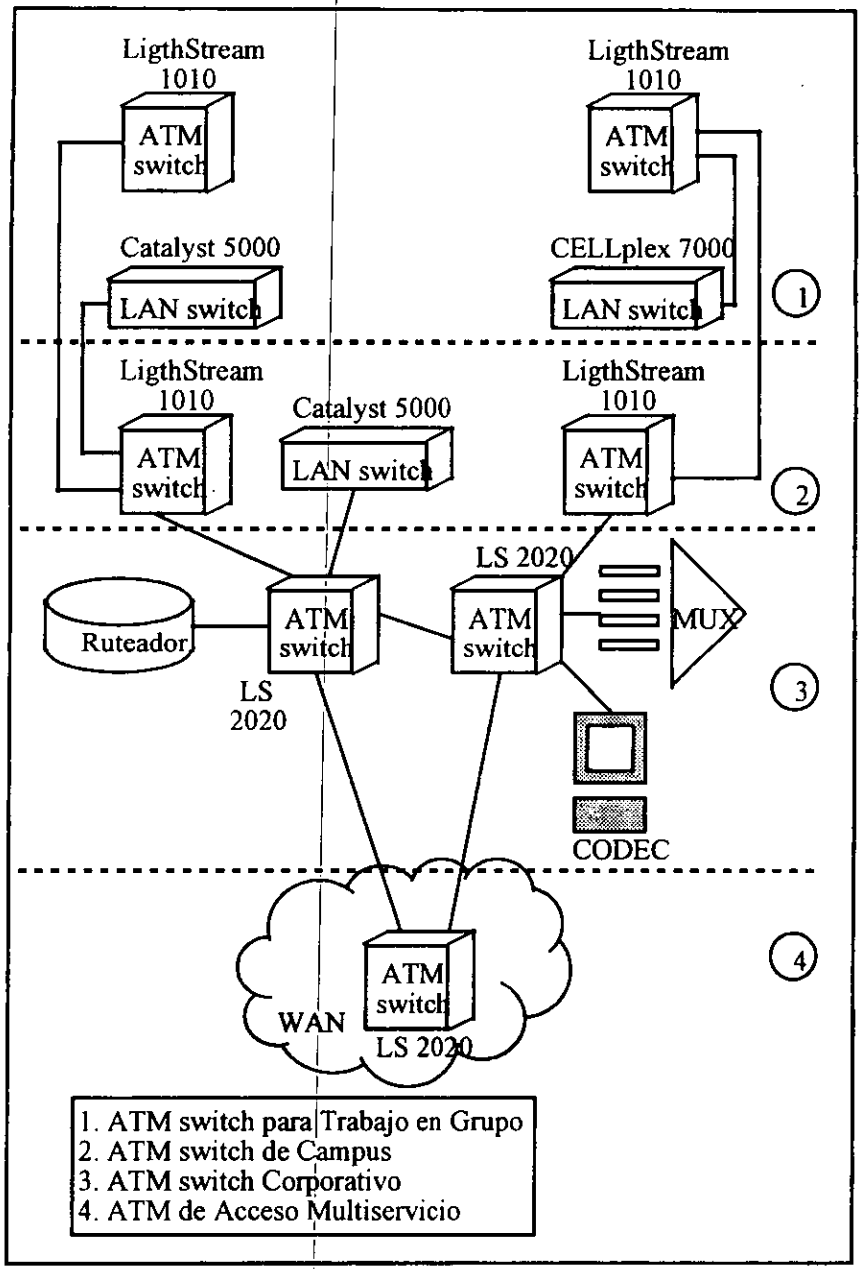


Figura 6.1 Tipos de ATM switches.

Los ATM switches pueden clasificarse de la siguiente manera:

- **ATM switches de trabajo en grupo.** Este tipo de switch esta optimizado para llevar ATM al escritorio sobre interfaces de "bajo costo", con señalización ATM para interoperar con los adaptadores ATM y QOS para multimedia.

- **ATM switches de campus.** Los ATM switches de campus son utilizados para backbone ATM de pequeña escala, por ejemplo: enlazar LAN switches y ruteadores con interfaces ATM, solucionan la congestión en el backbone y abren la posibilidad de manejar VLAN's. Los switches de campus necesitan soportar una amplia variedad de interfaces del backbone local e interfaces de área amplia, pero necesitan ser optimizados en precio/desempeño para su función de backbone local. También es importante sus capacidades de enrutamiento ATM para permitir a múltiples switches ser unidos.

- **ATM switches corporativos.** Los switches corporativos son dispositivos multiservicio sofisticados diseñados para formar backbones de redes corporativas grandes. Los switches corporativos serán usados como switches de campus para interconectar switches de trabajo en grupo y LAN switches. Los switches corporativos sin embargo, pueden actuar no únicamente como backbones, si no servir como un punto de integración de los múltiples servicios y tecnología encontrados en una red corporativa. Mediante la integración de todos esos servicios en una plataforma común y una infraestructura de transporte común, los administradores pueden obtener una mayor manejabilidad, y eliminar la necesidad de múltiples redes. Los ATM switches soportaran capacidades tales como LAN switching, interfaces WAN con Frame Relay, y mecanismos de adaptación multiservicio, incluyendo emulación de circuitos para troncales PBX, y optimizaran troncales WAN para transportar voz, datos y vídeo (ATM sobre DS3).

- **Switches de Acceso Multiservicio.** Más allá de las redes privadas, las plataformas ATM serán ampliamente desarrolladas por los proveedores de servicio dentro de redes públicas. Tal equipo será usado para soportar servicios WAN y MAN, por ejemplo Frame Relay Switching, interconexión de LAN o servicios ATM públicos en una infraestructura ATM común.

Algunos ejemplos de ATM switches son: Passport Magellan 160 de NORTEL y LigthStream 2020 de Cisco, que serían un ATM switches corporativos; el LigthStream 1010 de Cisco, un ATM switch de trabajo en grupo. En la figura 6.1 se ilustra el ambiente en que cada tipo de switch tendría mejor desempeño.

Las características que deben tomarse en cuenta en la elección de ATM switches depende mucho de la aplicación que les queramos dar, pero algunos requisitos fundamentales con que debe contar un switch son:

- Sea compatible totalmente con los estándares del Forum ATM.
- Soporte de señalización UNI 3.1/4.0 e ILMI.
- Soporte de interfaces estándar, como STM-1, STS-3c, OC-12, STM4c.
- Que sean escalables.
- Soporte de IISP y PNNI en su fase 1.
- Soporte de SVC´s o Soft PVC´s.
- Soporte de señalización punto-multipunto.
- Sistema de control de congestión.
- Clases de prioridad múltiples
- Administrable a través de SNMP, consola.
- Puerto para monitorear tráfico.
- Telnet y TFTP para acceso remoto y autoconfiguración.
- Características de valor-agregado (redundancia).

3. Ruteadores

La llegada de las tecnologías LAN switching y ATM switching no elimina la necesidad de los ruteadores. Aun cuando un LAN switch o un ATM switch tomen el lugar de los ruteadores en la red, los ruteadores se requieren para jugar un papel de integración. Switching y LANE operan en la capa 2 de una red. El ruteador es requerido para ejecutar funciones de la capa de red, el ruteador proveerá conectividad entre ELAN´s (LAN emuladas), estableciendo seguridad en el acceso. Aun las redes basadas primariamente en ATM requerirán a los ruteadores, a menos que todas las aplicaciones en la red cambien a ATM nativo puro; lo cual no puede ocurrir hasta que las API´s estén desarrolladas para sistemas operativos y sistemas operativos de red, de tal forma que esas aplicaciones puedan correr directamente sobre ATM.

Muchos de los LAN switches en el mercado, dependen de un dispositivo externo para funciones de ruteo. Por ejemplo una red puede contener varios LAN switches y un backbone ATM, el tráfico interno en una LAN emulada es llevado por los switches, pero el tráfico entre LAN´s emuladas es llevado por el ruteador, el cual puede ser conectado a uno de los switches con un enlace de alta velocidad (un enlace STM-1). Mientras ahora la función de enrutamiento es ejecutada por un ruteador, en el futuro esta función será distribuida. El concepto de enrutamiento distribuido es manejado en MPOA.

Entre los ruteadores disponibles en el mercado con interfaces ATM están: la serie 7500 de Cisco Systems Inc., así como el ruteador 4000 del mismo fabricante. El modulo ATM de la serie 7500 maneja los siguientes parámetros:

- AAL5
- Manejo de trafico UBR (Undefined Bit Rate)
- UNI 3.1 y posibilidad de soportar UNI 4.0.
- Multiprotocolo Encapsulation (RFC 1483)
- LANE 1.O.
- IP y ARP sobre ATM (RFC 1577 y 1755)
- Soporte de ELAN's
- 2048 VC's
- Soporte de flujo F5 y F4 OAM
- Soporte de ILMI
- Administración SNMP

6.3 OPERACIÓN DE UN LAN SWITCH CON ATM

Hablar de la operación de un LAN switch con ATM , es referirse a un LAN switch que tiene una o más interfaces ATM y que además tiene software de LANE para hacer posible la transmisión de información de redes LAN heredadas (Ethernet, Token Ring, etc.) a través de redes ATM ó a redes ATM; y viceversa.

Así pues, siendo el protocolo LANE la parte medular en la interacción entre LAN's heredadas y redes ATM, a continuación se hace un análisis detallado del proceso necesario para que dos LAN switches se comuniquen a través de una red ATM. La misma descripción es válida para el caso de la comunicación entre un LAN switch y un host con una NIC ATM y software LANE.

Como ya se vio en el capitulo anterior, el protocolo LANE está basado en un modelo cliente-servidor. Donde cada cliente (LEC) puede ser un LAN switch , un ruteador con interfaz ATM o un host con NIC ATM, donde los tres dispositivos pueden contener varios LEC's y por lo tanto participar en múltiples ELAN's. Los servidores LES (Servidor de LANE), LECS (Servidor de Configuración de LANE) y BUS (Servidor de Broadcast y Desconocido) pueden estar en cualesquiera de los tres equipos ya mencionados. En general se requiere una pareja LES-BUS por ELAN y un LECS por red ATM.

El LECS puede tener los siguientes registros :
- Nombre de la ELAN, dirección ATM del LES
- Dirección MAC del LEC, nombre de la ELAN
- Dirección ATM del LEC, dirección MAC del LEC
- El nombre por default de la ELAN

6.3.1 Operación LANE.

Aquí hemos llegado al punto principal del presente trabajo de tesis, por lo cual se hará una explicación detallada del protocolo LANE que es sin duda el punto de mayor impacto, cuando se quiere explicar el funcionamiento de LAN switches conectados a una red ATM.

