



**UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO**

**FACULTAD DE INGENIERIA**

**MIGRACION DE UNA RED X. 25 A UNA RED DE ALTA VELOCIDAD ATM.**

**T E S I S**

QUE PARA OBTENER EL TITULO DE:

**INGENIERO EN COMPUTACION**

P R E S E N T A N :

**MARIA CRISTINA LEON GONZALEZ**

**EDUARDO GABRIEL GARCIA GAMA**

**HECTOR AUGUSTO SOSA ROJAS**

DIRECTOR DE TESIS: ING. MANUEL MANRIQUEZ MIRANDA



CIUDAD UNIVERSITARIA.

*284905*

2000.



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

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

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

# TEMARIO

## Introducción

## Objetivo

### I. Antecedentes

	Páginas
I.1 Topologías de redes de computadoras.	1
I.1.1 Topología Jerárquica	1 - 3
I.1.2 Topología Horizontal o Bus	3
I.1.3 Topología de Estrella	3 - 4
I.1.4 Topología de Anillo o Token Ring	4
I.1.5 Topología de Malla	4
I.2 Análisis de las topologías de bus y anillo.	5
I.2.1 Análisis de la Topología Horizontal	5 - 7
I.2.2 Análisis de la Topología de Anillo	7 - 9
I.3 Arquitecturas y Protocolos.	9 - 12
I.4 Modelo de Referencia OSI.	12 - 13
I.4.1 Capa Física	13
I.4.2 Capa de Enlace de Datos	14
I.4.3 Capa de Red	14 - 15
I.4.4 Capa de Transporte	15
I.4.5 Capa de Sesión	15
I.4.6 Capa de Presentación	16
I.4.7 Capa de Aplicación	16
I.5 TCP/IP.	16 - 18
I.5.1 Protocolo IP	18 - 21
I.5.2 Protocolo TCP	21 - 27
I.5.3 Protocolo UDP	27 - 29

### II. Redes de Computadoras

II.1 Señalización y Conmutación.	30
II.1.1 Señalización	30 - 37
II.2 Redes de Area Local (LAN)	37 - 38
II.2.1 Métodos de Señalización de LAN	38 - 39
II.3 Redes de Area Metropolitana (MAN)	39 - 40
II.3.1 Características de las MAN	40
II.3.2 Topologías	41 - 47
II.4 Redes de Area Amplia (WAN)	47 - 49

### III. Técnicas de Transmisión en Redes de Computadoras

III.1 X.25.	50 - 51
III.1.1 HDLC (HIGH-LEVEL Data Link Control)	52
III.1.2 Configuraciones de Operación de HDLC	52 - 54
III.1.3 Formato de Trama de HDLC	54 - 55
III.1.4 Comandos y Respuestas de HDLC	56 - 58
III.1.5 Capas Inferiores de X.25	59 - 60
III.1.6 Características de X.25	60 - 63
III.1.7 Otros Tipos de Paquetes	63 - 64
III.1.8 Estados de los Canales Lógicas	65
III.1.9 Formatos de Paquete	65 - 67
III.1.10 Control de Flujo	68
III.1.11 Servicios de X.25	68 - 69
III.2 ISDN (Integrated Services Digital Network)	69 - 70
III.2.1 Servicios	70 - 71
III.2.2 Estándares	71 - 72
III.2.3 Estructura de Transmisión	72 - 74
III.2.4 Grupos Funcionales	74 - 75
III.2.5 B-ISDN (Broadband Integrated Service Digital Network)	75 - 78
III.3 Frame Relay.	79 - 80

III.3.1 Arquitectura de Frame Relay	80 - 82
III.3.2 Formato de la Trama de Frame Relay	82 - 87
III.3.3 Congestión de Red	87 - 88
III.3.4 Protocolo LMI	88 - 90
<b>IV. Tecnología ATM</b>	
IV.1 Definición y Conceptos.	91 - 92
IV.1.1 Multiplexaje Estadístico y Cell Relay Switching	92 - 93
IV.1.2 Modos de Transferencia	94
IV.1.3 Interfaces de una Red ATM	94 - 95
IV.1.4 Canal Virtual y Ruta Virtual	95 - 96
IV.2 Canal Virtual y Ruta Virtual.	
IV.2.1 Establecimiento de la Conexión de Canal Virtual (VCC)	96
IV.2.2 Identificadores de Canal Virtual (VCIs) e Identificadores de Ruta Virtual (VPis)	97
IV.3 Formato de la Celda ATM.	97 - 100
IV.4 Capas de Adaptación AAL.	100 - 103
IV.4.1 Servicios	103 - 104
IV.4.2 Protocolos AAL	104 - 109
IV.5 Control de Tráfico y Congestión	109
IV.5.1 Conceptos Generales	110 - 114
IV.5.2 Control de Admisión de Conexión (CAC)	114 - 121
IV.5.3 Control de Parámetros de Uso y de Red	121 - 122
IV.5.4 Control de Congestión	122 - 124
IV.6 Switch ATM.	124 - 131
IV.7 Emulación de Redes LAN.	131 - 138
IV.8 Operación y Mantenimiento.	138 - 140
IV.9 Administración en ATM.	140 - 145
<b>V. ATM contra X.25 y otras tecnologías</b>	
V.1 ATM contra X.25.	146 - 147
V.2 ATM contra Frame Relay.	147 - 149
V.3 ATM contra ISDN.	150 - 151
V.4 ATM contra Gigabit Ethernet.	151
V.4.1 Calidad de Servicio (QoS)	151- 152
V.4.2 Escalabilidad de Ancho de Banda	152
V.4.3 Redes Virtuales de Ruteo	152 - 153
V.4.4 Costo	153
V.5 IP + ATM	153 - 154
V.5.1 Redes IP - ATM	154 - 158
V.6 Voz sobre ATM	158 - 168
<b>VI. Migración de X.25 a ATM</b>	
VI.1 Proyecto de Migración.	169 - 170
VI.2 Estudio de la Red Actual.	171 - 179
VI.3 Propuesta de Solución.	179 - 189
VI.4 Propuesta de Implementación	189 - 190
VI.4.1 Etapa 1	190 - 192
VI.4.2 Etapa 2	193
VI.4.3 Etapa 3	193

**Conclusiones**

**Bibliografía**

**Apéndice A. Glosario de Términos**

## INTRODUCCION

Los rápidos avances que existen en las tecnologías de la computación y las comunicaciones han ocasionado una dependencia e interrelación cada vez mayor entre estos campos. Las líneas divisoras entre equipo de cómputo, conmutación y de transmisión digital son cada vez más difusas, y las mismas técnicas digitales se utilizan para transmisión de datos, voz e imágenes. Las tecnologías emergentes y la necesidad de una recolección, procesamiento y diseminación de información más eficiente, han llevado al desarrollo de sistemas integrales que transmitan y procesen todo tipo de datos. El objetivo final de esta evolución es algo que se conoce como la Red Digital de Servicios Integrados, o ISDN.

Aunque ISDN todavía necesita un gran esfuerzo de estandarización, ya se encuentra en su segunda generación. La primera generación, algunas veces referida como ISDN de banda angosta, se basa en la utilización de canales de 64 Kbps como la unidad básica de conmutación, y es orientada a la conmutación de circuitos. La mayor contribución del desarrollo de ISDN de banda angosta es *Frame Relay*.

La segunda generación, a la que se suele llamar ISDN de banda ancha, o B-ISDN, soporta tasas de datos muy altas (del orden de cientos de Mbps) y es orientada a la conmutación de paquetes. La mayor contribución técnica del esfuerzo B-ISDN es el Modo de Transferencia Asíncrono (ATM).

Algunos ejemplos de las tendencias actuales que están presionando para el desarrollo de ISDN y B-ISDN son las siguientes:

- *Computadoras trabajando en conjunto en lugar de trabajar aisladas.* El porcentaje de computadoras personales que tienen capacidad de comunicación con otros equipos va en aumento cada día. En el pasado, la típica computadora corporativa era un dispositivo aislado que funcionaba independiente de otros. Hoy día, los negocios dependen de una mezcla de una gran cantidad de computadoras grandes, medianas y pequeñas que intercambian mensajes y comparten recursos y datos.
- *El volumen y la riqueza de datos se está incrementando drásticamente.* La evolución de las computadoras personales ha dado como resultado sistemas a colores y con gráficos de alta resolución. Se están desarrollando aplicaciones que

cada vez requieren mucha mayor capacidad de las redes sobre las que se desempeñan. Ejemplos de estas aplicaciones incluyen los aparatos digitales de fax, procesadores de imágenes y de documentos y otros programas gráficos. Resoluciones de 1024 x 768 por página ya son comunes en este tipo de aplicaciones. Aún con técnicas de compresión, esto genera una carga muy grande de tráfico en las comunicaciones de datos.

- *Incremento a nivel nacional y global de transacciones comerciales electrónicas.* El negocio de la Bolsa se ha vuelto dependiente de redes casi en un 100%, en el cual la transmisión automática de información y órdenes de compra-venta es crucial. La Banca hoy en día consiste de algo más que cajeros automáticos y contabilización computarizada; el dinero en sí mismo está cada vez más relacionado con la información conforme se da la transferencia de fondos sobre redes de datos cada vez mayores. Compañías de todos los tamaños cada vez involucran más a las telecomunicaciones para sus actividades diarias, tales como entrada remota de datos, correo electrónico, transmisión de faxes y sistemas de apoyo a decisiones. Las corporaciones multinacionales y socios de negocio de diferentes países dependen del rápido intercambio de información. Las redes de comunicación son indispensables en la globalización del comercio y la industria.
- *Aumento en la interacción de persona a persona.* Los negocios están respondiendo a la necesidad de interacción de sus empleados que se encuentran en diferentes localidades, por medio de algo más que el teléfono, por medio de correo electrónico, correo de voz, transferencia de archivos, intercambio de documentos y videoconferencia. Todas estas aplicaciones demandan una gran utilización de recursos de las redes de comunicaciones.
- *Automatización de las oficinas.* Se puede definir como la incorporación de la tecnología apropiada en las oficinas para que las personas puedan administrar la información. La motivación principal para esta automatización es el incremento en la productividad. Conforme el porcentaje de trabajadores de 'cuello blanco' se ha incrementado, también ha aumentado la información y el papeleo. Los directores, administradores y trabajadores de la información se ven enfrentados a sus propias limitantes de productividad. El trabajo necesita hacerse más rápido con menor tiempo de espera entre segmentos de una tarea. Esto requiere de un mejor acceso a la información y una mejor comunicación y coordinación con otros.

## OBJETIVO

La finalidad del presente trabajo de tesis es el estudio para reemplazar una red privada de telecomunicaciones basada en x.25 hacia una red de Alta Velocidad ATM mediante los siguientes puntos:

- Realizar el análisis de la situación actual de una red de datos con tecnología X.25 y proponer su optimización mediante la migración de su backbone y nodos de mayor importancia a tecnología ATM.
- Aprovechar las ventajas de utilizar tecnología ATM sobre X.25, en la transmisión de voz, datos y video, además de mejorar, incrementar e integrar los servicios que proporciona.
- Ofrecer las recomendaciones sobre el desempeño efectivo de la red ATM cubriendo las necesidades actuales y futuras de telecomunicaciones.

# Capítulo I

## ANTECEDENTES

### I.1 Topologías de Redes de Computadoras

Se le conoce como topología de red a la forma o conectividad física de la misma, es decir, la forma como sus nodos se conectan y comunican entre sí. El término topología se toma prestado del campo de la geometría y se utiliza para describir la forma de algo.

Aunque pueden existir muchas configuraciones diferentes de redes de computadoras, casi todas ellas están formadas por uno o más de los siguientes tipos básicos, como se muestra en la fig. 1.1

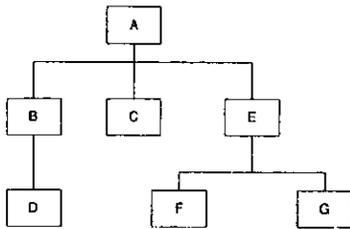
- Topología Jerárquica o de Arbol
- Topología Horizontal o de Bus
- Topología de Estrella
- Topología de Anillo
- Topología de Malla

#### I.1.1 Topología Jerárquica.

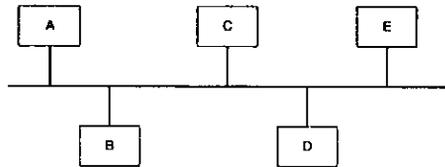
Es una topología muy común para sistemas centralizados de cómputo, puesto que el software de control es relativamente sencillo y se tiene un punto de concentración y solución de errores. En la mayoría de los casos, el nodo de mayor jerarquía es el que controla la red. En el esquema de la fig. 1.1(a), el flujo de datos entre los diferentes nodos es controlado por A. Algunas implementaciones incorporan un poco de distribución del sistema al permitir que los nodos de un orden de jerarquía controlen a sus subordinados de orden inferior. Esto reduce la sobrecarga del servidor central A.

Aunque esta topología es muy atractiva desde el punto de vista de la simplicidad de control, es muy sensible a problemas que ocasionen cuellos de botella. En algunos casos, el nodo más alto (que puede ser una computadora tipo mainframe) controla todo el tráfico entre los nodos. Esto no únicamente baja el rendimiento real del servidor para otros

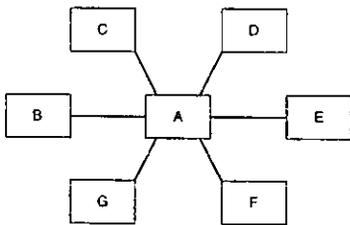
procesos, sino que también presenta problemas de confiabilidad. Si el servidor central falla, la red completa deja de operar, a menos que se tenga un servidor de respaldo o un servidor dedicado de comunicaciones. Sin embargo, el mantenimiento y crecimiento de este tipo de redes es muy sencillo, pues no cuesta demasiado trabajo agregar nuevos nodos subordinados.



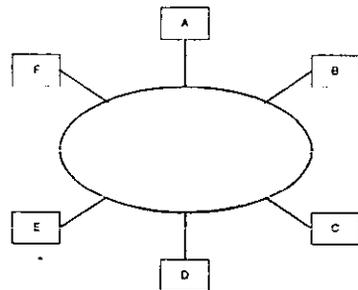
(a) Topología Jerárquica o de Arbol



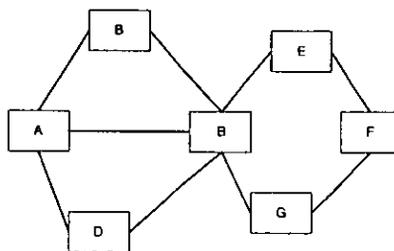
(b) Topología Horizontal o de Bus



(c) Topología de Estrella



(d) Topología de Anillo



d) Topología de Malla

**Fig. 1.1 Topologías de Red**

A este esquema también se le conoce como una red vertical o de árbol, debido a que su configuración es similar a la de ramas que van naciendo y multiplicándose de la rama del nivel anterior.