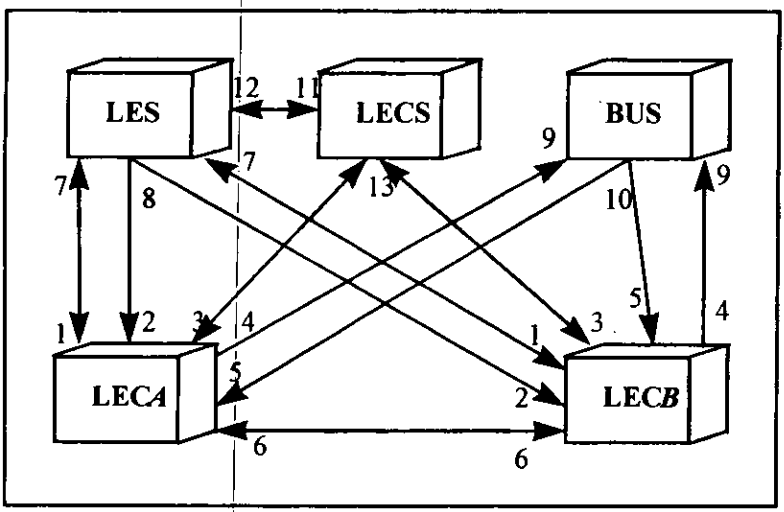


Figura 6.2. Tipos de VCC LANE.

La comunicación entre componentes LANE es ordinariamente manejada por varios SVC's, algunos son unidireccionales y otros bidireccionales, algunos son punto-punto y otros punto-multipunto. En la figura 6.2 se muestran todos los tipos de VCC's involucrados en LANE. Es posible manejar LANE con PVC's en el backbone.

6.3.1.1 Unión de un LEC a una ELAN.

Ahora consideramos el proceso de comunicación LANE, iniciando cuando un LEC es configurado en un LAN switch y pide unirse a una ELAN.

El proceso ocurre normalmente cuando un LEC ha sido habilitado en el modulo ATM de un LAN switch:

1. El LEC hace una petición de unirse a una ELAN. Para ello el LEC establece un VCC Directo de Configuración punto-punto bidireccional (3-13, figura 6.2a) para encontrar la dirección ATM del LES de su ELAN. Los LEC's encuentran al LECS usando las siguientes interfaces y direcciones en el orden listado:
   - Dirección ATM configurada localmente.
   - Vía Interfaz de Administración Local Interina (ILMI).
   - Dirección fija definida por el Forum ATM.

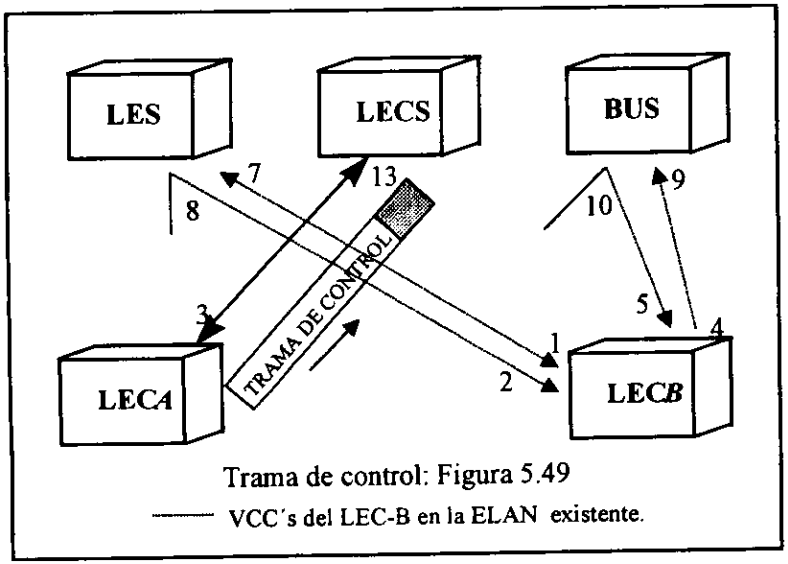


Figura 6.2a Petición del LEC-A para unirse a la ELAN existente.

2. Mediante el uso del mismo VCC (3-11, figura 6.2b), el LECS regresa la dirección ATM y el nombre del LES para la ELAN a la cual pertenece el LEC que hizo la petición de unión.
3. El LEC libera el VCC de Configuración Directa (3-11, figura 6.2c).

4. El LEC contacta el LES para su ELAN, estableciendo una conexión al LES para dicha ELAN (VCC Directo de Control punto-punto bidireccional, enlace 1-7, figura 6.2d) para intercambiar tráfico de control. Desde el momento en que el VCC Directo de Control es establecido entre un LEC y un LES, este permanece establecido.

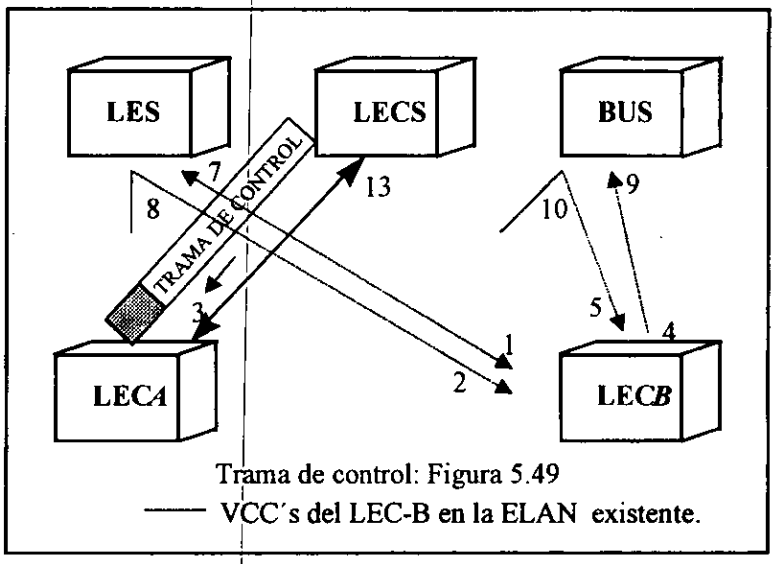


Figura 6.2b El LECS contesta con la dirección ATM (y más datos) de la ELAN solicitada.

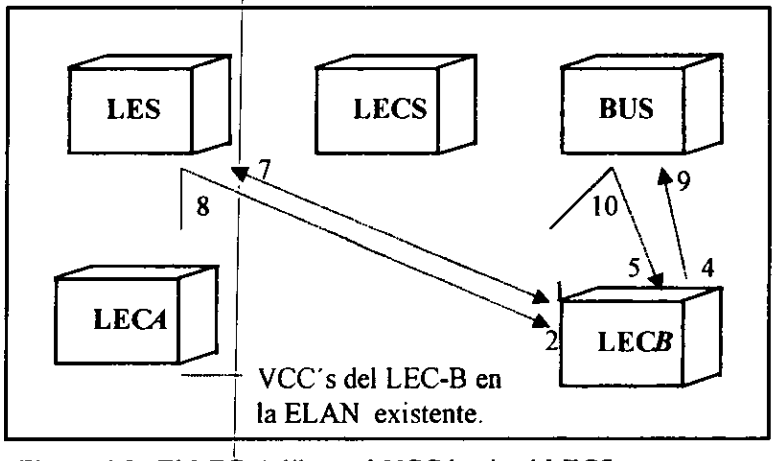


Figura 6.2c El LEC-A libera el VCC hacia el LECS.

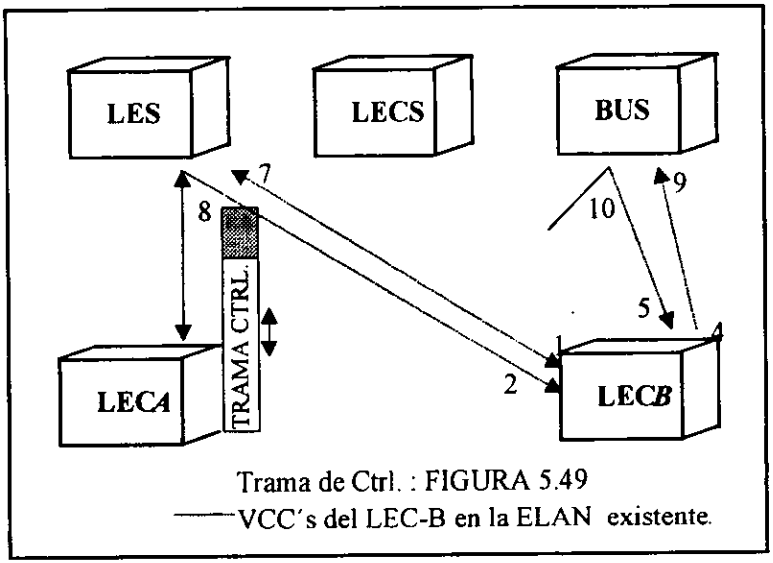


Figura 6.2d El LEC-A contacta el LES para su ELAN.

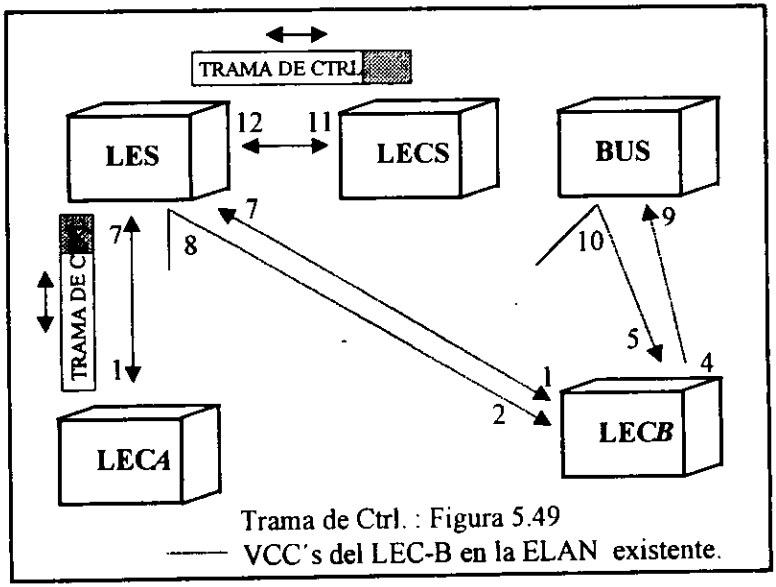


Figura 6.2e EL LES verifica con el LECS, si el LEC-A esta registrado en la ELAN del LES y el LEC-B.

5. El LES verifica que el LEC tenga permiso de unirse a esa ELAN. El LES de esa ELAN, establece una conexión al LECS (VCC de Configuración de Servidor punto-punto bidireccional, enlace 11-12, figura 6.2e) para verificar que el LEC está permitido unirse a la ELAN en cuestión. La petición de configuración del LES contiene la dirección MAC LEC, su dirección ATM y el nombre de la ELAN. El LECS investiga en su base de datos para saber si el LEC está o no permitido unirse a la ELAN; después el LECS usa el mismo VCC para informar ala LES que el LEC está o no permitido unirse.

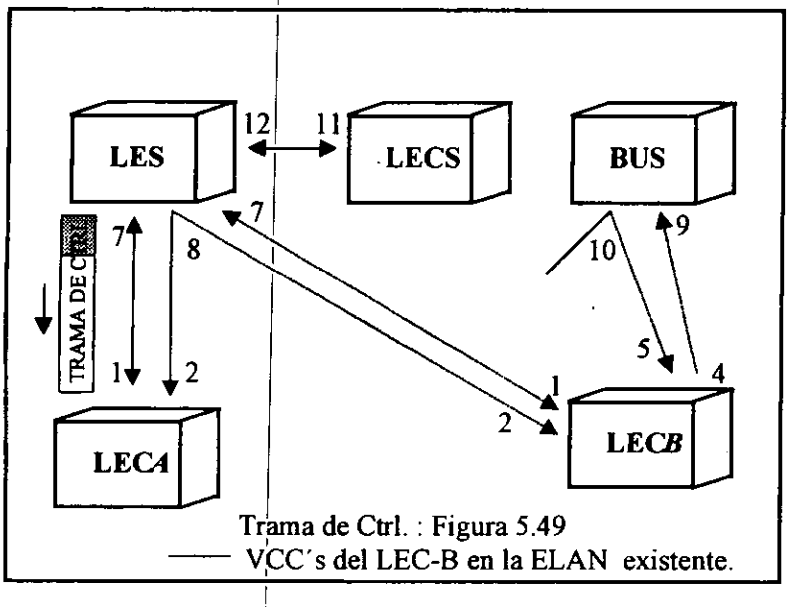


Figura 6.2f El LES adiciona al LEC-A a un VCC multipunto.

6. Dependiendo de la información recibida del LECS, el LES permite o niega la unión del LEC a la ELAN.
7. Si el LEC tiene permiso, el LES adiciona al LEC a un VCC Distribuido de Control punto-multipunto unidireccional (enlace 2-8, figura 6.2f) y confirma la unión sobre el VCC Directo de Control punto-punto bidireccional (1-7, figura 6.2f). Si el LEC no tiene permiso, el LES rechaza la unión sobre el VCC Directo de Control punto-punto bidireccional (enlace 1-7, figura 6.2f).
8. Después de que el LEC ha sido aceptado en la ELAN, el LEC envía paquetes LE ARP con la dirección de broadcast, la cual es todos 1's. Enviando paquetes

LE ARP con la dirección de broadcast, el LES regresa la dirección ATM del BUS. Entonces el LEC establece un VCC de Envío de Multicast (enlace 4-9, figura 6.2g) y el BUS adiciona al LEC al VCC de Transporte de Multicast (enlace 5-10, figura 6.2g) desde el BUS.

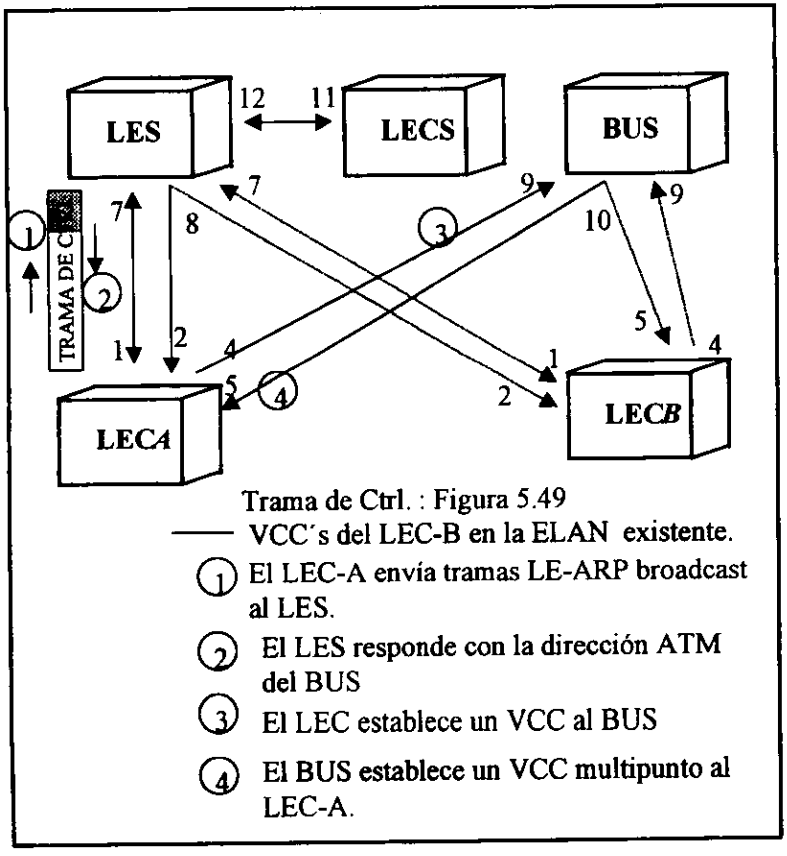


Figura 6.2g El LEC-A contacta al BUS .

6.3.1.2 Resolución de direcciones.

A medida que la comunicación ocurre en la ELAN, cada LEC en un LAN switch (o en otro dispositivo con interfaz ATM y software LANE) construye una tabla LANE ARP (LE ARP) local. Una tabla LE ARP en el LEC puede tener también

registros estáticos preconfigurados. La tabla LE ARP del LEC, mapea direcciones MAC a direcciones ATM

Cuando un LEC por primera vez se une a un ELAN, su tabla LE ARP no tiene registros dinámicos, y el LEC no tiene información a acerca de destinos en su ELAN o fuera de ella. Para saber el destino de un paquete que necesita ser enviado, el LEC inicia el siguiente proceso para encontrar la dirección ATM correspondiente a la dirección MAC conocida:

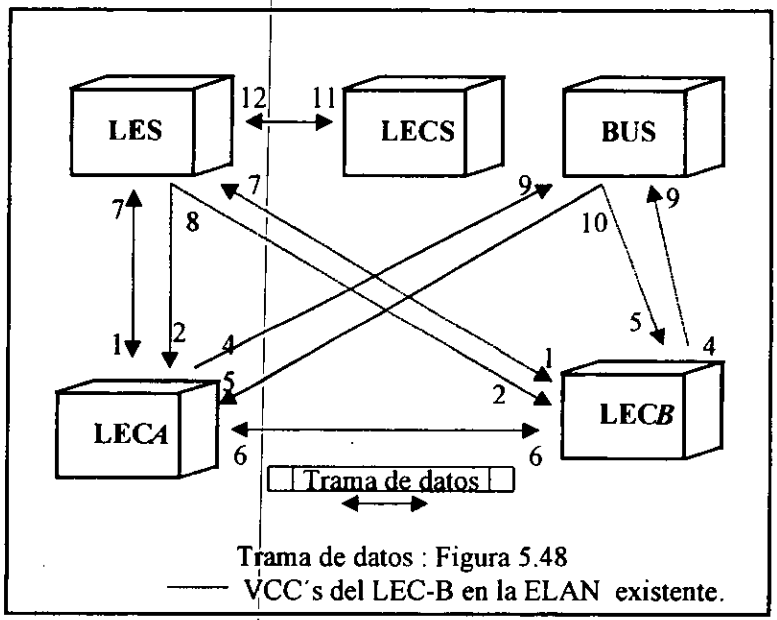


Figura 6.2h El LEC-A transmite datos al LEC-B .

1. El LEC envía una petición LE ARP al LES para su ELAN (por su VCC Directo de Control, 1-7 figura 6.2h).
2. Si la dirección MAC está registrada con el LES, este regresa la correspondiente dirección ATM. Si no, el LES lleva la petición LE ARP a todos los LEC en la ELAN (por el VCC Distribuido de Control punto-multipunto, enlace 2-8, figura 6.2h).
3. Cualquier LEC que reconozca la dirección MAC, responderá con su dirección ATM (a través del VCC Directo de Control punto-punto, enlace 1-7, figura 6.2h).

4. El LEC adiciona la pareja de direcciones MAC-ATM a su memoria cache LE ARP.
5. El LEC puede establecer un VCC al destino deseado y transmitir paquetes a esa dirección ATM (a través del VCC Directo de Datos punto-punto, enlace 6-6, figura 6.2).

6.3.1.3 Envío de tráfico Multicast.

Cuando un LEC tiene tráfico broadcast o multicast para enviar, o tráfico unicast con una dirección desconocida, ocurre el siguiente proceso:

- El LEC envía el paquete al BUS, a través del VCC de Envío de Multicast punto-punto (enlace 4-9, figura 6.2)
- El BUS lleva el paquete a todos los LEC's, a través del VCC de Envío Multicast punto-multipunto unidireccional (enlace 5-10 en la figura 6.2).

Este VCC se bifurca, en cada switch. El switch lleva tales paquetes a múltiples salidas (el switch no examina la dirección MAC, este sólo avanza todos los paquetes que este recibe).

6.3.2 Direccionamiento.

En una LAN, los paquetes son direccionados por las direcciones DESTINO y ORIGEN de la capa MAC. Para proveer una funcionalidad similar por LANE, el direccionamiento de la capa MAC debe ser soportado. Cada LEC debe tener una dirección MAC. Además cada componente de LANE (LECS, LES, BUS y LEC) debe tener una dirección ATM única.

En esta liberación de LANE (LANE 1.0), todos los LEC's en la misma interfaz, tienen automáticamente asignada la misma dirección MAC. Esta dirección MAC es también es usada como la parte que corresponde al identificador de sistema final (ESI) en la dirección ATM. Aunque las direcciones MAC LANE no son únicas, todas las direcciones ATM son únicas.
La dirección ATM LANE, tiene la misma sintaxis que una dirección NSAP, pero esta no es una dirección de nivel de red. En este tipo de dirección, se tiene un prefijo de 13 bytes, un ESI de 6 bytes y un campo selector de 1 byte. Su formato ya fue mostrado en el capítulo anterior.

La forma en que se construyen las direcciones ATM en un dispositivo ATM, depende del equipo en cuestión y del fabricante del equipo. A continuación se describe la forma en que se asignan y construyen direcciones MAC y ATM para usarse en una base de datos LECS, según Cisco Systems Inc. Un conjunto de direcciones MAC son asignadas a cada módulo ATM. El conjunto, tiene 16 direcciones MAC. Para construir direcciones ATM, las siguientes asignaciones son hechas a los componentes LANE:

- Los campos del prefijo son los mismos para todos los componentes LANE en ruteadores y módulos ATM para LAN switches Catalyst 5000; el prefijo indica la identidad del switch. El valor del prefijo debe ser configurado en el switch.
- El valor del campo ESI asignado a cada LEC en la interface es el primero del conjunto de direcciones MAC asignadas a esa interfaz.
- El valor del campo ESI asignado a cada LES en la interface, es el segundo del conjunto de direcciones MAC.
- El valor del campo ESI asignado al BUS en la interface, es el tercero del conjunto de direcciones MAC.
- El valor del campo ESI asignado al LECS es el cuarto del conjunto de direcciones MAC.
- El valor del campo selector, es puesto al número de subinterface del componente LANE, excepto por el LECS, el cual tiene un valor de campo selector de 0.