### **1.1.2 Topología Horizontal o Bus.**

Esta topología se encuentra ilustrada en la fig. 1.1(b). Este tipo de arreglo es muy popular en redes de área local, las cuales se discutirán en el siguiente capítulo. El control del flujo de tráfico es relativamente sencillo por el hecho de que todas las estaciones están conectadas a un medio de transmisión común, lo cual permite que todas ellas reciban todas y cada una de las transmisiones. Sin embargo, su principal desventaja consiste precisamente en que sólo existe un canal de transmisión para todos los dispositivos que se encuentran conectados a la red. En consecuencia, si existe una falla en dicho canal, se pierde toda la red. Esto se puede evitar mediante el uso de canales redundantes o de switches de *bypass* alrededor de los nodos por si éstos fallan.

Otro problema con esta configuración en particular es la dificultad que existe para aislar e identificar fallas en cualquier componente en particular, pues carece de puntos de concentración.

### **1.1.3 Topología de Estrella**

Es un esquema que presenta una gran simplicidad de control, el software no es complejo y el flujo de tráfico es sencillo. Fue muy utilizado en la década de los 60's y principios de los 70's.

Todo el tráfico emana del centro de la estrella - el servidor central A de la fig. 1.1(c). Este nodo tiene el control completo de los demás nodos conectados a él. En realidad es una configuración muy similar a la topología jerárquica, pero con menos capacidad de procesamiento distribuido.

En vista de que A es responsable de rutear el tráfico de los demás componentes, también es responsable de aislar las fallas. Esto es relativamente sencillo en una red tipo estrella porque las líneas pueden ser aisladas individualmente para identificar el

problema. Sin embargo, al igual que en la estructura jerárquica, este tipo de red también es susceptible de sufrir cuellos de botella y fallas en el nodo central. Del mismo modo, es posible establecer enlaces redundantes y un respaldo del nodo central, para aumentar su confiabilidad.

#### **1.1.4 Topología de Anillo o Token Ring**

Tal como se puede observar en la fig. 1.1(d), esta topología recibe este nombre por el aspecto circular del flujo de datos. En la mayoría de los casos, la información fluye exclusivamente en un sentido con una estación recibiendo la señal y transmitiéndola a la siguiente estación en el anillo.

Esta configuración es muy popular puesto que no tiene los problemas de cuellos de botella que presentan las estructuras jerárquicas. Además, la lógica necesaria para implementar una red en anillo es relativamente sencilla. Cada componente tiene la tarea de aceptar los datos, enviarlos al siguiente nodo, o enviarlos nuevamente al anillo al siguiente componente intermedio. Sin embargo, como todas las redes, esta configuración también tiene sus propios problemas. El principal es que, como en la topología de bus, existe un sólo canal que conecta a todos los componentes de la red. Si el canal entre dos nodos adyacentes falla, se pierde toda la red. Nuevamente, una solución a esta situación puede ser el tener canales de respaldo. También se pueden instalar switches que enruten automáticamente los datos para evitar nodos congestionados o inoperantes.

#### **1.1.5 Topología de Malla**

Representada en la fig. 1.1(e), tiene el atractivo de que es poco afectada por cuellos de botella y problemas de fallas de componentes. Debido a la multiplicidad de rutas posibles entre nodos, es posible rutear el tráfico por varios enlaces si uno de aquellos falla o se encuentra muy ocupado. Aunque esta configuración ofrece el máximo de confiabilidad, el control de flujo de información es sumamente costoso y complejo, tanto en consumo de recursos como en precio.

## I.2 Análisis de las Topologías de Bus y Anillo

Debido a la popularidad de estos dos tipos de redes, es conveniente entrar a un estudio más profundo de varios aspectos referentes a ellas.

### I.2.1 Análisis de la Topología Horizontal

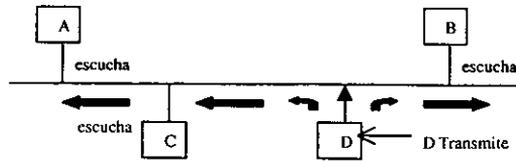
Una implementación particular de una topología de bus es la *Ethernet*, la cual ha tenido tanto éxito, que el término ha llegado a suplantar al original. Aquí también utilizaremos el término Ethernet para referirnos a las redes tipo bus. Ethernet fue desarrollada por Xerox, y fue llamada así por el *ether luminífero*, substancia que en el siglo XIX se pensaba existía y era responsable de la propagación de las ondas electromagnéticas. A continuación se describe su método de acceso al medio.

#### Método de Acceso al Medio (CSMA/CD)

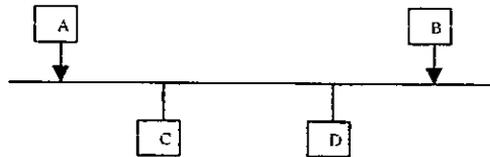
Este tipo de red utiliza una familia de métodos de acceso al medio y transmisión llamada CSMA/CD (Carrier Sense-Multiple Access/Collision Detection), o Múltiple Acceso-Sensado de Portadora/Detección de Colisiones.

Una de las técnicas que existen para que una estación pueda tomar control del canal y comience a transmitir, es la de sensado *no persistente* de portadora, la cual permite que las estaciones transmitan inmediatamente en cuanto determinan que el canal está libre. Si el canal está ocupado, esperan un tiempo arbitrario antes de volver a sensar el canal. Otra técnica, la de sensado *p-persistente* de portadora, tiene un algoritmo de espera en cada estación ( $p$  representa una probabilidad). Por ejemplo, en la fig. 1.2 se representan cuatro estaciones, A, B, C y D en una topología de bus. Supongamos que las estaciones A y B intentan transmitir, mientras que es la estación D quien se encuentra transmitiendo actualmente. Con esta técnica, las estaciones A y B no transmiten al momento que sensan que el canal se ha desocupado, sino que invocan a una rutina que genera una espera aleatoria, normalmente de unos cuantos microsegundos. Si una estación sensa el canal como ocupado, entonces espera una ranura fija de tiempo y vuelve a intentarlo. Dicha estación transmitirá con una probabilidad  $p$ , mientras que la probabilidad de que tenga que esperar hasta la siguiente ranura de tiempo es  $1 - p$ . Sin

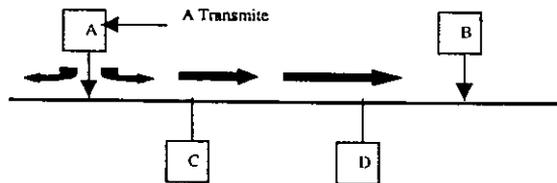
embargo, existe una tercera técnica, la portadora *1-persistente*, que permite que la estación transmita inmediatamente después de determinar que el canal se encuentra libre, pero si ocurre una colisión, entonces la estación espera un tiempo arbitrario antes de volver a sensar el canal. El método es llamado 1-persistente porque la estación transmite con una probabilidad de 1 cuando detecta que el canal esta libre. En la tabla 1.1 se muestran estas tres técnicas.



(a) Portadora sensada, las estaciones A y B difieren transmisión



(b) Canal libre, A y B Intentan Tomar Control



(c) A transmite y B Difiere

**Fig. 1.2** Sistemas de Sensado de Portadora y Colisión

Condición	no-persistente	p-persistente	1-persistente
Canal libre	Transmite inmediatamente	Transmite con $p$ , Espera con $1-p$	Transmite inmediatamente
Canal ocupado	Espera aleatoria y sensado	Transmite con $p$ , Espera con $1-p$	Sensa continuamente
Colisión	Retransmisión aleatoria	Retransmisión aleatoria	Retransmisión aleatoria

Tabla 1.1 Técnicas de sensado de portadora

La técnica p-persistente está diseñada para cumplir una meta 1-persistente de canal libre y una meta no-persistente de reducción de colisiones. Sin embargo, la técnica más favorecida es la 1-persistente.

Asumamos ahora que la estación A de la fig. 1.2(c) obtiene el control del canal antes de que la estación B tenga siquiera la oportunidad de terminar su espera aleatoria. Cuando B termina su espera, se encuentra con que A está transmitiendo. Sin embargo, puesto que la señal de A tiene un tiempo de propagación antes de que llegue a B, ésta estación puede transmitir un paquete aún cuando A supuestamente ha tomado el control. A este problema se le conoce como *ventana de colisión*, y es un factor del retraso por propagación de la señal y la distancia entre dos estaciones que compiten por el canal. Mientras más grande sea la distancia, mayor será la ventana y por tanto habrá mayores probabilidades de colisión. Sin embargo, este efecto puede ser mitigado al usar paquetes más grandes.

Las colisiones son detectadas gracias a la capacidad de las estaciones de transmitir y escuchar simultáneamente. Al chocar dos señales, se crean irregularidades de voltaje que son sensadas por las estaciones involucradas, que entonces suspenden su transmisión y esperan un periodo aleatorio. Ya que ambas estaciones generarán tiempos de espera diferentes, es poco probable que ambas estaciones incurran en una nueva colisión.

### 1.2.2 Análisis de la Topología de Anillo

Este tipo de redes ha estado presente por muchos años, pues uno de sus atractivos es el hecho de que el anillo no es un medio de transmisión común a todas las estaciones, como lo es el caso de la topología de bus; en cambio, es una colección de

enlaces punto a punto individuales que forman un círculo. Además, la ingeniería del anillo es puramente digital a diferencia de la anterior topología que tiene una componente analógica muy fuerte sobre todo en la detección de colisiones.

Existen varios tipos de anillos, pero aquí describimos el método de acceso y desempeño de un caso particular conocido como *Token Ring*

### **Método de Acceso al Medio (Paso de Token)**

El token es un patrón especial de bits que circula alrededor de la red, y que tiene la función de indicar si el medio se encuentra libre para transmisiones. Las estaciones se encuentran conectadas a un anillo concéntrico a través de una interfase. Esta interfase es la encargada de monitorear los datos que pasan a través de ella, así como regenerar la transmisión y pasarla a la siguiente estación o copiarla y entregarla a la estación a la cual se encuentra conectada si es que la trama está destinada a ella. Cuando una de ellas quiere transmitir, retira el token del anillo y coloca en su lugar la trama con información. Algunas implementaciones permiten que el token continúe circulando pero con una marca de ocupado. De cualquier forma, sólo puede tener control del canal la estación que posee el token marcado como libre cuando desea transmitir; de otro modo, tiene que esperar a que le llegue, y cómo sólo existe un token en el anillo, sólo puede transmitir una estación a la vez.

Como se mencionó anteriormente, un anillo en realidad es una colección de interfases conectadas por líneas punto a punto. Cada bit que llega a una de ellas se copia a un buffer de 1 bit y después se copia nuevamente al anillo. Mientras se encuentra en el buffer, se puede inspeccionar el bit y modificarlo, si es necesario, antes de escribirlo de vuelta al anillo. Este proceso de copia introduce un retraso de 1 bit entre cada interfase. Ahora bien, el token siempre debe estar contenido de manera completa en un instante dado en el anillo por lo que éste debe tener suficientes retrasos y capacidad de bits simultáneos. Por eso la importancia del llamado tamaño físico del bit.

Las interfases del anillo normalmente tienen dos modos de operación, atención y transmisión. En el modo de atención, simplemente se copian los datos de la entrada a la salida con el mencionado retraso de 1 bit. En el modo de transmisión, la interfase rompe

la conexión de entrada y salida e introduce sus propios datos al medio. Para poder cambiar de modo de escucha a modo de transmisión en el tiempo de 1 bit, la interfase normalmente debe tener guardadas en un buffer una o más tramas, para no tener que solicitarlas en ese momento a la estación. En este caso general, las tramas no tienen límite de tamaño, pues la trama nunca aparece completa en un instante dado en el anillo.

Cuando el tráfico es ligero, el token pasa la mayor parte del tiempo simplemente circulando alrededor del anillo. Ocasionalmente, una estación lo toma, transmite una trama, y luego regenera el token. Sin embargo, cuando el tráfico es tan pesado al grado de que existe una cola de tramas en cada estación, tan pronto como una de estas estaciones termina su transmisión y regenera el token, la siguiente estación adyacente verá y removerá el token. De este modo, el permiso de transmitir se trunca sin problemas en forma *round-robin*. La eficiencia de la red se aproxima al 100 por ciento bajo condiciones de carga pesada.

### **I.3 Arquitecturas y Protocolos**

Para poder entender lo que es la arquitectura de una red de computadoras, primero debemos exponer brevemente el concepto de protocolo. Un protocolo es una serie de convenciones utilizadas para comunicaciones, y es un conjunto de reglas mutuamente acordadas que establecen cómo dos o más elementos deben interactuar para establecer un intercambio de información.

Los elementos de cualquier protocolo son los siguientes:

- *Sintaxis*: La estructura de la información comunicada, incluyendo cosas tales como el formato de los datos, la codificación y la representación de los mismos en términos de niveles de señal.
- *Semántica*: El significado de la información que se intercambia, incluyendo control de información para coordinación y manejo de errores.
- *Tiempos de Coordinación*: Tiempos en los cuales los datos deben ser transmitidos o buscados para lectura por un receptor, la manera de secuenciar la información, igualación de velocidades, y otras por el estilo.

Para reducir la complejidad de diseño, la mayoría de las redes de computadoras se encuentran organizadas en una serie de capas o niveles, cada uno construido sobre su predecesor. El número, nombre, contenido y función de cada capa puede variar de red a red. Sin embargo, en todas las redes, el propósito de cada capa es ofrecer un tipo de servicio a las capas superiores, aislándolas de los detalles sobre cómo son proporcionados esos servicios. Estas capas se comunican con sus equivalentes en otra máquina por medio de un protocolo común. Si esta conversación se da en un nivel  $n$ , entonces se utiliza un *protocolo de capa  $n$* , como se puede apreciar en la fig. 1.3. para una red con siete capas.

El conjunto de capas y sus protocolos relacionados es a lo que se le conoce como una *Arquitectura de Red*. La especificación de la arquitectura debe contener información suficiente para permitir al implementador escribir el programa o construir el hardware de cada capa para que obedezca apropiadamente el protocolo respectivo. Ni los detalles de implementación ni la especificación de las interfaces forman parte de la arquitectura porque se encuentran escondidos en las máquinas y no son visibles desde fuera.