Dado que los componentes LANE son definidos en diferentes subinterface de una interfaz ATM, el valor del campo selector en una dirección ATM es diferente para cada componente. El resultado es una dirección ATM única para cada componente LANE, aún dentro del mimo switch (por ejemplo: Catalyst 5000).

Hay algunas reglas para asignar componentes LANE a interfaces y subinterfaces, estas son:

- El LECS es siempre asignado a la mayor interface. Si cualquier otro componente se asigna a la interfaz mayor, es idéntico a asignar ese componente a la subinterface 0.
- El LES y el LEC de la misma ELAN pueden ser configurados en la misma subinterface.
- LEC´s de diferentes ELAN´s no pueden ser configurados en la misma subinterface.
- Servidores de diferentes ELAN´s no pueden ser configurados en la misma subinterface.

Una forma de construir direcciones ATM es vía ILMI. Por ejemplo el LAN switch Catalyst 5000 de Cisco Systems Inc., usa ILMI para construir su dirección ATM y registrar esta dirección con el ATM switch. Para construir su dirección ATM, el Catalyst 5000 obtiene su prefijo de dirección ATM del ATM switch. Después este combina tal prefijo de dirección ATM con su propia dirección MAC y número de subinterfazce LEC. Una vez que el módulo ATM del Catalyst ha determinado su dirección ATM, este usa el registro ILMI para registrar su dirección ATM con el ATM switch.

6.3.4 Asociación VLAN-ELAN

Una vez que se han asignado direcciones ATM a cada uno de los componentes LANE (LECS, LES/BUS por ELAN, LEC's en un ELAN dada), en cada LAN switch es necesario hacer una asociación VLAN-ELAN. Siguiendo con el ejemplo del Catalyst, en este LAN switch una VLAN es un grupo lógico de estaciones finales, independientes de su localización física, con un conjunto común de requerimientos. Actualmente, se hace asignación de VLAN's por puerto (en el Catalyst), lo que significa que todas las estaciones finales conectadas al mismo puerto del LAN switch, corresponden a ala misma VLAN. El número asignado a ala VLAN, solo tiene significancia local.

En una red ATM, una LAN emulada es llamada una ELAN y es designada por un nombre. Para crear un VLAN que abarque varios LAN switches en una red ATM, se deben asignar todas las VLAN (puertos de distintos LAN switch) a la misma ELAN, es decir en cada LAN switch se debe asociar un puerto LAN a un LEC, participante en una ELAN en la red ATM.

Se debe usar un ruteador para permitir la comunicación entre dos o más ELAN's, ya sea que ellas estén o no en el mismo LAN switch.

6.3.5 Ejemplo de una Red LANE.

El siguiente ejemplo fue tomado de una página en Internet perteneciente a Cisco Systems Inc.; la dirección electrónica es : http://www. ij.com.

El ejemplo mostrado en al figura 6.3, muestra dos ruteadores Cisco y dos LAN switches conectados a un ATM switch LigthStream 1010. La red tiene tres ELAN's para ingeniería, manufactura y ventas. En este ejemplo no se restringe la membresía en las ELAN's.

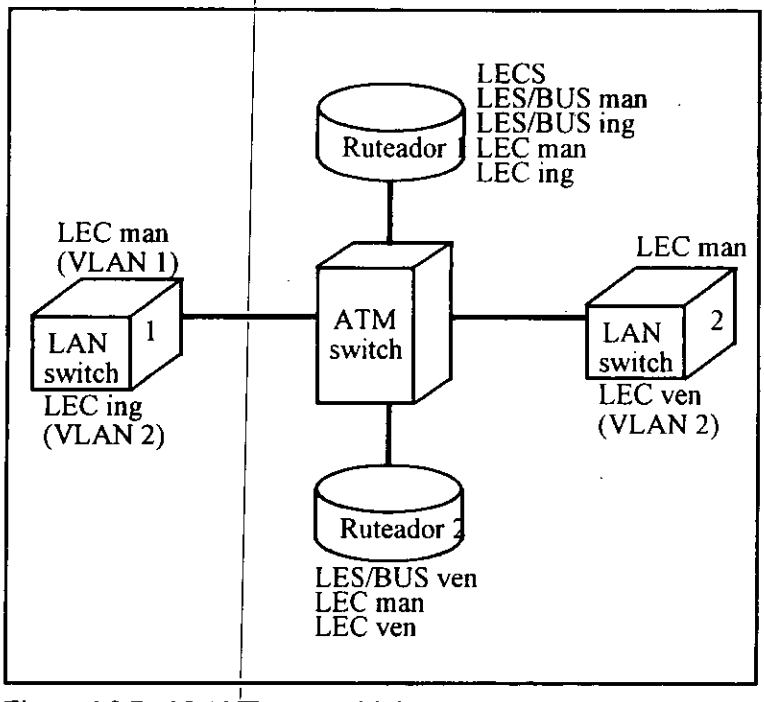


Figura 6.3 Red LANE con Múltiples LAN emuladas.

En este ejemplo, el ruteador 1 tiene los siguientes componentes:

- LECS (sólo hay un LECS para este grupo de ELAN's)
- LES/BUS para la ELAN de manufactura (man).
- LEC para la ELAN-man.
- LEC para la ELAN de ingeniería (ing).

El ruteador 2 tiene los siguientes elementos:

- LES/BUS para la ELAN de ventas (ven).
- LEC para la ELAN de manufactura.
- LEC para ELAN-ven.

El LAN switch Catalyst 5000-1 tiene los siguientes componentes:

- LES/BUS para ELAN-ing.
- LEC para ELAN-man.
- LEC para ELAN-ing en VLAN 2 (ing).

Equipo	Prefijo de dirección ATM	ESI Base
Ruteador 1	39.000001415555121100000000	0800-200c.1000
LAN switch 1	39.000001415555121100000000	0800-200c.2000
LAN switch 2	39.000001415555121100000000	0800-200c.3000
Ruteador 2	39.000001415555121100000000	0800-200c.4000

Tabla 6.1. Prefijo de dirección ATM y ESI base.

El LAN switch Catalyst 5000-2 tiene los siguientes componentes:

- LEC para la ELAN-man en VLAN 1 (man).
- LEC para la ELAN-ven en VLAN 3 (ven).

Para propósito del ejemplo, se asigna el siguiente prefijo de dirección ATM y base ESI:

Ruteador 1

El ruteador 1 tiene el LECS y su base de datos, LES/BUS para la ELAN de manufactura, un LEC para manufactura, y un LEC para ingeniería. Su configuración es de la siguiente forma:

```
! Las siguientes líneas dan nombre y configuran la base de datos del LECS.
lane database example2
name ing server-atm-address 39.000001415555121100000000. 0800-
200c.4000.02
name man server-atm-address 39.000001415555121100000000. 0800-
200c.4000.01
name ven server-atm-address 39.000001415555121100000000. 0800-
200c.4000.01
```

default-name man
!
! Las siguientes líneas establecen PVC's para señalización y para comunicación con la
! ILMI, además asocia la base de datos del servidor de configuración con un nombre.
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane auto-config-atm-address
lane congfig example2
!
! Las siguieb¡ntes líneas configuran el LES, BUS y LEC para la ELAN de manufactura
! en la subinterface atm1/0.1. El cliente es asignado a la ELAN por default.
interface atm 1/0.1
ip address 172.16.0.1 255.255.255.0
lane server-bus ethernet man
lane cliente ethernet
!
! Las siguientes líneas configuran el LEC "ing" en la interface 1/0.2. El cliente es
! asignado a la LAN emulada de "ing". Cada LAN emulada tiene un dirección IP en una
! subred diferente a la del cliente"man".
interface atm 1/0.2
ip address 172.16.1.1 255.255.255.0
lane client ethernet ing

Ruteador 2

El ruteador 2 tiene el LES/BUS para la ELAN-ven, un LEC para ventas, un LEC para manufactura. Debido a que el nombre por default para una ELAN es "man", el segundo LEC es enlazado al nombre de ELAN por default. La configuración del ruteador 2 es como sigue:

interface atm 3/0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
interface atm 3/0.1

lane server-bus ethernet ven
lane client ethernet ven
interface atm 3/0.2
lane cliente ethernet

LAN Switch 1

El LAN switch Catalyst 5000 1 es configurado para LES/BUS para la ELAN "ing", un LEC de la ELAN "man", y un LEC de la ELAN "ing". Debido a que el nombre ELAN por default es "man", el primer LEC es enlazado al nombre ELAN por default.

interface atm 0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
interface atm 0.1
lane client ethernet 1
interface atm 0.2
lane server-bus ethernet ing
lane cliente ethernet 2 ing

LAN Switch 2

El LAN switch Catalyst 2 es configurado para un LEC de la ELAN "man" y un LEC de la ELAN "ven". Dado que la ELAN por default es "man", el primer LEC es enlazado al nombre ELAN por default.

interface atm 0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
interface atm 0.1
lane client ethernet 1
interface atm 0.2
lane client ethernet 3 ven

La finalidad de poner un ejemplo en el presente trabajo de tesis, es hacer notar parte de la gran cantidad de conceptos que deben manejarse para poder construir una red LANE. También se intenta hacer ver que la función de los **LAN switches** con conexión a ATM, es precisamente ser la interface entre las redes LAN heredadas y la red ATM, y que **LANE** es indispensable para la conexión de

LAN's heredadas a un red ATM. Un punto importante que puede apreciarse es que los **LAN switches no sustituyen a los Ruteadores.**

6.4 PROPUESTA DE UN RED CON ATM SWITCHES Y LAN SWITCHES, PARA C.U.

En los capítulos anteriores, hemos desarrollado los temas necesarios para entender el por que surgen los LAN switches, por que la necesidad de ATM; y como interactuan los LAN switches con la tecnología ATM, haciendo énfasis en esto último dado que es precisamente el tema de tesis que presentamos.

En las secciones anteriores a esta, se ha detallado el funcionamiento de un LAN switch cuando se conecta a una red ATM. Es preciso dejar, claro que sólo se profundizó en los temas que son necesarios para entender este funcionamiento.

En esta sección, se presenta una propuesta para el backbone de la red de datos de Ciudad Universitaria de la Universidad Nacional Autónoma de México. Cabe mencionar que la UNAM ya cuenta con un backbone ATM formado por ATM switches NORTEL; y LAN switches 2500 y 7000 3COM, así como de ruteadores Cisco 7500.

La finalidad de proponer un backbone diferente es hacer notar que con los conceptos tratados en el transcurso de este trabajo de tesis, es posible hacer una propuesta coherente para mejorar una red de datos dada, utilizando las tecnologías de **LAN switching** y **ATM switching**, sin pasar por alto que la red de datos seguramente está trabajando en forma paralela con redes de voz y vídeo.

6.4.1 Problemática de la Red

La red anterior tenía las siguientes características:

- Redes de datos voz y vídeo, separadas.
- Lo anterior implicaba gastos de operación, monitoreo y administración, multiplicados por 3.

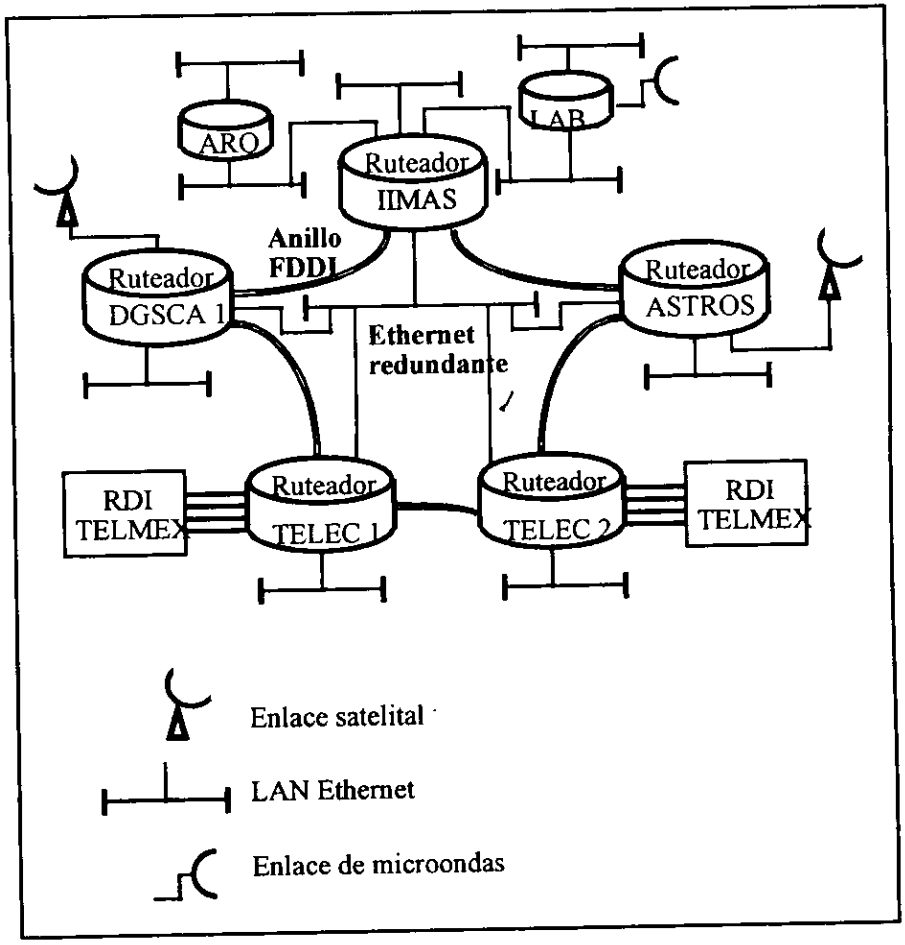


Figura 6.4. Red de datosde la UNAM en CU.

- Gran desperdicio de ancho de banda por la red de videoconferencia dado que son sólo a determinadas horas del dia se utiliza, además de utilizar multiplexores TDM (Multiplexaje por División en el Tiempo). La velocidad estándar en toda la red de videoconferencia de la UNAM es de 384 Kbps. (CBR).
- Desperdicio de ancho de banda por los enlaces telefónicos, debido a que dichos enlaces utilizan multiplexores TDM.

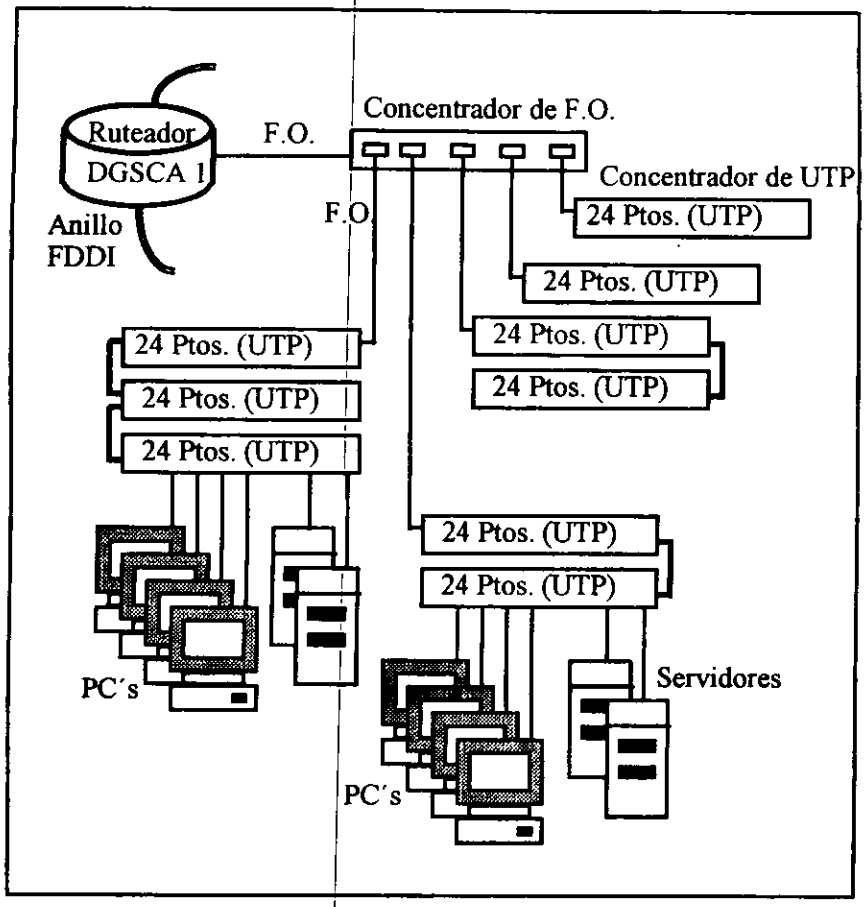


Figura 6.5. LAN´s Ethernet heredadas.

Hablando específicamente de la red de datos, tenía las siguientes características:

- Un backbone FDDI, que funciona muy bien.
- Redes LAN Ethernet, con muchos problemas de lentitud de transmisión dado el número de PC´s, Servidores y Estaciones de Trabajo conectadas por segmento, y las aplicaciones corridas sobre la red, las cuales incluyen consultas de bases de datos, transferencias de archivos, manejo de imágenes, aplicaciones cliente-servidor, etc.
- Un número de usuarios en constante aumento, por ello la necesidad de una red escalable.

- Los protocolos que corren sobre la red son: TCP/IP, IPX, APPLE TALK, NetBEUI.
- Hay gran cantidad de enlaces seriales que llegan a tres puntos de la red en C.U., algunos de esos enlaces representan la salida a Internet para la UNAM, los enlaces restantes son de instituciones externas que tienen necesidad de comunicarse con C.U. u ocupan la infraestructura de la UNAM para conectarse a Internet. La topología del backbone es la que se muestra en al figura 6.4.
- A nivel local de tiene una topología en estrella, y Ethernet no conmutado. La figura 6.5 siguiente muestra la configuración más común en tales redes locales.

6.4.2 Propuesta a Nivel Local y a Nivel de Backbone

Nivel local

A nivel local, la solución propuesta es con tecnología LAN "switching", es decir se propone utilizar LAN switches en lugar de concentradores para trabajo en grupo, la topología es la que se muestra en la figura 6.6.

Características de la red local propuesta:

- Se optó en ocupar LAN switches de la familia Catalyst de Cisco Systems Inc.: 5000, 3000, 1700 y 2000, dependiendo de la funcionalidad requerida. Sin embargo, cuando sea necesaria la conexión de un LAN switch a ATM, se utilizarán los LAN switches Catalyst 5000, dado su alto desempeño, sus interfaces .
- El "corazón" de las redes a nivel local, sería el Catalyst 5000, cuando se tratara de redes locales grandes que tuvieran conexión directa al backbone ATM.
- Con el LAN switch 5000, se tiene la posibilidad de una ELAN-VLAN por puerto LAN.
- Se acaba con el problema de ancho de banda a nivel local, y a medida que se requiera se puede ir llevando Ethernet "conmutado" al escritorio. El Catalyst tiene la capacidad para ello.
- Se asignan servidores que demandan gran ancho de banda, a un puerto 100BaseT ó 10BaseT.

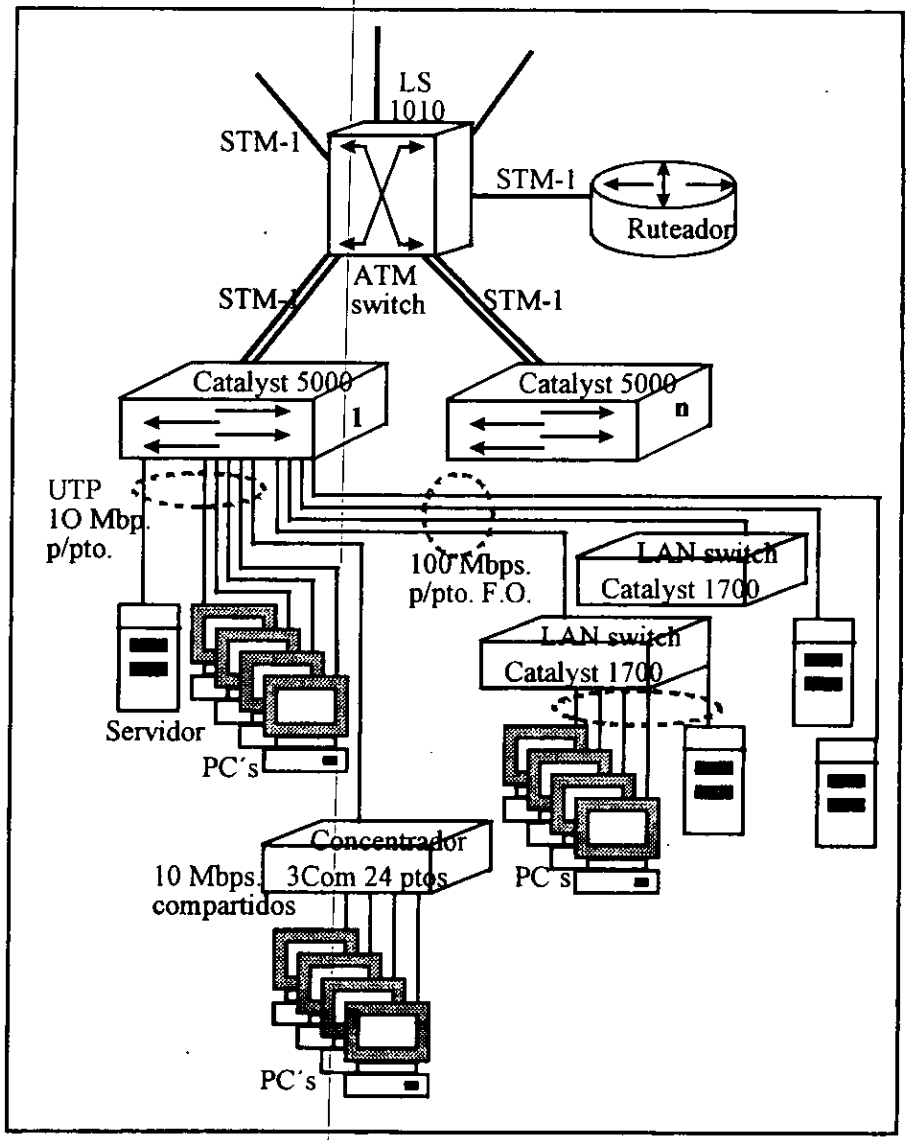


Figura 6.6. Solución propuesta a nivel local con LAN switching.