Las entidades que enlazan capas del mismo nivel en diferentes máquinas se conocen como *procesos comunicantes*. En otras palabras, son estos procesos los que se comunican entre sí utilizando los protocolos.

La forma en que se realiza el enlace entre dos capas de nivel  $n$  en diferentes máquinas para la transferencia de datos, se realiza pasando los datos e información de control a la capa directamente abajo de ella, hasta alcanzar la más baja o capa 1. Después de la capa 1, se encuentra el medio físico o canal por donde se transmiten realmente los datos. En la fig. 1.3 se muestra la comunicación virtual por líneas punteadas y la comunicación física por líneas sólidas

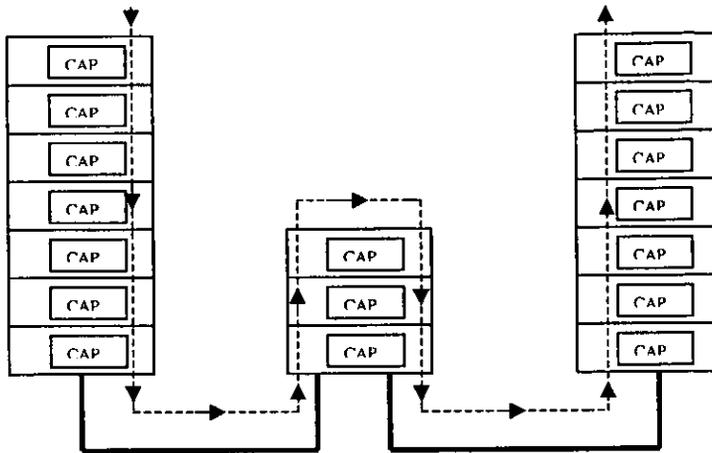


Fig. 1.3 Arquitectura de Capas

Entre cada par de capas adyacentes existe una interfase que define las operaciones básicas y servicios que le ofrece la capa inferior a la superior. Una interfase limpia minimiza la cantidad de información que debe ser comunicada entre capas, y además hace más sencillo el reemplazar una implementación de una capa con una diferente cuando cada capa realiza una colección específica de funciones bien comprendidas.

Se explica ahora con un ejemplo la comunicación multinivel para el esquema de la fig. 1.3

Un mensaje  $m$  se produce en la capa 7. El mensaje se pasa de la capa 7 a la capa 6 de acuerdo a la interfase 6/7. La capa 6 hace algún tipo de proceso (compresión de datos, por ejemplo) y luego envía el nuevo mensaje,  $M$ , a la capa 5 a través de la interfase 5/6. La capa 5, en este ejemplo, no modifica la información sino que únicamente regula la dirección del flujo de información.

En la mayoría de las redes, no existe tamaño límite para el tamaño de los mensajes aceptados por la capa 4, pero si existe un límite impuesto por la capa 3. En consecuencia, el nivel 4 debe dividir el mensaje entrante en unidades mas pequeñas, agregándole un *encabezado* a cada unidad. Dicho encabezado contiene información de control, tal como números de secuencia, para permitir que la capa 4 en la máquina de

destino pueda reensamblar el mensaje original en caso de que las capas inferiores no conserven la secuencia original.

La capa 3 decide cuál de las líneas de salida utilizar, agrega sus propios encabezados, y pasa los datos a la capa 2. La capa 2 no únicamente agrega un encabezado a cada pieza de información, sino también una *cola*, y entrega la unidad resultante a la capa 1 para su transmisión física. En la máquina receptora el mensaje se mueve hacia arriba, de capa en capa, y siendo removidos sus encabezados progresivamente. Ninguno de los encabezados de las capas inferiores a  $n$  son vistos por la capa  $n$ .

#### **1.4 El Modelo de Referencia OSI**

Una vez que hemos explicado en la sección 1.3 la forma en que se divide en capas una red, presentaremos el modelo estándar que actualmente predomina en los sistemas de comunicaciones y que está basado en el concepto de arquitectura en forma de capas.

Para resolver los problemas que dificultaban la comunicación entre sistemas, debido a las diferentes arquitecturas en las telecomunicaciones, la Organización Internacional de Estándares, International Standards Organization (ISO) desarrolló una arquitectura de comunicación estándar que permite a los sistemas, comunicarse abiertamente. Después de dos años de trabajo, en 1980 se obtuvo el "Modelo de Referencia para la Interconexión de Sistemas Abiertos" (Open Systems Interconnection - OSI - Reference Model), comúnmente llamado "Modelo OSI", el cual fue aprobado y adoptado como un estándar internacional en el año de 1983.

El modelo consiste de siete capas y su propósito principal es proporcionar las bases para coordinar el desarrollo de estándares que relacionen la interconexión flexible de los sistemas, utilizando las facilidades de la comunicación de datos. Cada capa cumple con un conjunto de funciones específicas para a su vez proporcionar un conjunto de servicios a la capa superior, sin informar al resto de las capas de la forma en que esto se logra.

La estructura del modelo OSI se muestra en la fig. 1.4, la cual indica el intercambio de datos entre dos aplicaciones, con un nodo intermedio. La figura muestra el flujo bidireccional de información, la cual pasa en ambas direcciones por las siete capas en los dos puntos finales, pero solamente a través de las tres capas más bajas en los puntos intermedios. Al igual que en la fig. 1.3, las líneas punteadas representan la comunicación virtual y las líneas continuas representan la comunicación física. A continuación describiremos brevemente cada capa del modelo, comenzando por la capa más baja.

#### **1.4.1 Capa Física**

Es la responsable de la transmisión de bits a través de un medio físico. En este nivel se especifican las conexiones de cables y las reglas eléctricas necesarias para transferir datos entre dispositivos. También es responsable de asegurarse que un bit 1 se interprete correctamente en el extremo receptor y esto implica determinar cuantos volts se requieren para representar un 1 y cuantos para un cero, cuantos pins tiene el conector de red y para que es usado cada uno de ellos.

Los protocolos para esta capa incluyen procedimientos mecánicos, eléctricos u ópticos y funcionales para la activación, el mantenimiento y la desactivación física de la conexión, considerando las especificaciones de conectores físicos, cables y señales eléctricas u ópticas.

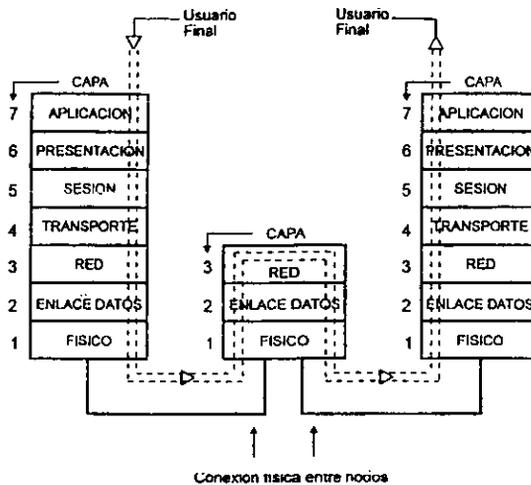


Fig. 1.4 Modelo de Referencia OSI

### 1.4.2 Capa de Enlace de Datos

El nivel de enlace de datos permite la transmisión de datos sin errores entre dos entidades de la red, controlando la transmisión cuando varios dispositivos comparten el mismo circuito físico. La información se concentra en forma de tramas.

Por diferentes razones se pueden presentar daños o pérdidas de tramas o de acuses de recibo de tramas y esta capa es la responsable de resolver estos problemas. También protege a las capas superiores de cualquier cosa que tenga que ver con el medio físico de transmisión.

### 1.4.3 Capa de Red

Es la responsable de establecer, mantener y terminar la conexión de red entre dos entidades de transporte y de la transferencia de datos de tal manera que permita mantener a cualquier capa superior al tanto del estado de la conexión. Entre las funciones principales de la capa de red se incluyen la determinación de un enrutamiento óptimo sobre las posibles conexiones de red, segmentar paquetes con el propósito de facilitar la

transferencia de paquetes sobre conexiones de red, seleccionar y conservar una calidad de servicio y actividades de administración.

#### **1.4.4 Capa de Transporte**

Esta capa cumple con las funciones de establecer las conexiones de transporte entre entidades, transferencia de datos y liberación de conexiones. Además se encarga de transferir los mensajes completos entre dos entidades de sesión a un nivel de calidad de servicio preestablecido.

Sus principales funciones son, el control de error, secuenciación de las unidades de datos transferidas, control de flujo de datos para prevenir sobrecargas de la red y administración de actividades de supervisión.

La capa de red tiene que ver con la interfase entre los dispositivos del usuario y la red, mientras que la capa de transporte y las capas superiores tienen que ver con la interacción de extremo a extremo entre los procesos de los usuarios. Las funciones ejecutadas en la capa de transporte pueden incluir controles de integridad de extremo a extremo para prevenir pérdidas o doble procesamiento de operaciones, control de flujo de operaciones y direccionamiento de los dispositivos del usuario final o procesamientos. En esta capa no es importante la ruta específica que se use a través de la red, sólo es importante que la transferencia de datos se haga de manera confiable.

#### **1.4.5 Capa de Sesión**

La capa de sesión proporciona un conjunto de reglas que estandarizan los procesos de inicio y terminación de una sesión. Una sesión permite transporte ordinario de datos, tal como lo hace la capa de transporte, pero también provee servicios que pueden ser útiles para algunas aplicaciones.

Uno de los servicios de la capa de sesión, es proporcionar el control de diálogo. Las sesiones pueden permitir que el tráfico vaya en ambas direcciones al mismo tiempo o bien, en una sola dirección.

#### **1.4.6 Capa de Presentación**

La capa de presentación realiza funciones relacionadas con la sintaxis y semántica de la información transmitida. Entre las funciones que se ejecutan en esta capa se encuentran la iniciación de una transferencia de datos desde una entidad de aplicación o usuario a otro, negociación y re-negociación para la selección de la sintaxis que será utilizada en la transferencia de datos y transformación o conversión de datos que se solicite.

#### **1.4.7 Capa de Aplicación**

La capa de aplicación tiene que ver con las funciones de las capas superiores que proporcionan soporte a las actividades del sistema o la aplicación, por ejemplo, soporte al operador, control de la transferencia de archivos, actividades de bases de datos distribuidos, etc.

También proporciona procesos de aplicación con un punto de acceso al sistema y proporciona un medio para que los procesos de aplicación tengan acceso a las facilidades de interconexión del sistema para el intercambio de información. Efectúa todas las funciones relacionadas a la comunicación entre sistemas las cuales no fueron proporcionadas por las capas inferiores. Estas funciones incluyen aquellas realizadas por la gente o por los programas de aplicación. Esta es la capa más difícil de estandarizar y el modelo OSI no define las funciones específicas que deben ser realizadas.

#### **1.5 Protocolo TCP/IP**

El origen de TCP/IP se debe a la DARPA (Defense Advanced Research Projects Agency) que depende del Departamento de Defensa (DoD) de los Estados Unidos. En 1969, el DoD comenzó a desarrollar una red de conmutación de paquetes llamada ARPANET que abarcaba varios proyectos de ciencias de la computación e investigación militar.

La red creció con diferentes tipos de computadoras en universidades y centros de investigación alrededor del país. En 1973, un proyecto de interconexión de redes se inició

en la universidad de Stanford que involucró después a otras universidades. Para el año de 1978 existían 4 versiones desarrolladas y probadas de TCP; para 1980 la *suite* era estable facilitando la conectividad a través de las computadoras en ARPANET. En 1983, todos los usuarios de ARPANET estaban siendo conectados con los nuevos protocolos TCP/IP. Ese año, TCP/IP se convirtió en el estándar para el uso de la internet del DoD, incluyendo ARPANET. A pesar de que ARPANET ha sido reemplazado por otras redes los protocolos TCP/IP se siguen usando.

TCP/IP es una familia de protocolos formada por el *Transmission Control Protocol* (TCP), *Internet Protocol* (IP), *User Datagram Protocol* (UDP), *Address Resolution Protocol* (ARP), *Reverse Address Resolution Protocol* (RARP) y el *Internet Control Message Protocol* (ICMP).

El principal propósito de TCP/IP es construir una interconexión de redes que proporcione servicios de comunicación universal. Cada red física tiene su propia interfase de comunicación dependiente de la tecnología que proporciona funciones de comunicación básicas. Los servicios de comunicación son proporcionados por el software que corre entre la red física y las aplicaciones del usuario y que proporciona una interfase común para esas aplicaciones, independientemente de la red física establecida. La arquitectura de las diferentes redes físicas interconectadas es transparente para el usuario, de tal forma que le da la apariencia de estar conectado a una sola red. Tal conjunto de redes interconectadas es llamado internetwork o internet.

TCP/IP comprende esencialmente las capas de red, de transporte, de presentación y de aplicación del modelo OSI. Las dos últimas se engloban en una sola capa llamada de aplicación y no incluye una capa de sesión debido a que ésta es propia de los sistemas de tiempo compartido que no se emplean en un medio ambiente como el de TCP/IP.

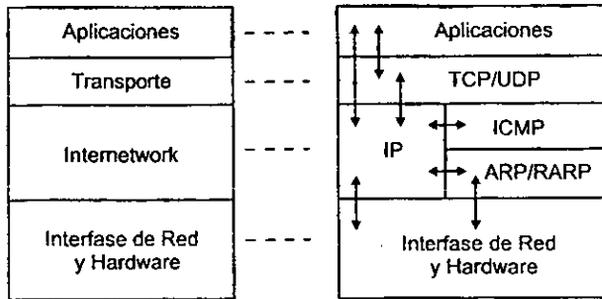


Fig. 1.5 Estructura de TCP/IP

El software del protocolo IP corre tanto en las computadoras que se comunican como en los routers que las enlazan, mientras que el software del protocolo TCP sólo corre en las computadoras donde están las aplicaciones.

TCP es un protocolo *full duplex*, orientado a conexión que envía mensajes de extremo a extremo y es confiable porque asegura que los mensajes serán entregados al programa de aplicación destino en secuencia, sin pérdida, sin error y sin duplicación.

### 1.5.1 Protocolo IP

IP es el protocolo que hace transparente la red física creando una visión de red virtual. Es un protocolo de la capa de red no orientado a conexión que enruta paquetes (datagramas) a través de la red internet pero no garantiza que lleguen a su destino sin error, sin pérdida y sin duplicación.