- La idea de utilizar LAN switches con interfaces ATM, es que tales LAN switches se conecten a un backbone ATM que agrupe todos los servicios para finalmente consolidar la red.

- Con el uso de LAN switches a nivel local, se utiliza la misma infraestructura de cableado e incluso gran parte del equipo activo (concentradores, tranceivers, etc.) lo que ayuda a preservar la inversión existente. En lo que a tarjetas de red se refiere, se utilizan las mismas, excepto en el caso de servidores que se quieran conectar a Fast Ethernet.

Con el uso de LAN switches Catalyst 5000, se cuenta con el Protocolo de Redundacia de Servidor Simple (SSRP). El cual permite poner LECS's, LES's/BUS's de respaldo, lo que permite eliminar un punto de falla en el protocolo LANE: los servidores.

- El switch Catalyst 5000 también cuenta con una tarjeta LANE fisica dual.

Propuesta del Backbone

El backbone propuesto es una doble delta de switches ATM, la topología fisica se muestra en la figura 6.7.

La topología anterior tiene las siguientes características:

- Se compone de una delta doble. La delta externa está compuesta por ATM switches LigthStream 1010, los cuales manejan una alta densidad de puertos ATM necesaria para la conexión de varios LAN switches Catalyst, y del ruteador 7500. Los ATM switches LigthStream 1010 tienen la capacidad de manejar SVC's, los cuales facilitan la programación y puesta en operación de una red LANE. El LigthStream soporta ILMI, lo cual facilita la autoconfiguración de sistemas finales a través de registro de direcciones. También manejan el protocolo de Interfaz Red-Red Privada, que es un protocolo de enrutamiento dinámico ATM, que provee rutas con determinada calidad de servicio (QOS). Además manejan el protocolo de enrutamiento ATM estático IISP (Protocolo Interswitch Interino).
- La delta interna se compone de tres ATM switches LigthStream 2020. Este tipo de ATM switches, se escogió para poder soportar tráfico CBR (voz y video de velocidad constante, manejado en la UNAM). Cuenta con las interfaces ATM necesarias para conectar el ATM switch 1010 y los demás ATM switches 2020. El LigthStream 2020 puede tener interfaces ATM WAN (DS3, T3), lo que significa que nuestra red estará preparada para conectarse a un red ATM pública, cuando esta exista. El switch 2020 soporta "soft PVC's" lo que habilita el reenrutamiento automático de tráfico a través de rutas alternas provistas por los switches 1010.

- La finalidad de la doble delta es de tener un backbone redundante: con la topología propuesta, difícilmente quedará sin operar la parte de datos.
- Una característica muy importante es la inclusión de tres ruteadores para que realicen la comunicación entre ELAN's y además provean la comunicación hacia el lado WAN. Las salidas E1 hacia Internet en U.S.A. están distribuidas en los tres ruteadores, con el objetivo de evitar que toda la red se quede sin salida a Internet en caso de que un sólo ruteador fallara y este tuviera todas los enlaces a Internet. Otra razón, por la que se usan tres ruteadores, y no uno sólo, es que el ruteador no sea un "cuello de botella".
- La escalabilidad, en lo que a ancho de banda se refiere, no tiene problema. Se están considerando que todos los enlaces ATM son STM-1 (155 Mbps.), en el momento en que esa velocidad se ocupe en un alto porcentaje, se pueden montar tarjetas de 622 Mbps.

Cabe mencionar, que un factor de suma importancia en el diseño de una red LANE (y de cualquier red), es el dinero disponible para llevarla a cabo. Además, seguramente tanto la red sea más capaz de soportar fallas (redundante) y seguir operando normalmente, más cara será. También, en tanto más ancho de banda se requiera a nivel local y a nivel de backbone, se incrementarán los costos. Por lo tanto, es necesario hacer un balance entre costo de la red y la disponibilidad de la misma, en el momento de hacer una propuesta.

La confiabilidad y disponibilidad de la red, estarán en función del valor crítico de las aplicaciones que se corren sobre ella.

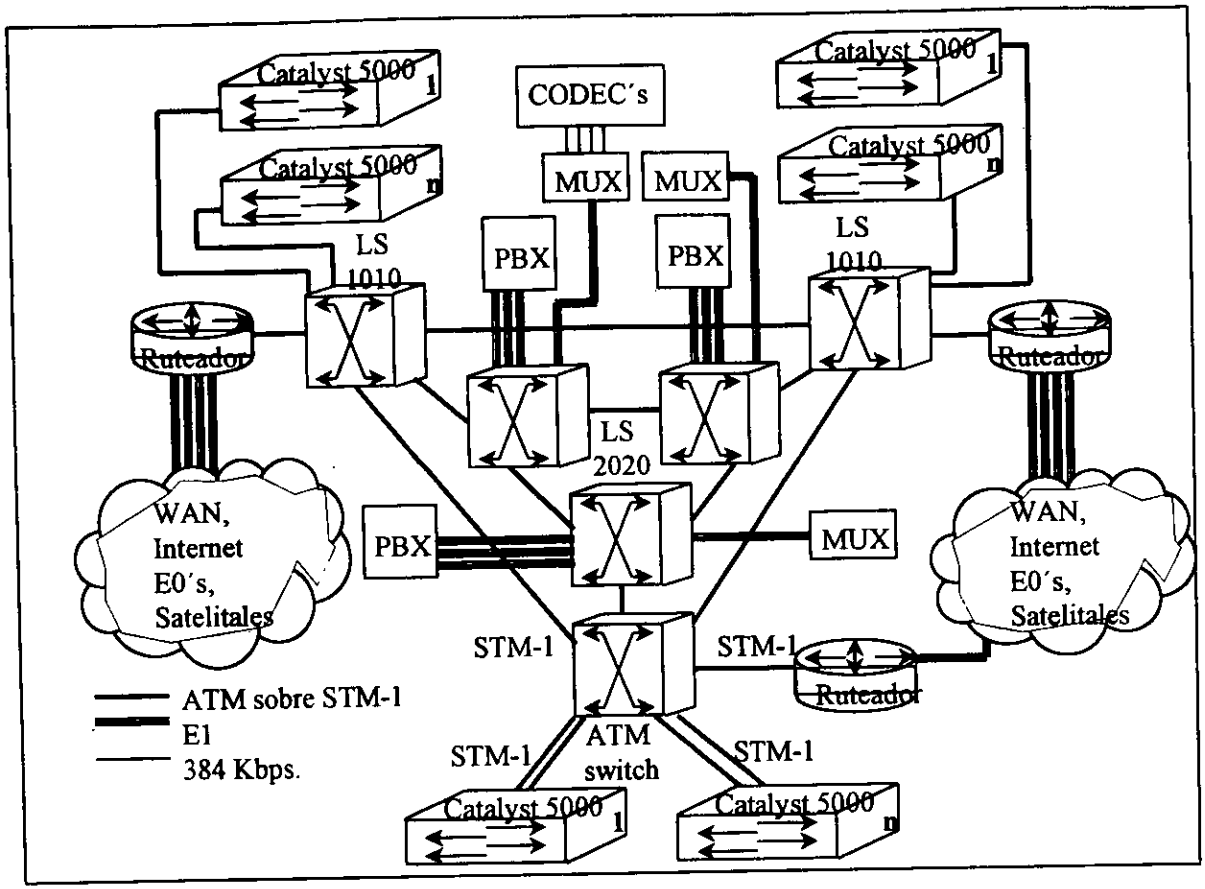


Figura 6.7. Propuesta para el Backbone de la RedUNAM en CU.

6.5 CONCLUSIONES GENERALES

Durante el desarrollo del presente trabajo de tesis hemos procurado mencionar todos los temas necesarios para entender el funcionamiento de los LAN switches, cuando estos equipos de conmutación LAN se conectan a una red de ATM.

Se han estudiado los tipos de redes LAN más comunes tales como Ethernet, Token Ring y FDDI; el funcionamiento de las mismas, sus topologías físicas (estrella, anillo, bus) y los medios físicos (UTP-Unshielded Twisted Pair, fibra óptica, microondas, enlaces satelitales, etc.). También se analizó el conjunto de protocolos TCP/IP que como ya se había mencionado, es la arquitectura de red más utilizada hoy en día; sin embargo existen más arquitecturas (Novell Netware, Apple Talk, NetBEUI) que aunque no son tan ampliamente usadas como TCP/IP, deben ser soportadas por los dispositivos que enrutan o conmutan datagramas en una red de datos dada.

Los temas anteriormente mencionados fueron tratados en los primeros tres capítulos; y representan la información sobre las redes LAN "heredadas"; los protocolos que sobre ellas corren.; los problemas de ancho de banda que tienen este tipo de redes, frente al fuerte incremento en el numero de dispositivos en red (PC'S, Estaciones de Trabajo, Terminales) y al uso de aplicaciones que demandan ancho de banda de la red.

El capítulo 4 fue dedicado a los LAN switches: su operación independiente de ATM, los tipos que existen, sus ventajas, las topologías físicas que se pueden formar con estos, etc. En el capítulo 5 se habló sobre lo más sobresaliente de la tecnología ATM, por ejemplo: portadoras que pueden llevar celdas ATM , tipos de interfaces ATM, tráfico que maneja ATM; y soluciones (LANE, MPOA e IP sobre ATM) para poder llevar tráfico de datos generados por las aplicaciones de las arquitecturas de red existentes, sobre una red ATM.

Finalmente en este capítulo se hace un análisis detallado de la comunicación necesaria para que una LAN switch pueda comunicarze con otro LAN switch (ó con un Host ATM) a través de una red ATM; dado que ambos LAN switches tengan cargado el software de LANE.