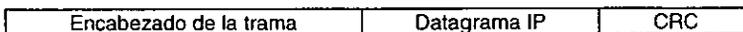
#### Datagrama IP

El datagrama IP es el paquete básico de transferencia en el protocolo IP. Está formado por un campo de encabezado que contiene información para IP y otro de datos que son relevantes solamente para los protocolos de las capas altas.



Datagrama IP

El datagrama IP está encapsulado en la trama de la red física, la cual usualmente tiene un tamaño máximo dependiendo del hardware utilizado, mejor conocido como MTU Maximum Transfer Rate. Para Ethernet, éste es típicamente de 1500 bytes, para Token Ring de 4464. En lugar de limitar la longitud del datagrama IP a algún tamaño máximo, IP puede fragmentar y reensamblar los datagramas. En particular, el estándar IP no impone un tamaño máximo, pero establece que todas las subredes deben manejar el datagrama de al menos 576 bytes.



Trama de la red física

Todos los fragmentos de un datagrama tienen un encabezado, básicamente copiado del datagrama original. Los fragmentos son tratados como datagramas IP normales mientras son transportados a su destino. Sin embargo, si uno de los fragmentos se pierde, el datagrama completo se considera perdido ya que IP no proporciona mecanismos de reconocimiento, de tal manera que los fragmentos restantes simplemente son descargados por el sitio destino.

### Formato del datagrama IP

El encabezado del datagrama IP tiene un máximo de 20 bytes; el esquema se muestra en la fig. 1.6

Versión	Long. de encabezado	Tipo de servicio	Longitud total del paquete
Identificación		Flag	Offset del fragmento
TTL	Protocolo	Checksum del encabezado	
Dirección IP fuente			
Dirección IP destino			
Opciones		Padding	
DATOS			

Fig. 1.6 Formato del Datagrama IP

En donde:

- Versión.- Indica la versión del protocolo IP.
- Longitud del encabezado.- Indica la longitud del encabezado en palabras de 32 bits. Este no incluye el campo de datos.
- Tipo de servicio.- El tipo de servicio (TOS) es la indicación de la calidad de servicio requerido para este datagrama IP, donde se tienen los siguientes parámetros:

0	2	3	4	5	6	7
precedencia	retardo	throughput	confiabilidad	costo	sin uso	

- Los tres primeros bits indican la procedencia del datagrama.
  - El campo de retardo le indica a un ruteador que si conoce a una red de menor retardo que otras, la seleccione para el envío de éste datagrama.
  - El campo throughput indica al ruteador que provea la ruta que maximice el número de datagramas por segundo.
  - El campo de confiabilidad le indica al ruteador que escoja una trayectoria que minimice la probabilidad de que el datagrama sea descartado.
  - El bit de costo indica al ruteador que seleccione la trayectoria con menor costo.
- Longitud Total.- Contiene la longitud total del datagrama, encabezado y datos, especificado en bytes.
  - Identificación.- Un número único asignado por el transmisor. Cuando el software IP del ruteador fragmenta el datagrama, copia este número en el campo de identificación de cada fragmento para ayudar al reensamble del datagrama fragmentado.
  - Banderas.- Existen varias banderas de control, donde: DF (Don't Fragment), MF (More Fragments)

DF = 0.- Permitir fragmentación  
DF = 1.- No permitir fragmentación  
MF = 0.- Último fragmento del datagrama  
MF = 1.- No es el último fragmento del datagrama

- Offset del fragmento.- Se usa con datagramas fragmentados para ayudar a reensamblar el datagrama. Su valor es el número de partes que están contenidas en los primeros fragmentos. En el primer fragmento éste valor siempre es 0.

- TTL (Time To Live - Tiempo de vida).- Especifica el tiempo (en segundos) que se le permite viajar al datagrama. Cada ruteador por donde éste pasa, le resta al valor actual el tiempo de procesamiento, establecido en un segundo, aunque en realidad un ruteador procesa un datagrama en menos de 1 segundo. Cuando éste valor llega a cero, se supone que el datagrama ha estado viajando en círculo y entonces se descarga. El valor inicial es colocado por el protocolo de más alto nivel el cual crea el datagrama.
- Protocolo.- El número de este campo indica el protocolo de la capa superior de la arquitectura TCP/IP, al cual deberán ser entregados los datos encapsulados en el datagrama. Algunos valores importantes son:

1	ICMP
6	TCP
17	UDP

- Checksum del Encabezado.- Es el checksum del encabezado solamente, sin incluir los datos. Si el checksum no coincide con el contenido, el datagrama se descarga.
- Dirección de origen IP.- Es la dirección IP de 32 bits del sitio que envía el datagrama.
- Dirección de destino IP.- Es la dirección IP de 32 bits del sitio de destino para este datagrama.
- Opciones.- El campo de opciones es variable en longitud y se usa para funciones de reporte de error y de depuración.
- Finalmente, el Pad es el colchón para ajustar el campo a los 32 bits.
- El campo de datos contenido en el datagrama pasa al protocolo de la capa superior como se ha especificado en el campo de protocolo.

### **1.5.2 Protocolo TCP**

Después de IP, el protocolo más usado de la familia TCP/IP es TCP. Opera en la capa de transporte y su función principal es establecer una conexión confiable para la transferencia de datos de una aplicación corriendo en una computadora, a otra aplicación corriendo en otra computadora remota. Responsable de hacer confiables los servicios proporcionados por IP, tiene los siguientes atributos:

- Orientado a conexión, ya que se encarga de establecer una conexión entre dos computadoras.
- Confiable ya que asegura la entrega de los datos a la aplicación destino en la secuencia correcta y sin error. Para ello el extremo receptor envía un acuse de recibo por cada secuencia de bytes recibida.
- Implementa control de flujo. Si el buffer de datos en el extremo receptor de la conexión comienza a saturarse, TCP le indica al extremo transmisor que reduzca la velocidad de transmisión.
- Implementa checksum no sólo en el encabezado sino en todo el segmento (encabezado y datos), de modo que permite al receptor detectar si ha ocurrido un error en la comunicación.
- Entrega datos como una secuencia de bytes al protocolo IP, el cual los encapsula en datagramas IP.
- Provee un servicio *full duplex*, mediante el cual maneja simultáneamente dos segmentos de datos, lo que significa que actúa al mismo tiempo como un transmisor y un receptor.

### Segmento TCP

El formato del segmento TCP se muestra en la fig. 1.7:

Puerto Fuente				Puerto destino				
Número de secuencia								
Número de ACK								
Long. del encabezado	Reserva do	U R G	A C K	P R H	S S T	S Y N	F I N	Tamaño de la ventana
Checksum				Apuntador de datos urgentes				
Opciones				Padding				
Area de datos								

Fig. 1.7 Segmento TCP

- Puerto fuente.- Este campo identifica a la aplicación en el transmisor que hace uso de TCP, puede tener valores de 0 a 65,535. Los valores de 0, 1023 y 1024 son reservados. Los valores en el rango de 1 a 1022 son llamados puertos bien conocidos (well-known ports) y son administrados por Internet. El número de puerto fuente y la

dirección IP fuente, se combinan para identificar en forma única cada conexión TCP. A esta combinación se le conoce como dirección de socket.

- Puerto destino.- Este campo identifica la aplicación en el extremo remoto con la cual se desea establecer la conexión. Tiene las mismas características del puerto fuente.
- No. de secuencia.- Este campo identifica el primer byte de datos de un segmento TCP.
- No. de ACK.- Este campo identifica el siguiente byte de datos que el transmisor espera recibir del módulo TCP remoto de la conexión.
- Longitud del encabezado.- Este campo especifica la longitud del encabezado del segmento TCP en palabras de 32 bits y permite al módulo TCP receptor calcular donde comienzan los datos. Cuando no hay opciones, la longitud del encabezado es de 20.
- Banderas.- Existen 6 banderas y tienen longitud de 1 bit, a continuación se describe el significado de cada una de ellas:

URG: Habilita al campo de Apuntador de Datos Urgentes,

ACK: Valida al campo No. de ACK.

PSH: Función de empuje.

RST: Indica al módulo destino que debe reinicializar la conexión porque se detectó un problema en la conexión.

SYN: Solicita la sincronización de los números de secuencia.

FIN: Indica el fin de la transmisión de datos.

- Tamaño de la ventana.- Este campo indica cuantos bytes de datos puede aceptar el sistema. Tamaños típicos de ventana son 4096 bytes, 8192 bytes y 16384 bytes.
- Checksum.- Es el resultado de la suma del encabezado y datos de TCP.
- Apuntador de datos urgentes.- Este campo contiene un apuntador al primer byte de datos urgentes en el área de datos de TCP. Sólo es válido si la bandera de URG es puesta a uno.
- Opciones.- Tiene el mismo significado que el campo de opciones del datagrama IP.

## Operación del protocolo TCP

La operación del protocolo TCP comprende las siguientes fases:

- Establecimiento de una conexión
- Transferencia de datos
- Terminación de conexión

### Establecimiento de una conexión

En un servicio orientado a conexión, el establecimiento de la misma comienza cuando el programa de aplicación que usa los servicios de protocolo TCP, le envía una función de connect, especificando la dirección del socket remoto. El establecimiento de la conexión se hace con un esquema de intercambio de los tres pasos siguientes:

1.- El módulo TCP cliente que requiere la conexión, envía un segmento al módulo TCP del servidor, que contiene lo siguiente:

- a) La bandera SYN es puesta a 1, para indicar al módulo TCP en el servidor, que un programa cliente desea establecer una conexión.
- b) En el campo de número de secuencia asigna un valor inicial (ISN), que es un número aleatorio que indica el comienzo de la numeración de la secuencia de datos.
- c) En el campo de opciones especifica el tamaño máximo del segmento (MSS:Maximum Segment Size).

2.- El módulo TCP del servidor acepta la solicitud para establecer una conexión enviando al módulo TCP del cliente, un segmento que especifica:

- a) La bandera SYN puesta a 1, para solicitar al módulo TCP del cliente, sincronización con el número de secuencia con el módulo TCP del servidor.
- b) En el campo de número de secuencia asigna su propio número de secuencia inicial (ISN).
- c) La bandera ACK es puesta a 1, para indicar al módulo TCP del cliente que el campo número de ACK es válido y que contiene el siguiente número de secuencia que el

módulo TCP del servidor espera recibir del módulo TCP del cliente. El valor, es el número de secuencia indicado por el módulo TCP del cliente, mas 1. Con ello el módulo TCP del servidor acepta la petición para establecer una conexión.

d) En el campo de opciones, se especifica el tamaño máximo del segmento e indica que el módulo TCP del servidor no desea recibir segmentos TCP más grandes que el valor indicado por MSS. Para evitar que el módulo IP haga fragmentación, se pone este campo a un valor de 1024 bytes, pero el valor por omisión es 536 bytes.

3.- El módulo TCP del cliente acepta la respuesta del módulo TCP del servidor enviándole un acuse de recibo, donde acepta la petición del módulo TCP del servidor para identificar el número de secuencia inicial del módulo TCP del servidor. Para ello le envía un segmento que contiene:

a) La bandera ACK puesta a uno para indicar que el campo de número de ACK contiene un número válido.

b) En el campo número de ACK pone el siguiente número de secuencia que el módulo TCP del cliente espera recibir del módulo TCP del servidor; éste es el número de secuencia indicado en el mensaje del servidor incrementado por 1.

En este mensaje no se pone la bandera SYN puesto que ambos lados ya han sincronizado uno con otro su número de secuencia inicial.

### **Transferencia de datos**

Una vez establecida la conexión, el cliente y el servidor pueden comenzar la transferencia de datos, numerando cada byte que transfieren a partir del número de secuencia inicial (ISN). El tamaño del número de secuencia es limitado a 32 bits, por eso puede ir de 0 a  $2^{32} - 1$ . Cuando el valor llega al límite superior se regresa al número 0.

Para asegurar que el transmisor no sature al receptor con más datos de los que puede aceptar, TCP usa técnicas de control de flujo y para garantizar la confiabilidad en la entrega de la secuencia de bytes, usa técnicas de control de error. Ambas técnicas se describen brevemente a continuación:

### Control de error

Cuando el módulo TCP destino recibe del extremo remoto una secuencia de bytes, le envía un acuse de recibo; sin embargo, el módulo TCP no espera hasta recibir el acuse de recibo para enviar el siguiente mensaje de datos, sino que utilizando la técnica de ventanas deslizantes (sliding windows), puede enviar varios mensajes antes de esperar un acuse de recibo.

### Ventanas deslizantes

La técnica de ventanas deslizantes permite a un módulo TCP enviar varios segmentos sin esperar por un acuse de recibo para cada segmento individual. Si varios segmentos son recibidos en un nodo antes que un acuse de recibo esté listo para enviarse, es posible transmitir un acuse de recibo sólo para el último segmento recibido, eliminando así la necesidad de transmitir acuses de recibo para cada segmento, lo cual permite utilizar en forma más eficiente el ancho de banda de la red.

### Ventana del módulo TCP del transmisor

El transmisor de datos mantiene un *buffer* de transmisión que registra dos cosas:

1. Cuantos datos han sido enviados y reconocidos
2. El tamaño de la ventana de recepción del módulo TCP en el otro extremo.

El *buffer* de transmisión se extiende desde el primer byte NACK hasta el extremo derecho de la ventana de recepción actual. En este punto el campo número de ACK del encabezado del segmento TCP desarrolla dos funciones importantes:

- Acuse de recibo
- Control de flujo

El número de ACK es el número de secuencia del último byte recibido del extremo remoto e indica que todos los bytes recibidos hasta el indicado no han tenido error.

El campo de ventana del encabezado, contiene el número de bytes que el extremo remoto es capaz de aceptar. La ventana indica al transmisor que puede seguir enviando segmentos hasta en tanto el número total de bytes que envíe sea más pequeño que el

tamaño de la ventana, es decir la ventana indica al transmisor, que puede seguir transmitiendo segmentos mientras el número total de bytes que envíe, sea más pequeño que el tamaño de la ventana.

#### Control de flujo

Los números de secuencia empleados en los segmentos TCP son la base de la técnica usada para el control de flujo. Con la técnica de control de flujo se evita que el módulo TCP transmisor remoto envíe más datos de los que el módulo receptor puede aceptar. El control de flujo se basa en la técnica de ventanas deslizantes, mediante la cual, el receptor controla el flujo de bytes del transmisor cambiando el tamaño de la ventana. Una ventana 0, le indica al transmisor que cese de transmitir hasta que reciba un valor de ventana diferente más grande que cero.

El encabezado de cada paquete TCP contiene el número de ACK y un campo de ventana. Estos dos números limitan el margen de bytes que el sistema está dispuesto a recibir.

#### Terminación de la conexión

Para terminar una conexión se usa el intercambio de los dos mensajes siguientes:

- 1.- El extremo TCP que inicia el cierre de la conexión, lo hace enviando un mensaje con la bandera FIN puesta.
- 2.- El extremo de la conexión contesta con un mensaje de ACK.

Con estos pasos sólo se termina la conexión en un sentido, pero la conexión en el otro queda activa. Para terminarla, el otro módulo TCP debe enviar también un mensaje con la bandera FIN puesta y el otro responder con un mensaje de ACK.

#### 1.5.3 Protocolo UDP

Es el otro protocolo que junto con TCP opera en la capa de transporte. Es un protocolo no orientado a conexión, no confiable y que usa datagramas para entrega de datos. Cabe mencionar que un datagrama IP y un datagrama UDP difieren en contenido y

en formato, además IP y UDP difieren en que el primero entrega datos a un solo host y el segundo entrega datos a un programa de aplicación o a múltiples programas de aplicación corriendo en ese host.

El cliente se comunica con el servidor usando TCP o UDP de la capa de transporte. TCP encapsula los datos de la aplicación en segmentos y emplea un servicio orientado a conexión, en tanto UDP los encapsula en datagramas y utiliza un servicio de entrega de datos no orientado a conexión. Ambos usan puertos para distinguir una aplicación de otra. UDP usa los puertos en forma diferente a TCP. En TCP antes de transferir datos se establece una conexión entre las aplicaciones. UDP no establece una conexión entre el transmisor y el receptor antes de transferir datos, sino que simplemente los pone en el puerto al que van destinados, pero no notifica al protocolo de aplicación de ese puerto que ha recibido datos.

### Datagrama UDP

El encabezado de un datagrama UDP es de 8 bytes de longitud y se muestra en la fig. 1.8:

Puerto fuente	Puerto destino
Longitud del datagrama UDP	Checksum UDP
Datos UDP	

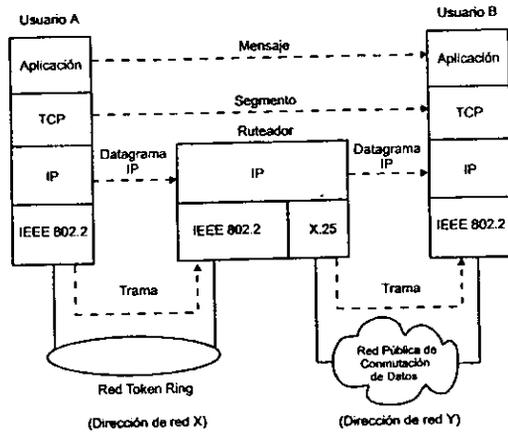
**Fig. 1.8** Datagrama UDP

**Puerto fuente.**- Es el puerto asignado al proceso cliente que envía el datagrama.

**Puerto destino.**- Es el puerto al cual va dirigido el datagrama.

**Longitud del datagrama UDP.**- Indica la longitud del datagrama e incluye el encabezado y los datos de la aplicación en bytes.

**Checksum.**- Se calcula a la suma de grupos de 16 bits y sirve al receptor para detectar si ha habido un error en la comunicación.



**Fig. 1.9** Estructura de una comunicación con TCP/IP

La fig. 1.9 describe el proceso de comunicación a través de dos redes físicas. Al igual que en el modelo de referencia OSI, en el nodo intermedio, en éste caso un router, sólo se involucran las capas bajas del protocolo TCP/IP.

## **Capítulo II**

### **REDES DE COMPUTADORAS**

#### **II.1 Señalización y Conmutación**

##### **II.1.1 Señalización**

La señalización se entiende como el intercambio de información entre dos entidades para el establecimiento y supervisión de un enlace. La señalización en telefonía puede ser del tipo CAS (Channel Associated Signaling) cuando se maneja en el mismo canal de voz o en un canal asociado a éste, o del tipo CCS (Common Channel Signaling) si la señalización viaja en un canal completamente separado de los canales de voz y es común para el manejo de la señalización de un gran número de canales de voz.

##### **Sistema de Señalización Número 7 (SS7)**

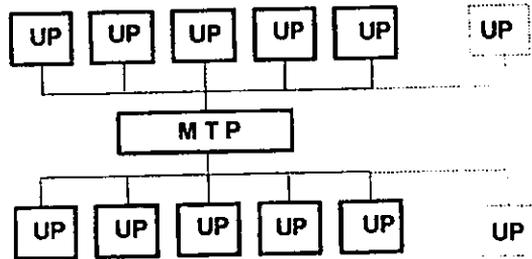
En 1980 la CCITT desarrolló un sistema de señalización por canal común CCITT # 7 el cual fue rápidamente adoptado como el estándar internacional. Ha tenido revisiones en 1984, 1988 y 1992. Conocido ahora como SS7 (Signaling System Number 7), es el mecanismo que provee el control interno y la inteligencia de la red en ISDN, tecnología para la que fue específicamente diseñado.

El alcance de SS7 es inmenso, debido a que debe cubrir todos los aspectos de señalización de control para redes digitales complejas, incluyendo el ruteo confiable, la entrega de mensajes de control y el contenido orientado a aplicación de esos mensajes.

##### **Estructura Básica**

El sistema de señalización SS7 esta formado básicamente por dos partes: la de usuario UP (User Part) y la de transferencia del mensaje MTP (Message Transfer Part). Las UP's generan y analizan los mensajes de señalización y utilizan al MTP como una función de transporte para llevar la información a otra UP de la misma clase.

Existen diversos ejemplos de UP: Para los servicios básicos de telefonía, se tiene el TUP (Telephony User Part); para el servicio de conmutación de circuitos de datos, existe el DUP (Data User Part); para proporcionar los servicios de voz, datos y vídeo combinados, el ISUP (ISDN User Part); para los servicios de operación y mantenimiento, el OMAP (Operation and Maintenance Application Part); y finalmente, para el caso de telefonía móvil, el MTUP (Mobile Telephony User Part).



**Fig. 2.1 Estructura básica de SS7**

El MTP es responsable de las siguientes funciones:

- Transferencia sin errores
- Transferencia en la secuencia correcta
- Evitar pérdidas o duplicación de información

### **Unidades de señalización**

El SS7 utiliza tramas para manejar y transmitir los mensajes de señalización entre un UP y otro, a las cuales se les conoce como unidades de señalización. Existen tres tipos de unidades:

MSU (Message Signal Unit), unidad de mensaje de señalización

F	CRC	SIF	SIO		LI	FIB	FSN	BIB	BSN	F
---	-----	-----	-----	--	----	-----	-----	-----	-----	---

LSSU (Link Status Signal Unit), unidad del estado del enlace de señalización

F	CRC	STATUS		LI	FIB	FSN	BIB	BSB	F
---	-----	--------	--	----	-----	-----	-----	-----	---

FISU (Fill in Signal Unit),

F	CRC		LI	FIB	FSN	BIB	BSN	F
---	-----	--	----	-----	-----	-----	-----	---

Toda la información de señalización asociada con configuración de llamada, bloqueo y administración de red SS7 está contenida en la MSU. La LSSU se utiliza para la administración de los enlaces de señalización y la FISU es una unidad que se utiliza para ocupar el enlace cuando no hay unidades MSU's o LSSU's que enviar y facilita el constante monitoreo de la calidad de los enlaces en la ausencia de tráfico de señalización.

Los Campos son:

F: Bandera

BSN: Backward Sequence Number

FSN: Forward Sequence Number

FIB y BIB: Forward y Backward Indicator Bit

LI: Length Indicator

SIO: Service Information Octet

SIF: Signaling Information Field

CRC: Cyclic Redundancy Check

## Redes de señalización

Las redes de señalización están formadas por tres entidades, los puntos de señalización, SP (Signaling Point), puntos de transferencia de señalización, STP (Signaling Transfer Point) y los enlaces de señalización, SL (Signaling Link). Un SP es cualquier punto en la red de señalización que sea capaz de manejar mensajes de control SS7. Un STP es un punto de señalización que es capaz de rutear mensajes de control, es decir, un mensaje recibido en un enlace de señalización es transferido a otro enlace. Finalmente, un SL es un enlace de datos que conecta puntos de señalización.

## Mensajes de señalización ISUP

La ISUP se usa para la señalización entre nodos dentro de ISDN. Es capaz de procesar información específica, la cual es más compleja que la señalización en telefonía. Un TUP en una central se puede comunicar con un TUP en otra central, pero un TUP y un ISUP no se pueden comunicar. Esto obliga a que todos los nodos ISDN con conexiones directas a la red telefónica necesiten tanto TUP como ISUP.

Algunos de los mensajes de señalización ISUP se listan en la tabla 2.1 especificando los nombres y la referencia a los cuadros de la recomendación Q.763 del "libro azul" de la CCITT.

<i>Tipo de Mensaje</i>	<i>Cuadro (Q.763)</i>
Dirección completa	5
Respuesta	6
Bloqueo	23
Acuse de bloqueo	23
Conexión	11
Información	14
Dirección inicial	16
Sobrecarga	23
Liberación	17

Tabla 2.1 Mensajes de señalización ISUP

## SCCP

La parte de control de la conexión de señalización SCCP (Signaling Connection Control Part), fue añadida como un módulo más en la versión de 1984 de SS7. Proporciona funciones adicionales a las necesidades del MTP para soportar nuevas aplicaciones. La combinación MTP-SCCP se conoce como parte de servicio de red NSP (Network Service Part). El propósito es sumar una capacidad de enrutamiento para la parte superior de los servicios de MTP que permitan al NSP ofrecer un servicio de transmisión extremo a extremo entre los puntos finales de señalización. Juntos son equivalentes a las funciones de las capas 1, 2 y 3 del modelo OSI.

El servicio extremo a extremo proporcionado por el NSP se puede asociar con una conexión de usuario sobre la red, pero normalmente se usa para la transferencia de información de señalización de relevancia solamente para los puntos extremos SP.

### Servicios de SCCP

SCCP provee servicios mejorados de transferencia de mensajes, dos orientados a conexión y dos no orientados a conexión. Cada servicio está definido como una clase.

**Clase 0:** No orientada a conexión. En esta clase, el usuario provee las unidades de datos del servicio de red NSDU (Network Service Data Unit), para ser entregadas a través del SCCP a un usuario en otro nodo. Las NSDU's son transportadas independientemente unas de otras y se pueden enviar fuera de secuencia.

**Clase 1:** No orientada a conexión. Las características de la clase 0 se complementan por una característica adicional que permite a las capas altas del SCCP enviar un flujo de NSDU en secuencia.

**Clase 2:** Orientada a conexión. La transferencia bidireccional de NSDU entre los usuarios SCCP se hace estableciendo una conexión de señalización permanente a temporal. Los mensajes pertenecientes a una conexión de señalización dada contendrán el mismo valor del campo SLS para asegurar la secuenciación de la misma manera que la clase 1.

Clase 3: Clase de control de flujo orientada a conexión. El control de flujo significa que la tasa de flujo de datos se puede controlar tanto en las capas adyacentes como entre dos nodos. Las funciones de control de flujo permiten a una entidad receptora limitar el flujo de datos desde la entidad transmisora. También incluye una capacidad adicional de detención de pérdida de mensajes o pérdida de secuencia. En tal circunstancia la conexión de señalización se restablece y el SCCP proporciona una notificación a las capas superiores.

## II.1.2 Conmutación

Es la técnica que se utiliza para establecer la conexión entre dos entidades durante el tiempo necesario para la transferencia de información. Existen tres tipos de dicha técnica: conmutación de circuitos, conmutación de mensajes y conmutación de paquetes. A continuación se describen las principales características de cada una de ellas.

### Conmutación de circuitos

Este tipo de técnica consiste en establecer la conexión entre dos entidades permitiendo la utilización de la conexión completa hasta su liberación, es decir, ninguna otra conexión podrá ocupar estos recursos. En todas las redes telefónicas analógicas se utiliza ésta técnica. En la fig. 2.2 se muestra un ejemplo y únicamente se representan enlaces físicos con el fin de simplificarla pero también intervienen enlaces de microondas a través de los cuales se pueden multiplexar miles de conexiones.

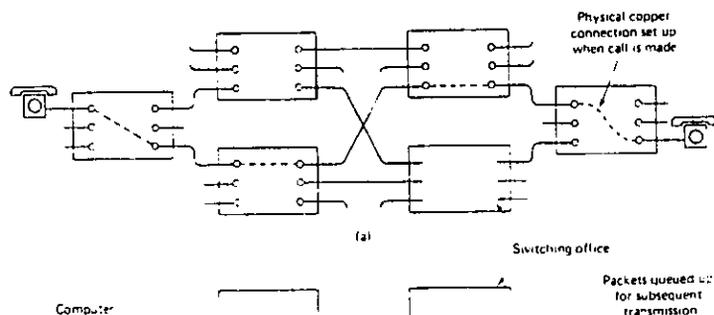


Fig. 2.2 Conmutación de circuitos

## Conmutación de mensajes

En éste tipo de conmutación no se utiliza un enlace físico dedicado entre el receptor y transmisor. Cuando el transmisor tiene un mensaje que transmitir, lo envía añadiéndole un encabezado que contiene la dirección destino. Después se establece una ruta a través de la cual se transmitirá el mensaje completo, almacenándose en cada uno de los nodos, donde se examina para detectar posibles errores y se retransmite. Debido al proceso de almacenamiento de los mensajes en cada nodo, se produce un retardo global considerable y el aumento del tráfico en la red contribuye a elevar éste retardo. Una red que utiliza éste tipo de conmutación se conoce como store-and-forward.

## Conmutación de paquetes

La técnica de conmutación de paquetes se basa en el multiplexaje estadístico e implica la combinación de paquetes constituidos por porciones de longitud fija. Los mensajes se subdividen en paquetes a fin de evitar que mensajes largos puedan ocupar la línea de comunicación originando retrasos importantes en la red. Los paquetes pueden ser transferidos por la misma ruta de nodo a nodo o por otra distinta hasta su destino, donde se deben reensamblar para formar el mensaje original. La principal característica de la conmutación de paquetes es la forma en la cual son compartidos los enlaces de transmisión dependiendo de las necesidades de dichos enlaces.