Dada la gran cantidad de redes LAN "heredadas" instaladas en el mundo, y dados los problemas de ancho de banda que sufren dichas redes; es necesario encontrar alguna solución que elimine estos problemas de ancho de banda, que

esa solución preserve la inversión existente en infraestructura de red, y que además dicha solución sea adecuada a corto y mediano plazo (por lo menos). No sólo se tiene problemas de ancho de banda, también se tiene problemas para evitar que la red determine la ubicación física de un grupo de trabajo. En redes "heredadas", el espació que ocupa un grupo de trabajo esta dado por la ubicación de los equipos de red, lo cual no siempre es lo más conveniente. Esto último puede solucionarse con el manejo de VLAN's.

También debe tomarse en cuenta, que existe numerosas redes corporativas que tienen backbones de datos, independientes de su red telefónica y de su red de video. Esto no es en realidad un problema, pero si representa desventajas; entre ellas tenemos: gastos en la operación y mantenimiento de las tres redes por separado; desperdicio de ancho de banda, que cuesta y que puede aprobecharse si se emplea la tecnología adecuada. Además es importante contar con un backbone que sea escalable, con la finalidad de que soporte los requerimientos de ancho de banda que demandan nuevos usuarios y aplicaciones, y que no degrade la calidad de servicio prestada a los usuarios ya existentes.

Los problemas mencionados en los dos párrafos anteriores, se encuentran en muchas redes existentes, el trabajo para los administradores de dichas redes es: solucionar dichos problemas. El administrador de la red debe escoger una tecnología que termine con los problemas existentes en su red, una tecnología que le ahorre dinero, y que además esta tecnología sea una solución a mediano plazo al menos.

La solución que proponemos para aliviar los problemas antes mencionados de las redes corporativas, y que cumpla con las perspectivas del administrador de red ya también citadas, no es una tecnología; es la combinación de dos tecnologías: ***LAN "switching"*** a nivel local y ***ATM*** en el backbone, junto con **LANE** instalado en los **LAN switches** y en los ruteadores.

La utilización de LAN switches en redes LAN representa grandes ventajas, entre ellas tenemos las siguientes:

- Más ancho de banda a nivel local. A diferencia de los concentradores de medio compartido, los cuales tienen un ancho de banda dado (10 Mbps. en el caso de Ethernet) que se distribuye entre todos los dispositivos conectados en todos sus puertos; los LAN switches asignan un ancho de banda dedicado a cada uno de sus puertos, lo cual da como resultado más ancho de banda por

puerto y por tanto más ancho de banda por PC (Workstation, terminal, etc.) en la red local.

- En un concentrador (Ethernet) de medio compartido todos los dispositivos conectados a este participan en el único (pero grande) dominio de colisiones del segmento LAN, lo que origina gran cantidad de colisiones. Dado que los LAN switches trabajan en la capa 2 del modelo OSI y no solo a nivel físico, se reduce el dominio total de colisiones del concentrador de medio compartido, a dominios de colisiones más pequeños (un dominio por puerto), lo cual reduciría la probabilidad de colisiones, evitando el desperdicio de ancho de banda por ese motivo.
- Los beneficios de mejora de ancho de banda y reducción del dominio de colisiones, se hace sin cambiar de tecnología LAN. Esto tiene la ventaja de no requerir nuevo cableado y nuevas tarjetas de red. Si se tratara de mejorar el ancho de banda a nivel local, instalando una nueva tecnología (Fast Ethernet, por ejemplo) se tendría necesidad de cambiar tarjetas de red de todas la PC´s y Workstations, y comprar concentradores de medio compartido Fast Ethernet, si esta fuera la tecnología escogida.
- Es posible llevar la tecnología LAN "switching" hasta el escritorio, lo cual es conveniente para el caso de servidores y Workstations generen mucho tráfico hacia la red y reciban mucho tráfico de la misma.

Nosotros pensamos que la tecnología ATM, es una tecnología que va a prevalecer por mucho tiempo dadas sus características únicas, tales como:

- El manejo de voz, vídeo y datos en una misma infraestructura.
- Manejo eficiente de ancho de banda.
- Tecnología aplicable al ambiente WAN, LAN, público y privado.
- Se trata también de una tecnología escalable en lo que ancho de banda se refiere.

Por estas razones, y a pesar de las desventajas actuales de ATM, como: alto costo para llevarse al escritorio, estándares importantes aún no definidos, complejidad de software, etc.; esta tecnología es muy conveniente para usarse en backbones y también para conectar Workstations de muy alto desempeño.

Como ya se vio en el transcurso de este trabajo de tesis, ATM y las redes LAN difieren marcadamente. Para lograr la interoperabilidad de ATM y una red LAN "heredada", aprobechando las ventajas de los LAN switches y de ATM a la

vez; es necesario utilizar un mecanismo que haga posible esa interoperabilidad, el "mecanismo" es LANE.

LANE es la única posibilidad, por el momento, de hacer convivir redes LAN (con varias arquitecturas de red corriendo sobre ellas) con dispositivos ATM, sin tener que modificar tales arquitecturas. Los LAN switches con interfaces ATM tienen cargado el software y hardware asociado a LANE.

Para el caso de que se tenga un ambiente LAN con varias arquitecuras de red, se esta desarrollando MPOA, pero precisamente ese es el problema: aún esta en desarrollo.

Al terminar nuestro trabajo de tesis, nos dimos cuenta que en el área de comunicaciones se están desarrollando tecnologías y equipos, con mucha rapidez y la única forma de estar actualizado es tener la costumbre de informarse diariamente, lo cual es difícil dado que hay muy poco tiempo para dedicar a la lectura, debido al ritmo de vida que llevamos. Sin embargo siempre puede uno encontrar momentos para leer, y la prueba es que pudimos concluir nuestra tesis (a pesar de que nos costo mucho trabajo). Una herramienta muy poderosa con que contamos que nos puede ayudar para estar informados, es la Internet; aunque toda la información escrita siempre tiene un valor agregado.

Uno de los objetivos que perseguimos al hacer una investigación de esta naturaleza, es generar un material de apoyo para los administradores de red que tengan la necesidad de solucionar problemas de ancho de banda a nivel local, y quiera consolidar su red a nivel de backbone Esta investigación cubre los puntos mas importantes, para que el administrador de red tenga bases sólidas (en la investigación en si, en la bibliografía y en las direcciones Internet) para decidir si: ***LAN "switching", ATM y LANE*** son la mejor solución a los problemas de su red.

La importancia del presente trabajo de tesis radica en lo siguiente: si un administrador de red quiere mejorar el nivel de desempeño de su red (a nivel local y a nivel de backbone) tiene que informarse sobre las tecnologías que hay disponibles y que le ofrecen esas tecnologías; para informarse tiene que leer una inmensa cantidad de material bibliográfico, manuales e información en la Internet; y todo sólo para informarse (aunque finalmente no adopte la tecnología). Este trabajo de tesis es un condensado de la información necesaria para decidir si **LAN "switching" y ATM** , son o no, la solución más adecuada a los problemas de red

dada. Si LAN "switching" y ATM no son la solución a la problemática de la red del administrador, el administrador no deperdició demasiado tiempo en conocer una tecnología que no adoptara.

GLOSARIO

AAL ATM Adaptation Layer
ABM Asynchronous Balance Mode
ABR Available Bit Rate
ADCCP Control Avanzado de Procedimineto de Comunicación de Datos
AFI Authority and Format Identifier
ANSI American National Standar Institute
API Aplication Programated Interface
ARM Asynchonous Response Mode
ARP Address Resolution Protocol
ARPA Advanced Research Projects Agency
AS Autonomous System
ASCII Amaerican Standard Code for Information Interchange
ASIC Application Specific Integrated Circuit
ASK Amplitude Shift Keying
ATM Asynchronous Transfer Mode
AU Administraive Unit
AUI Attachment Unit Interface
BBN Bolt Baranek and Newman
BCD Binary Coded Decimal
BGP Border Gateway Protocol
BICI Broadband Inter-carrier Interface
BIP-8 Bip Interleaved Parity-8
BIP-X Bip Interleaved Parity
B-ISDN Broadband ISDN
BRI Basic Rate Interface
BUS Broadcast and Unknown Server
CAC Control de Admisión de Conexión
CAD Computer Assisted Design
CAM Computer Assisted Manufacture
CBR Constant Bit Rate
CCITT International Telegraph and Telephone Commitee

CDDI Coper Distributed Data Interface
CDV Variación de Retardo de la Celda
CER Cell Error Rate
CLP Cell Loss Priority
CLR Cell Lost Rate
CPCS Subcapa de Convergencia de Parte Común
CPE Client Premises Equipment
CPI Common Part Indicator
CRC Cyclic Redundancy Check
CS Sublayer Convergence
CSMA/CA CSMA/CA Collision Anulation
CSMA/CD Carrier Sense Multiple Access/ Collision Detect
CSMA/CE CSMA/ Collisión Elimination
CTD Cell Transfer Delay
CU Ciudad Universitaria
DA Destination Address
DAC Dual Attachment Concetrator
DARPA Defense Advanced Projet Research Agency
DAS Dual AttachmentStation
DCC Data Country Code
DDN Data of Defense Network
DFI Identificador de Formato de Parte específica de Dominio
DOD Department of Defense
DQDB Distributed Queue Data Bus
DRI Defense Research Internet
DS3 Data Stream 3
DTE Data Terminal Equipment
DTL Listas de Tránsito Diseñadas
E1Trama básica europea para transmisión de voz.
ED Edge Device Dispositivo de Frontera
ED End Delimiter
EGP External Gateway Protocol
EIA Electronics Industries Association
ELAN Emulated LAN
ESF Extended Super Frame
FAS Frame Align Signal

FC Frame Control
FCS Field Check Sequence
FDA Foods and Drugs Administration
FDDI Fiber Distributed Data Interface
FDM Frecuency Division Multiplexing
FEBE Far End Block Errors
FEP Front-End Procesor
FIFO First Input First Output
FS Frame Status
FSK Frecuency Shift Keying
FTP File Transfer Protocol
GAN Global Area Network
GFC Generic Flow Control
HDLC High-level Data Link Control
HEC Header Error Control
Hubs Concentradores
ICD International Code Designator
IE Information Elements (en P-NNI)
IEEE Institute Electrics and Electronics Engineers
IETF Comisión de Investigación de Ingeniería Internet
IISP Interin Inster-Switch Protocol
ILMI Interim Local Managment Interface
IP Internet Protocol
IPX Internet Paquet Exchange
IRP Interior Routing Protocol
IS Intermediate System
ISDN Integrated Services Digital Network
ISL Inter-Link Switch
ISO International Organization for Standarization
ITU-T The Telecommunications Standardization Sector of the International Telecommunications
LAN Local Area Network
LANE Emulación LAN
LANE LAN Eulation
LAP-B Link Access Protocol Balanced
LE-ARP LAN Emulation ARP
LEC LAN Emulation Client
LECS LAN Emulation Configuration Server