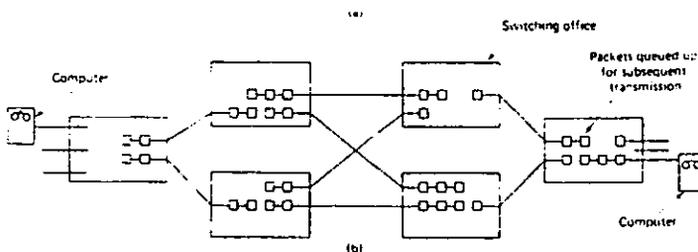
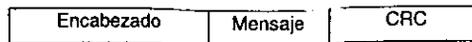


Fig. 2.3 Conmutación de paquetes

## Formato de paquetes

El formato de los paquetes en una red de conmutación de paquetes puede variar significativamente de una red a otra. Algunos formatos incluyen numerosos campos para información de control mientras que otros sistemas se utilizan paquetes especiales para transmitir este tipo de información. En general, es más común que la información de control asociada a un mensaje o enlace en particular este incluida en el encabezado de un paquete de mensaje.



**Fig. 2.4** Formato de paquete

Como se indica en la fig. 2.4, un paquete contiene 3 campos principales, el encabezado, el mensaje y el CRC (Cyclic Redundancy Check). Algunos paquetes pueden no contener un campo de mensaje si son usados estrictamente para propósitos de control. Un encabezado generalmente contiene numerosos subcampos además del campo de dirección, como el número de secuencia para reensamblar los mensajes en el nodo destino.

## II.2 Redes de Area Local (LAN)

El origen de las redes de área local se puede considerar en 1974 cuando IBM introdujo una serie de terminales diseñadas para utilizarse en aplicaciones de procesamiento de transacciones de bancos y tiendas. Lo que tenían de especial esas terminales era la manera como se encontraban conectadas entre sí, con un cable que formaba un enlace para proveer de comunicaciones a una región geográfica bien delimitada. Desafortunadamente, la incompatibilidad entre diferentes equipos y enlaces evitó que se popularizara esta forma de interconexión. Sin embargo, la economía que representa el compartir el medio de transmisión y la habilidad de proveer acceso a un recurso centralizado, son los factores clave que indujeron a IBM y otros fabricantes a investigar sobre el cómo comunicar diferentes equipos en una región determinada. Esto llevó al desarrollo de diferentes topologías de conexión, tales como: bus, estrella, anillo, malla y árbol.

En 1977, una compañía llamada Datapoint Corporation comenzó a vender su *Attached Resource Computer Network (ARCNET)*, o Red de Computadoras de Recursos Agregados, la cual muchas personas consideran como el primer producto en el mercado de redes locales de computadoras. A partir de entonces, cientos de fabricantes han desarrollado este tipo de productos, y el número de equipos conectados a este tipo de redes ha crecido exponencialmente, hasta llegar a últimas fechas a decenas de millones.

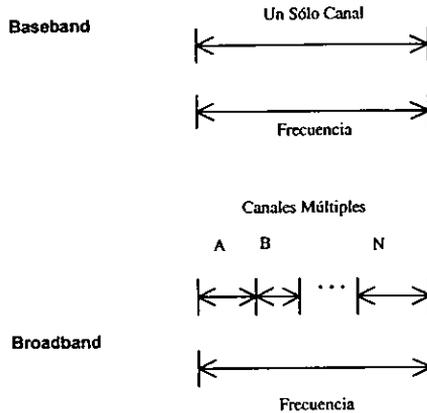
Como su nombre lo indica, una LAN (Local Area Network) es una red de comunicaciones que cubre un área local de relativamente pequeñas proporciones. Dicha área puede ir desde un mismo cuarto en un departamento, hasta los diferentes edificios dentro de un campus universitario.

Independientemente del área de cobertura de la red, el principal factor limitante de una LAN es la longitud entre dispositivos del medio de transmisión físico de la red, y la longitud total de la misma. Estas restricciones son impuestas por factores físicos de caída de señal y de tiempos de respuesta.

### **II.2.1 Métodos de Señalización de LAN**

El método de señalización que se utiliza en una red de área local involucra tanto la codificación de datos para la transmisión así como la utilización del espectro de frecuencia del medio, aunque de hecho se refiere más a la utilización de ese espectro.

Dos métodos de señalización que se utilizan en las LAN son la *baseband* y la *broadband*. En la señalización de *broadband*, el total del ancho de banda del medio se subdivide por frecuencia para formar uno o más subcanales, cada uno de los cuales permite la transferencia de datos independiente de la transferencia en otro canal. En la señalización de *baseband* sólo se puede transmitir una señal por el medio en cualquier momento dado. En la fig. 2.5 se muestra la diferencia de uso del canal.



**Fig. 2.5 Métodos de Señalización**

Debe notarse que, por ejemplo, aunque un sistema de alambrado de par trenzado puede utilizarse para transmitir voz y datos, la transmisión en sí es de *baseband* puesto que normalmente sólo un canal se utiliza para los datos. En cambio, un sistema en *broadband* se puede diseñar para que transporte voz y varios subcanales de datos, así como fax y transmisión de vídeo.

### **II.3 Redes de Area Metropolitana (MAN)**

Las redes locales de computadoras operan a altas velocidades de transmisión con protocolos sencillos, mientras que las redes de área ancha operan a velocidades mucho más bajas con protocolos más complejos. Por un lado, las LAN se utilizan para conectar equipos de una misma organización a través de distancias pequeñas, mientras que las WAN (Wide Area Networks) proveen comunicaciones de larga distancia entre puntos muy separados entre sí, por ejemplo a lo largo de un país o continente. Por estas circunstancias surge la necesidad de una red que opere en distancias de una ciudad más o menos modesta (de alrededor de 25 km. de radio), a velocidades similares a las de una LAN y con un protocolo medianamente complejo. La tecnología MAN tiene las mejores características de ambos enfoques.

El esfuerzo de creación de las redes de área metropolitana comenzó en 1982, y sus metas funcionales originales eran proveer interconectividad para LAN, transferencia

masiva de datos, voz digitalizada y vídeo, así como tráfico convencional entre terminales. Cuando se tienen diversos equipos de comunicaciones distribuidos a través de una ciudad, lo más eficiente es conectarlos entre sí en forma de redes, y después conectar estas redes por medio de otra red de alta velocidad, y es aquí donde entran en funcionamiento las MANs. Por lo tanto, una MAN es una red de alta velocidad que interconecta un cierto número de LAN, permitiendo compartir recursos e información en una comunidad metropolitana.

### **II.3.1 Características de las MAN**

Una MAN se comporta como una LAN en el sentido de que los usuarios no se dan cuenta si se están comunicando a través de un cuarto o a través de una ciudad. Aunque el concepto de la MAN se modela de acuerdo a los principios de las LAN, existen varias diferencias entre éstos tipos de redes, siendo las principales las siguientes:

- **Distancia:** Mientras que una LAN opera dentro de unos cuantos kilómetros, una MAN opera sobre una ciudad y sus suburbios. La IEEE recomienda una distancia óptima de 50 Km.
- **Backbone:** Se necesita una red central (backbone) para conectar las LAN entre sí, para facilitar la administración de la MAN
- **Servicio:** Es muy común que las MAN transporten voz digitalizada, no datos de computadora, por lo que es deseable que este tipo de redes se optimice para este fin, además de tener capacidades para transmisión de vídeo y datos. Esto demanda requerimientos muy estrictos, impuestos por la voz.
- **Administración centralizada:** Una MAN requiere una administración central para la instalación, operación y mantenimiento de la red, así como el servicio de facturación a usuarios. Una MAN se comparte entre varias organizaciones, en lugar de pertenecer a una sola, como las LAN. Esto trae como consecuencia asuntos relacionados con la seguridad y privacidad de la información, además de la necesidad de una operación centralizada y mayor control de tráfico.

### II.3.2 Topologías

Así como en el caso de las LAN, existen algunas topologías básicas en las redes de área metropolitana. Algunas de ellas son extensiones naturales de las redes de área local, mientras que otras siguen esquemas muy diferentes. A continuación se describen algunas de ellas.

#### Topología de Arbol

Bajo este esquema, las estaciones se particionan en subgrupos, los cuales están enlazados a la raíz o cabeza del árbol por medio de concentradores y subconcentradores, tal como se muestra en la fig. 2.6. Esta topología puede utilizar como protocolos de acceso una variante del CSMA/CD o bien un método de control de acceso conocido como poleo de grupo, en el cual la cabeza o raíz interroga a cada subgrupo de una manera cíclica.

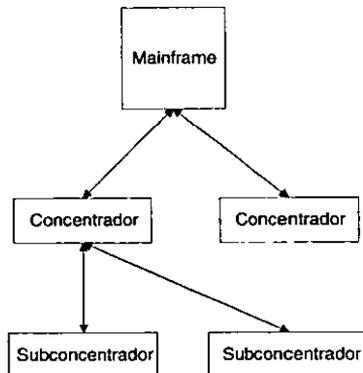


Fig. 2.6 Topología de Arbol

Una de las mayores ventajas de la topología de árbol es que utiliza el mínimo número de enlaces para interconectar los puntos de la red. Sin embargo, tiene la desventaja aún mayor de su falta de confiabilidad, ya que si falla la raíz del árbol se pierde toda la red. Del mismo modo, si llega a fallar un concentrador o un subconcentrador, se perderá la comunicación con todos los subgrupos correspondientes.

## Topología Toroidal

La topología toroidal tiene múltiples rutas de acceso entre los nodos fuente y los destino, lo que incrementa de gran manera la confiabilidad de la red y ayuda a obtener una carga de tráfico balanceada. El precio que se paga es el de algoritmos de ruteo más complejos y mayor tiempo de proceso en cada nodo.

Una red toroidal es una malla o matriz rectangular, donde los nodos opuestos de los extremos derecho e izquierdo se conectan entre si y los nodos en los extremos superior e inferior también se encuentran conectados entre si, de manera similar a como se enrolla una pieza rectangular de material para formar un toroide. Las principales características de esta topología se mencionan a continuación:

- Son homogéneas, carecen de fronteras o límites, y tienen geometría cartesiana
- Son isotrópicas, es decir, cada nodo tiene un conjunto similar de conexiones hacia sus vecinos
- Los algoritmos de direccionamiento y ruteo son muy sencillos en esta configuración.

En la fig. 2.7 se muestra una topología de este tipo, en donde cada enlace es unidireccional, y los enlaces adyacentes, tanto en los renglones como en las columnas, transmiten paquetes en direcciones opuestas.

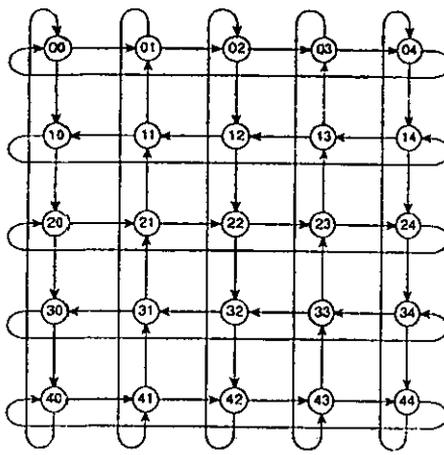


Fig. 2.7 Topología toroidal

Una de las principales ventajas de la topología toroidal es su tolerancia a fallas, ya que tiene al menos una ruta redundante entre cualquier par de nodos, lo cual sirve para rodear al componente de la red que haya fallado, ya sea enlace o nodo. Otra ventaja es que tiene el mismo número de enlaces por nodo y un número máximo de concentradores muy bajo, lo cual hace el ruteo muy sencillo. También es posible agregar nodos adicionales y crear jerarquías. Una desventaja es que requieren nodos muy complejos con capacidad de *store-and-forward*.

## **MAN Basadas en LAN**

La interconexión de las LAN que forman este tipo de redes, se realiza ya sea directamente o por medio de un *backbone*. La conexión directa se lleva a cabo por medio de un puente o de un *gateway*. Dos LAN homogéneas se conectan por medio de un puente que lleva a cabo las funciones de ruteo y control de flujo. Si las redes son heterogéneas, se utiliza entonces un *gateway*. En la fig. 2.8 se muestra un ejemplo típico de interconexión directa de tres redes bus y dos redes de anillo

La interconexión por *backbone* se puede hacer bajo dos esquemas diferentes: por medio de una red conmutada o por una red de difusión (*broadcast*). Esta última es una red en la cual todas las estaciones comparten un medio de transmisión común, y los datos que se transmiten por una estación se reciben por todas las demás. En la fig. 2.9 se ilustran dos redes, una con un *backbone* tipo anillo y la otra con *backbone* tipo bus.

Cuando se tiene una cantidad más o menos alta de LAN interconectadas, es mejor utilizar un conmutador central. Una red conmutada consiste de un sistema interconectado de nodos en el cual se transfieren los datos de origen a destino ruteándose de nodo a nodo. Como este tipo de red utiliza protocolos diferentes a los de las LAN, todas las conexiones hacia el backbone conmutado se realizan por medio de un *gateway*.

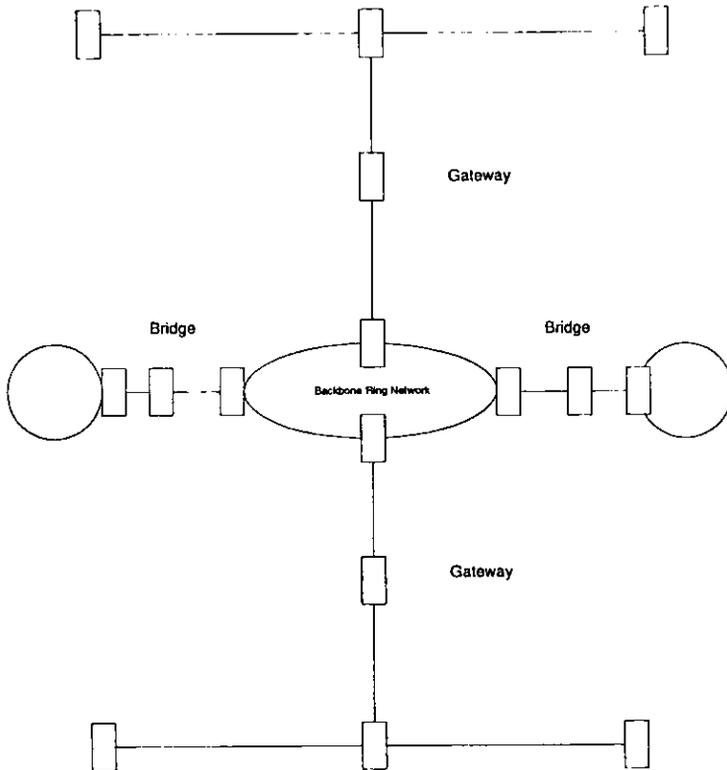
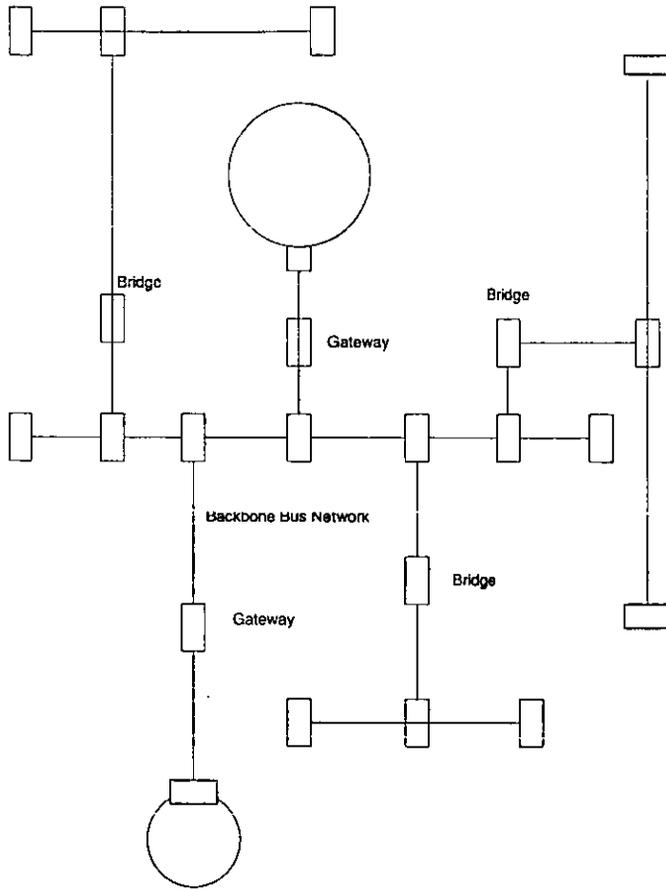
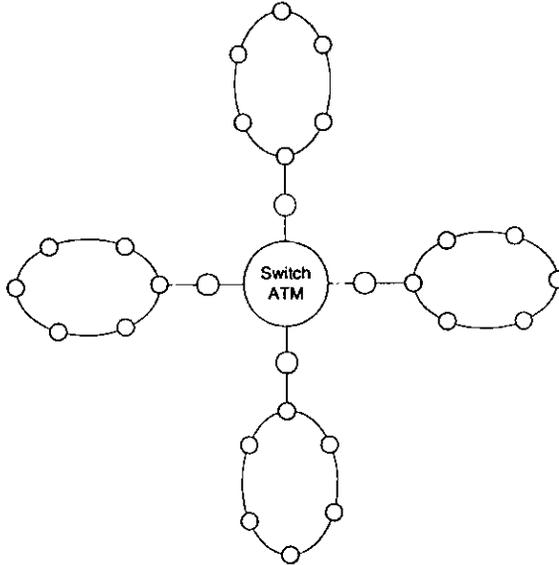


Fig. 2.9 (a) MAN con un Backbone Tipo Anillo



**Fig. 2.9 (b) MAN con un backbone Tipo Bus**



**Fig. 2.10** Múltiples LAN Interconectadas por un Switch ATM.

Se puede conectar un número casi ilimitado de LAN si se utiliza un switch ATM, como se muestra en la figura 2.10. Este tipo de switches permite que la MAN pueda ofrecer servicios tales como videotelefonía, debido a la alta capacidad de transferencia.

#### **II.4 Redes de Area Amplia (WAN)**

Se puede considerar que la evolución de las redes de área amplia comenzó a mediados de los 50's, junto con la aparición de la primera generación de computadoras. Por el precio y tamaño de estos equipos, las grandes compañías tenían un centro de procesamiento de datos, hacia el cual se transmitía toda la información desde las localidades remotas, para que fuera procesada. En la fig. 2.11 se muestra de manera esquemática una terminal en una localidad remota, la línea de transmisión, los módems y el centro de datos. Puesto que la línea de transmisión conectaba a una terminal localizada en área geográfica con una computadora en un lugar diferente, esta figura también representa uno de los primeros tipos de redes de comunicación de área amplia.

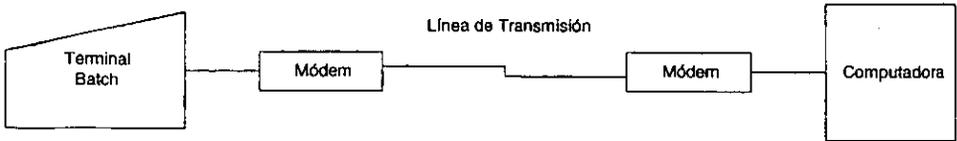


Fig. 2.11 Transmisiones Batch Remotas

El siguiente paso evolutivo en las WAN se muestra en el esquema de la fig. 2.12. Se han incorporado los controladores de comunicaciones y unidades lógicas de control. En términos generales, el controlador de comunicaciones transmite un mensaje a la unidad de control, la cual examina la dirección de la terminal y retransmite el mensaje a la terminal adecuada. Existen unidades de control locales y remotas, siendo la principal diferencia entre ellas la manera como se conectan al *mainframe* y el uso de equipo intermedio.

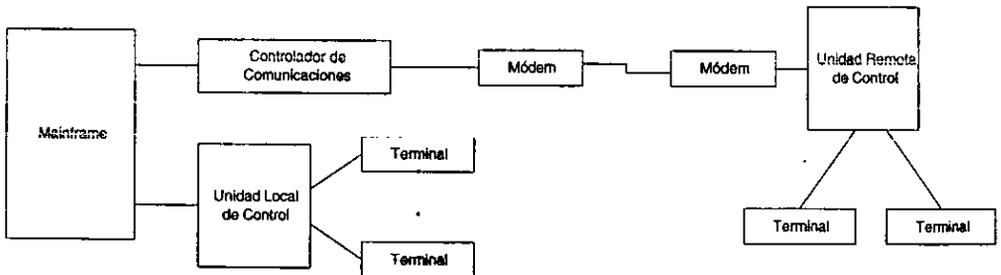


Fig. 2.12 Relación entre los Diferentes Dispositivos de Información

Conforme crecieron las necesidades de las organizaciones de agregar terminales remotas para sus *mainframes*, el costo para proveer las comunicaciones necesarias también creció. Esto ocasionó que se desarrollaran productos que permitieran compartir líneas de transmisión, conocidos como multiplexores y concentradores. Aunque la mayoría de las organizaciones operaban redes separadas para voz y datos, a mediados de los 80's comenzaron a estar disponibles a nivel comercial circuitos de alta capacidad conocidos como T1 en Estados Unidos y E1 en Europa y Latinoamérica. A través del desarrollo de estos multiplexores, se pudo integrar el envío de voz, datos y vídeo a través

de una sola línea. Ya que la interconexión entre oficinas corporativas normalmente cubre una distancia más allá de los límites de una ciudad, la red resultante se conoce como una red de área amplia.

A continuación se describe una WAN que cubre casi todo el territorio de México, para una compañía dada. En este ejemplo, las oficinas regionales en Tijuana y Monterrey están conectadas con las oficinas corporativas en el Distrito Federal por medio de multiplexores y líneas de transmisión E1 que operan a 2.048 Mbps. Suponiendo que cada multiplexor E1 es capaz de soportar la conexión directa de un PBX (Private Branch Exchange), entonces cada circuito E1 puede transportar voz y datos. Estos tres circuitos E1 se pueden considerar como el *backbone* de la red corporativa.

Supongamos ahora que además de los tres sitios antes mencionados, la corporación del ejemplo también tiene tres oficinas más pequeñas localizadas en Guadalajara, Veracruz y Querétaro. Si estas localidades únicamente requieren terminales de datos, un posible mecanismo para proveer el soporte de red es utilizando *trail circuits*. Estos circuitos se pueden usar para conectar un multiplexor estadístico por división de tiempo (STDM) en cada oficina para conectar a cada grupo de terminales al multiplexor E1 más próximo. Este multiplexor entonces se configura para rutear tráfico de datos a través del *backbone* corporativo.

## Capítulo III

### TECNICAS DE TRANSMISION EN REDES DE COMPUTADORAS

#### III.1 X.25

En 1974, la CCITT (Comité Consultivo Internacional de Telégrafo y Teléfono, ahora conocida como la ITU) emitió el primer esquema de X.25 (conocido como el 'Libro Gris'). Desde entonces, X.25 se ha expandido para incluir más opciones, servicios y facilidades.

Entre los mecanismos de control que deben de existir entre una estación de usuario y la red de paquetes, quizá el más importante sea el de *control de flujo*, que consiste en limitar la cantidad de tráfico que se genera por las estaciones, para prevenir el congestionamiento de la red, así como regular el tráfico que las estaciones reciben desde la red. También es necesario tener procedimientos de control de errores para asegurar que todo el tráfico sea recibido correctamente. X.25 provee estas funciones de control de flujo y errores.

X.25 define los procedimientos para el intercambio de datos entre las estaciones de usuario (en adelante referidas como DTEs, Data Terminal Equipment, por consistencia con la especificación) y un nodo de red de paquetes (DCE, Data Communications Equipment), el cual se utiliza para establecer la conexión entre dos DTEs finales. Estos procedimientos incluyen funciones tales como identificar paquetes de computadoras y terminales específicas (a través de los llamados *números de canales lógicos* o LCN por sus siglas en inglés), acuses de recibo y rechazo de paquetes. Sin embargo, es pertinente mencionar el hecho de que X.25 no posee algoritmos de ruteo de paquetes, tarea que es delegada a implementaciones particulares.

También se debe enfatizar que, a pesar de que dos interfaces DTE/DCE en los extremos de una red son independientes una de otra en la manera como X.25 define el diálogo respectivo con los nodos intermedios, X.25 sí puede utilizarse para comunicaciones de extremo a extremo, pues el tráfico seleccionado es entregado a la red

para que sea ruteado. Es por esto que la recomendación es *asimétrica*: sólo se define un lado de la interfaz de red (DTE/DCE).

Para evitar confusiones con respecto a la ausencia de algoritmos de ruteo, se presenta la fig. 3.1, que muestra cómo funciona X.25 en la capa de red (capa 3) para llevar a cabo esta actividad. El tráfico se transmite desde el DTE A a un nodo intermedio, que puede ser el nodo de entrada del usuario a la red (en X.25, el DCE). En este nodo, la capa física (1), la capa de liga de datos (2) y la de red (3) son invocadas para atender al usuario A. En esta ilustración, el usuario se identifica a sí mismo ante la red con el número de canal lógico (LCN) 11. A continuación, los datos se entregan al software de ruteo, que provee las funciones de conmutación de paquetes. Se regresan los datos a X.25 y a las capas inferiores para después transmitirse fuera del nodo intermedio (que puede ser el nodo de red [DCE] del usuario B) y se entrega al DTE B. El nodo de red asigna el LCN 16 para su sesión con el DTE B.

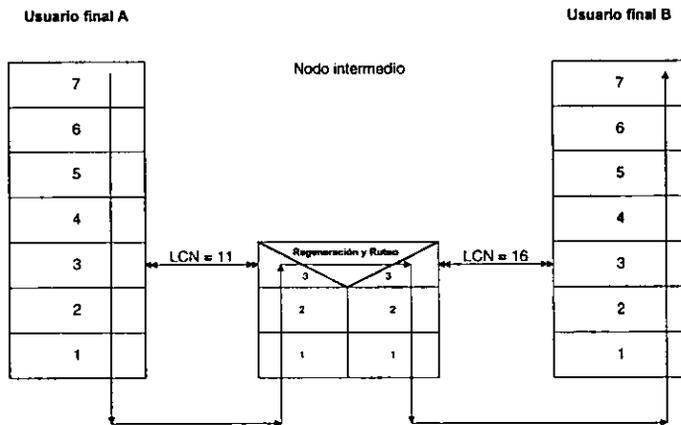


Fig. 3.1 Flujo y Ruteo de Datos en X.25

X.25 se apoya en el protocolo de capa 2 HDLC para proveer sus servicios, por lo que a continuación se describe este último.

### III.1.1 HDLC (High-Level Data Link Control)

HDLC es un estándar para la capa de enlace de datos publicado por ISO que se utiliza en todo el mundo. Soporta transmisión half-duplex y full-duplex, configuraciones multipunto y punto a punto, así como canales conmutados y no conmutados.

### III.1.2 Configuraciones de Operación de HDLC

Para HDLC, existen 3 tipos de estaciones:

- La estación *primaria* está en control del enlace o canal. Esta estación transmite tramas de *comando* a las estaciones secundarias en el canal. A su vez, recibe tramas de *respuesta* de esas estaciones. Si el enlace es multipunto, la estación primaria es responsable de mantener una sesión separada con cada estación en el enlace.
- La estación *secundaria* actúa como esclava de la primaria. Responde a los comandos de ésta y mantiene únicamente una sesión, que debe ser con la estación primaria. No tiene responsabilidad alguna del control del enlace.
- La estación *combinada* transmite tanto comandos como respuestas y recibe ambos tipos de tramas de otra estación combinada. Mantiene una sesión con cada una de las otras estaciones combinadas.

Las estaciones se comunican entre sí a través de uno de tres estados lógicos:

- El *estado lógicamente desconectado (LDS, Logically Disconnected State)* prohíbe que una estación transmita o reciba información. Si la estación secundaria se encuentra en un *modo normal desconectado*, entonces puede transmitir una trama sólo después de recibir un permiso explícito de la estación primaria para hacerlo. Si la estación se encuentra en *modo asíncrono desconectado*, la estación secundaria puede iniciar una transmisión sin recibir permiso explícito, pero la trama debe ser sencilla, indicando únicamente el estatus de la estación secundaria.
- El *estado de inicialización (IS, Initialization State)* se define por implementaciones específicas y está fuera de los estándares de HDLC

- El estado de transferencia de información (ITS) permite que las estaciones secundarias, primaria y combinadas transmitan y reciban información de usuario. Este estado se puede cambiar al emitir comandos de desconexión, que se discutirán más adelante.