LES LAN Emulation Server
LIFO Last Input First Input
LIS Logical IP Subnetwork
LOH Line Overhead
LTE Line Terminal Equipment
LLC Logical Link Control
MAC Medium Access Control
MAN Metropolitan Area Network
MARS Multicast Address Resolution Server
MAU Medium Attachment Unit
MAU Multistation Access Unit
MCTD Retardo de Transferencia de la Celda Medio
MFAS Multiframe Align Signal
MIB Managment Information Base
MID Identificador de Mensaje
MILNET Military Network
MPOA Multiprotocol over ATM
MPU Maximum Protocol Unit
MR Razón de Inserción de Celdas
MTU Maximum Transfer Unit
NAK Negative Acknowledge
NCC Network Control Center
NDC National Destination Code
NHRP Protocolo de Enruramiento de Próximo Brinco
NIC Netrwork Information Center
NIC Netrwork Interface Card
NLRI Network Layer Reachable Information
NNI Interface Red-Red, Interface Nodo-Red
NRM Normal Response Mode
NRZI Non Return Zero Inverted
NSAP Network Service Access Point
NSFNET National Science Foundation Network
NSN Número de Significancia Nacional
OAM Operation, Administration and Manteniance
OC-n Optical CARRIER
OSI Open System Interconection
OSIRM Open Systems Interconnection Reference Model

OSPF Open Shortest Path First
OUI Identificador Unico Organizacional
P/F Poll/Final
PAD Paquet Assambler and Disassambler
PBX Private Branch Exchange
PC Personal Computer
PDH Plesiochronous Digital Herarchy
PDM Physical Depend Medium
PDU Protocol Data Unit
PLCP Protocolo de Convergencia de Capa Física
PLR Paquet Lost Rate
P-NNI Protocol Network-Node Interface
POH Path Overhead
PRI Primary Rate Interface
PSCS Subcapa de Convergencia de Protocolo Específico
PSK Phase Shift Keying
PSP Paquet Per Second
PT Payload Type
PTE Path Terminal Equipment
PTSP Paquetes de Estado de la Topología (en P-NNI)
PVC Circuito Virtual Permanente
PVC Permanent Virtual Channel
QOS Quality of Service
RAI Remote Alarm Indicator
RARP Reverse ARP
RD Dominio de Enrutamiento
REJ Reject
RFC Request For Comments
RIP Routing Information Protocol
RNR Receive Not Ready
RR Receive Ready
SA Source Address
SAC Single Attachment Concetrator
SAP Service Access Point
SAR Subcapa de Segmentación y Reensamblaje
SAS Single Attachment Stations
SD Start Delimiter
SDH Sinchronous Digital Herarchy

SDU Service Data Unit
SEAL Capa de Adaptación Eficiente y Simple
SECBR Razón de Bloques de Celdas Serveramente Erroneos
SEL Selector
SMDS Switched Multimegabit Data Service
SMTP Simple Mail Transfer Protocol
SN Suscriber Number
SNA System Network Architecture
SNAP Subnetwork Attachment Point
SNMP Simple Network Managment Protocol
SOH Section Overhead
SONET Synchonous Optical Network
SPE Sinchronous Payload Envelop
SSCS Subcapa de Convergencia de Servicio Específico
SSRP Simple Server Redundancy Protocol
STDM Multiplexaje por División de Tiempo Estadístico
STE Section Terminal Equipment
STM-1 Sincronous Transport Module
STP Shielded Twisted Pair
STS-n Synchonous Transport Signal
SVC Switched Virtual Crcuit
SVC Swithced Virtual Channel
T1Trama de24 canales de voz en Norte America
TC Convergencia de Transmisión
TCP Transmission Control Protocol
TCP/IP Protocolo de Control de Transporte/Protocolo Internet
TDM Time Division Multiplex
TELNET Protocolo utilizado para establecer una sesión en una máquina remota.
TFTP Trivial File Transfer Protocol
TS Time Slot
TU Tributary Unit
TVL Tipo-Largo-Valor
UBR Undefined Bit Rate
UME Entidad de Administración UNI
UNAM Universidad Nacional Autonoma de Mexico

UNI User Network Interface
UTP Unshielded Twisted Pair
UU User to User
VBR Variable Bit Rate
VC Virtual Containers
VCC Virtual Channel Connection
VCC Virtual Channel Control
VLAN Virtual LAN
VP Virtual Path
VPC Virtual Path Connection
VPI Virtual Path Identifier
VT Virtual Tributary
WAN Wide Area Network

Bibliografía

1.-Bellamy, John
Digital Telephony
Sec. Edition
John Wiley & Sons, 1990

2.-Black, Uyless
Redes de Computadoras
Macrobit Editores, 1990

3.-Boisseau, M.
High Speed Networks
John Wiley & Sons, 1994

4.-Comer, Douglas
Internetworking with TCP/IP
Sec. Edition.
Prentice Hall, 1991

5.-Comer, Douglas
Redes Globales de Información con Internet y TCP/IP
Prentice Hall, 1996

6.-Flanagan, William
ATM Asychronous Transfer Mode User's Guide
Flaitron Publishing, Inc. Book, 1994

7.-Goralski, Walter
ATM
Computer Techonology Research Corp. 1994

8.-Hopper & Temple
Diseño de Redes Locales
Addison-Wesley Iberoamericana, 1994

9.-Martin, James
Local Area Networks
Sec. Edition
Prentice Hall,1994

10.-Mc Dysan & Spohn
ATM Theory and Application
Mc Graw Hill Series on Computer Communications, 1995

11.-Miller, Mark A.
Internetworking
A Guide to Network Communications LAN to LAN; LAN to WAN
M&T Books, 1990

12.-Schatt, Stan
Understanding ATM
Computer McGraw-Hill, 1996

13.-Stallings William
Data and Computer Communications
Mcmillan Publishing Company,1985

14.-Stallings, William
Data and Computer Communications
Fourth Edition
Mc Millian Publishing Company, 1994

15.-Stallings, William
Local and Metropolitan Area Networks
Fourth Edition
Mc Millian Publishing Company, 1993

16.-Stallings, William
Local and Metropolitan Area Networks
Fifth Edition
Mc Millian Publishing Company, 1996

17.-Craig Partridge
Gigabit Networking
Addison Weesley Publising Company

18.-Daniel Minoli
1st, 2nd, and Next Generation LAN´s
Ed. Mc. Graw Hill

19.-Gary C. Kessler, David A. Train
Metropolitan Area Networks
Ed. Mc. Graw Hill Inc.

20.-Gary y. Kim
Broadband LAN Technology
Ed Artech House

21.-Gilbert Held
Virtual LAN´s
Ed. John Wiley & Sons Inc.

22.-Howard W. Johnson
Fast Ethernet
Ed. Prentice Hall

23.-Mark A. Miller P.E.
Analyzing Broadband Networks
M&T Books

24.-Robert W. Klessing, Kaj Tesink
SMDS
Ed. Prentice Hall

25.-S. Fdida
High Performance Networking, V
Ed. North Holland

26.-The Forum ATM
ATM (User-Network Interface Specification)

27.-Uyless Black
TCP/IP and Related Protocols
Ed. Mc. Graw Hill Inc.

28.-Walter Goralski
ATM
Ed. Computer Technology Research Corp.

29.-William Stallings
Networking Standards
Addison Weesley Publising Company

DIRECCIONES ELECTRONICAS

- ATM, Gigabit Ethernet y Frame Relay
  http://www.specialty.com/hiband/atm.html

- Protocolos
  http://www.webcom.com/~llarrow/protocol.html

- Diseñando LAN´s conmutadas y VLAN´s.
  http://www.clarktech.com/al202.htm

- Conmutación Ethernet
  http://hpcc920.external.hp.com/rnd/technol/whtpaper/switch/switch.htm

- "White Paper" de LANE
  http://www.zeitnet.com/atm/lan1-2.html

- Generalidades de LAN Emulation
  http://www.iphase.com/Products/Technology/ATM/WP/LAN.html

- Tecnología Ipsilon-IP "switching"
  http://www.ipsilon.com/technology/papers/newman0001.htm

- LAN Emulation en Ambientes de Trabajo en Grupo
  http://www.impact.nl/Whiteppr/zeitnet/lan1-2.html

- Generalidades de 100VG-AnyLAN
  http://www.hp.com:80/rnd/technol/whtpaper/100vg/appnote/anylan.htm

- Software de ATM switches CISCO
  http://www.tech.ukerna.ac.uk/networking/atm/ls2020/IOSATM.html

- Aplicación de ATM en LAN´s
  http://www.uq.edu.au/~ccjon/itn530/assign2/itn530a2.htm

- Generalidades sobre Tecnología "Internetworking"
  http://www.CISCO.COM/univercd/data/doc/cintrnet/75818.htm

- Diseño de Interredes LAN Conmutadas
  http://www.ij.com/univercd/data/doc/cintrnet/idg3/idglans.htm

- Guía de Diseño de Interredes
  http://www.ij.com/univercd/data/doc/cintrnet/idg.htm

- Manual de Tenologías "Internetworking"
  http://www.cisco.com/cpress/data/cpress/fund/ith.htm

- Configuración de LANE e IP sobre ATM (CISCO)
  http://www.ij.com/univercd/data/doc/hardware/wbu/ls1010/rel_11_2/sw_cfg/enet_cnf.htm

- Configurando LANE (CISCO)
  http://www.ij.com/univercd/data/doc/software/11_0/rpcg/clane.htm

- El ATM switch LigthStream 1010 de CISCO
  http://www.ij.com/univercd/data/doc/hardware/wbu/ls1010/rel_11_2/pam_ins/pam_intr.htm

- Conmutación de Capa-3
  http://www.hp.com:80/rnd/technol/whtpaper/switch/abc/abc.htm

- Modulo ATM del Catalyst 5000
  http://www.ij.com/univercd/data/doc/hardware/cat5000/cfig_nts/3486_01.htm

- Configuración de Enrutamiento ATM y PNNI
  http://www.ij.com/univercd/data/doc/hardware/wbu/ls1010/rel_11_2/sw_cfg/pnni_cnf.htm

- Entendiendo Soluciones mediante Conmutación
  http://www.xyplex.com/product/white-paper/swexcpt.html

- MPOA
  http://www.data.com/Tutorials/MPOA_Ties_It_All_Together.html

- Caso de Estudio de Diseño de una Red
  http://cio.cisco.com/warp/public/729/c5000/netdn_wp.htm

- Conmutación de Capa de Red en el Catalyst 5000
  http://cio.cisco.com/warp/public/729/c5000/nlsc5_sd.htm

- Migrando a las LAN's conmutadas
  http://www.baynetworks.com/more/index.html

- Protocolo de Enruramiento de Respaldo
  http://www.cisco.com/warp/public/705/9.html
  http://www.cisco.com/warp/public/417/27.html

- Fast Ethernet
  http://moose.byu.edu/~christof/Fast_Ethernet.html