Cuando las estaciones se encuentran en un estado de transferencia de información, se permite que se comuniquen en uno de tres modos de operación. Estos modos pueden ser iniciados y reiniciados en cualquier momento durante la sesión, lo que permite una gran flexibilidad en cómo se comunican las estaciones entre sí; los modos son:

- *Modo de respuesta normal (Normal Response Mode, NRM)*. Requiere que la estación secundaria reciba permiso explícito de la primaria antes de transmitir. Después de recibirlo, inicia una transmisión de respuesta que puede contener datos, y que puede consistir de una o más tramas. Después de la última trama de la transmisión, se debe esperar nuevamente el permiso antes de volver a transmitir
- *Modo de respuesta asíncrono (Asynchronous Response Mode, ARM)*. Permite que una estación secundaria inicie transmisiones sin recibir permiso explícito por parte de la estación primaria (normalmente cuando el canal está desocupado). La transmisión puede contener tramas de datos sencillas o múltiples, o bien pueden contener información de control que refleje los cambios de estatus de la estación secundaria.
- *Modo asíncrono balanceado (Asynchronous Balanced Mode, ABM)*. Utiliza estaciones combinadas. La estación combinada puede iniciar transmisiones sin recibir el permiso previo de la otra estación de este tipo.

Además de todo lo anterior, HDLC provee tres maneras de configurar el canal para el uso de estaciones primarias, secundarias y combinadas.

- Configuración *desbalanceada*: Permite que operen una estación primaria y una o más estaciones secundarias. Se llama desbalanceada porque la estación primaria es la responsable de controlar cada estación secundaria y de establecer los comandos de determinación de modo.
- Configuración *simétrica*: Permite dos configuraciones de estaciones independientes, desbalanceadas y de punto a punto. Cada estación tiene un

estatus de primaria y secundaria; y por lo tanto cada estación se considera lógicamente como dos. No es muy utilizada.

- Configuración *balanceada*: Consiste de dos estaciones combinadas, las cuales tienen igual estatus en el canal y tienen iguales responsabilidades en cuanto al control del enlace.

A estas configuraciones se les conoce respectivamente como *balanceada normal* (UN, *Unbalanced Normal*), *asíncrona desbalanceada* (UA, *Unbalanced Asynchronous*) y *balanceada asíncrona* (BA, *Balanced Asynchronous*).

### III.1.3 Formatos de Trama de HDLC

Existen tres tipos de trama en HDLC:

- El *formato de información* se utiliza para transmitir datos de usuario final entre dispositivos. La trama de información también puede acusar recibo de datos de una estación transmisora, así como algunas funciones de control muy limitadas.
- El *formato supervisor* realiza funciones de control tales como el acusar recibo de tramas, la solicitud de retransmisión, y la solicitud de suspensión temporal de transmisión de las mismas. El uso específico de la trama supervisora depende del modo operacional del enlace.
- La trama con *formato no numerado* también se usa con fines de control, y es utilizada para llevar a cabo la inicialización o desconexión del enlace, entre otras (todas relacionadas con el enlace). La trama contiene cinco posiciones de un bit, lo cual permite definir hasta 32 comandos y 32 respuestas.

La trama consiste de cinco o seis campos (seis si es de información), que se muestran en la fig. 3.2.

Bandera	Dirección	Control	Información	FCS	Bandera
---------	-----------	---------	-------------	-----	---------

Fig. 3.2 Formato de la trama HDLC

Todas las tramas deben comenzar y terminar con los *campos de bandera (flag fields)*. Las estaciones que están escuchando el enlace de datos deben esperar continuamente encontrar la secuencia de bandera, que es 01111110. Una vez que la estación detecta una secuencia que no sea de bandera, sabe que ha encontrado el comienzo de una trama, un problema (condición de aborto) o una condición de canal desocupado. Cuando encuentra la segunda bandera, sabe que tiene la trama completa.

El *campo de dirección (address field)* identifica a la estación primaria o secundaria involucrada en la transmisión de la trama particular. Se asocia una dirección única a cada estación. En una configuración desbalanceada, los campos de dirección tanto en comandos como respuestas contienen la dirección de la estación secundaria. En una configuración balanceada, la trama de comando contiene la dirección de destino y la trama de respuesta contiene la dirección de la estación de origen.

El *campo de control (Control Field)* contiene los comandos y las respuestas, así como los números de secuencia que se utilizan para mantener la contabilidad del flujo de tráfico entre las estaciones. El formato y el contenido de este campo varían dependiendo del tipo de trama HDLC.

El *campo de información (Information Field)* contiene los datos del usuario, y se encuentra únicamente en la trama con formato de información. Este campo es inexistente en el formato supervisor o no numerado.

El *campo de verificación de secuencia (FCS, Frame Check-Sequence Field)* se utiliza para verificar errores de transmisión entre dos estaciones. La estación emisora efectúa un cálculo sobre los datos del usuario y anexa el resultado del cálculo como el campo FCS. Si las respuestas son consistentes, existe una buena probabilidad de que la transmisión se haya llevado a cabo sin errores. Si las comparaciones fallan, es indicio de que hubo un error de transmisión, en cuyo caso la estación receptora emite un acuse de recibo negativo para solicitar la retransmisión de la trama. Al cálculo del FCS se le conoce como verificación de redundancia cíclica (Cyclic Redundancy Check, CRC) y utiliza el generador polinomial  $X^{16} + X^{12} + X^5 + 1$ .

El CRC puede detectar todas las cadenas de errores sencillos que no excedan 16 bits, y el 99.99% de todas las cadenas posibles más grandes.

### III.1.4 Comandos y Respuestas de HDLC

En la figura 3.3 se muestran los tipos de comandos y respuestas en HDLC para cada una de las configuraciones de canal que existen. El formato de trama supervisora provee cuatro de estos comandos y respuestas, y son *Listo para Recibir (RR, Receive Ready)*, *No Listo para Recibir (RNR, Receive Not Ready)* y *Rechazo Selectivo (SREJ, Selective Reject)*.

Balanceada Normal (UN)

Primario	Secundario
Comando	Respuesta
↓ RR RNR SNRM DISC	↓ RR RNR UA DM FRMR

Desbalanceada Asíncrona (UA)

Primario	Secundario
Comando	Respuesta
↓ RR RNR SNRM DISC	↓ RR RNR UA DM FRMR

Balanceada Asíncrona (BA)

Primario	Secundario
Comando	Respuesta
↓ RR RNR SABM DISC	↓ RR RNR UA DM FRMR

Fig. 3.3 Comandos y respuestas de HDLC

**RR:** Se utiliza por la estación primaria o secundaria para indicar que se encuentra lista para recibir una trama de información y/o emitir acuses de recibo. También puede cambiar el estatus de ocupado del enlace.

**SREJ:** Una estación emite una trama de este tipo cuando solicita la retransmisión de una trama en particular. Acusa recibo de tramas en grupo. Las tramas recibidas posteriormente a la emisión del SREJ se aceptan y se espera por la trama solicitada para retransmisión.

**Reject (REJ).** Se usa para solicitar la retransmisión de tramas a partir de un número, y acusa recibo de todas las tramas recibidas con un número inferior al indicado.

El formato no numerado es el que provee la mayoría de los comandos y respuestas de HDLC, y se pueden agrupar de acuerdo a su función:

- *Comandos de definición de modo:* SNRM, SARM, SABM, SNRME, SARME, SABME, RIM, SIM, DISC).
- *Comandos de transferencia de información:* UI, UP
- *Comandos de recuperación:* RESET
- *Comandos misceláneos:* XID, TEST

A continuación se describen estos comandos/respuestas:

*UI (Información no Numerada, Unnumbered Information).* Este comando permite la transmisión de tramas sin número de secuencia.

*RIM (Request Initialization Mode, Modo de Solicitud de Inicialización).* La trama RIM es una solicitud de una estación secundaria para que la estación primaria emita un comando SIM.

*SIM (Set Initialization Mode, Establecer Modo de Inicialización).* Este comando se utiliza para inicializar la sesión primaria/secundaria. Espera una respuesta UA.

*SNRM (Set Normal Response Mode, Establecer Modo de Respuesta Normal).* Esta trama coloca a la estación secundaria en NRM, modo que evita que la estación secundaria envíe tramas no solicitadas. Esto significa que la estación primaria controla todo el flujo de tráfico en la línea.

*DM (Disconnect Mode, Modo de Desconexión).* Esta trama se transmite desde una estación secundaria para indicar que está en modo no operacional o desconectado.

*DISC (Disconnect, Desconexión).* Este comando de una estación primaria coloca a la estación secundaria en modo desconectado, de manera similar a cuando se cuelga un teléfono. El acuso de recibo que se espera es una trama UA.

*UA (Unnumbered Acknowledgement, Acuso de Recibo no Numerado).* Esta es una respuesta para los comandos de definición de modo (y SIM, DISC, RESET). También se utiliza para reportar el final de la condición de ocupado de una estación.

*FRMR (Frame Reject, Rechazo de Trama).* La estación secundaria la envía cuando se encuentra con una trama inválida. No se refiere a errores de bits indicado por el CRC, sino a condiciones menos comunes, como las que siguen:

1. Recepción de un campo de control inválido.
2. Recepción de un campo de información demasiado largo.

3. Recepción de un campo de información no permitido o de una trama supervisora/no numerada de tamaño incorrecto.

*RD (Request Disconnect, Solicitud de Desconexión)*. Es una solicitud de una estación secundaria para que se le coloque en un estado lógicamente desconectado.

*XID (Exchange Station Identification, Intercambio de Identificación de Estación)*. Este comando pregunta por la identificación de una estación secundaria. Es muy útil en facilidades conmutadas para identificar a la estación que efectúa la llamada.

*TEST (Test, Prueba)*. Se utiliza para solicitar respuestas de prueba de una estación secundaria.

*SARM (Set Asynchronous Response Mode, Establece Modo de Respuesta Asíncrono)*. Establece el modo de operación para permitir que la estación secundaria transmita sin una petición de la estación primaria. Coloca a la estación secundaria en el estado de transferencia de información (IS). Ya que SARM establece dos estaciones desbalanceadas, se debe emitir en ambas direcciones del enlace.

*SABM (Set Asynchronous Balanced Mode, Establece Modo Asíncrono Balanceado)*. Este comando coloca a ambas estaciones como estaciones combinadas, por lo que no necesitan requerimientos de transmisión.

*SNRME (Set Normal Response Mode Extended, Establece Modo de Respuesta Normal Extendido)* Igual a SABM pero con dos bytes extras en el campo de control.

*SABME (Set Asynchronous Balanced Mode Extended, Establece Modo Asíncrono Balanceado)* Establece SABM con dos bytes extras en el campo de control.

*UP (Unnumbered Poll, Requisición no Numerada)*. Requiere para transmisión a una estación sin importar el secuenciamiento o acuse de recibo.

*RSET (Reset, Reinicialización)* Reinicializa el estado de ambas estaciones, la emisora y la receptora. Se utiliza para recuperación de errores. Tramas que falten por acusarse de recibo, no se acusan.

### III.1.5 Capas Inferiores de X.25

#### X.25 y la Capa Física

Aunque X.25 está definido para la capa 3, en realidad también cubre las capas 1 y 2. La interfaz física recomendada entre el DTE y el DCE debe ser similar a la RS-232. Es decir, debe tener las siguientes señales y circuitos:

Enviar Datos	<i>Send Data</i>	TX
Recibir Datos	<i>Receive Data</i>	RX
Solicitud de Envío	<i>Request to Send</i>	RTS
Listo para Enviar	<i>Clear to Send</i>	CTS
Conjunto de Datos Listo	<i>Data Set Ready</i>	DSR
Terminal de Datos Lista	<i>Data Terminal Ready</i>	DTR
Detector de Portadora	<i>Carrier Detect</i>	CD

Para que estas interfaces se puedan usar, X.25 necesita que los circuitos RTS, DSR, DTR y CD estén en condición de ENCENDIDO. Los datos se intercambian por TX y RX. Si estos circuitos se encuentran apagados, X.25 asume que la capa física está inactiva, y las capas de enlace de datos y red no operarán.

#### X.25 y la Capa de Enlace de Datos

X.25 asume que la capa de enlace de datos usa el protocolo *LAPB (Link Access Procedure, Balanced, Procedimiento de Acceso al Enlace, Balanceado)*. Este protocolo es un subconjunto de HDLC que utiliza el modo asíncrono balanceado y, además, permite el rechazo simultáneo de tramas en un modo de transmisión en dos sentidos. No permite transmitir información en tramas de tipo respuesta; sin embargo, esto no representa ningún problema ya que en el modo asíncrono balanceado la información puede transferirse en las tramas de comando, y como ambas estaciones son estaciones primarias ambas pueden transmitir comandos.

LAPB y X.25 interactúan de la siguiente manera:

El paquete de X.25 es transportado dentro de la trama de LAPB como el campo I (información). La tarea de LAPB es asegurarse que los paquetes de X.25 se transmitan libres de errores a través del canal.

LAPB utiliza un subconjunto específico de HDLC para soportar X.25, consistente de 13 comandos y respuestas, estos son:

<b>Comandos</b>	<b>Respuestas</b>
<i>Información (I)</i>	Recepción Lista (RR)
<i>Recepción Lista (RR)</i>	Rechazo (REJ)
<i>Rechazo (REJ)</i>	Recepción no Lista (RNR)
<i>Recepción no Lista (RNR)</i>	Acuse de recibo no numerado (UA)
<i>Desconexión (DISC)</i>	
<i>Establece Modo de Respuesta Asíncrono (SARM)</i>	Rechazo de Trama (FRMR)
<i>Establece Modo Asíncrono Balanceado (SABM)</i>	Modo Desconectado (DM)

De acuerdo con las reglas de HDLC de direccionamiento, las tramas de información siempre tendrán la dirección de destino, lo que evita cualquier ambigüedad en tratar de determinar la interpretación correcta de la trama. Si, por ejemplo, la estación A recibe una trama REJ con la dirección de A, sabe que se trata de un comando. Si la trama REJ contiene la dirección de B, la estación sabe que recibió una respuesta.

### **III.1.6 Características de X.25**

X.25 opera en base a utilizar servicios de circuitos virtuales. Un circuito virtual (también conocido como canal lógico en la terminología de X.25) es aquel en el cual un usuario percibe la existencia de un circuito físico dedicado a su computadora, aunque en realidad está asignado a múltiples usuarios. Utilizando técnicas de multiplexaje, los diferentes paquetes de los usuarios son 'entretreídos' en un sólo canal físico. X.25 utiliza números de canales lógicos (LCN) para identificar las conexiones de DTE a la red. Puede soportar hasta 4095 canales lógicos en un sólo canal físico.

## Opciones de Canal

El estándar X.25 provee cuatro mecanismos para establecer y mantener las comunicaciones:

- Circuito Virtual Permanente (PVC, Permanent Virtual Circuit)
- Llamada Virtual (VC, Virtual Call)
- Llamada de Selección Rápida (Fast-Select Call)
- Llamada de Selección Rápida con Limpiado Inmediato (Fast-Select Call with Immediate Clear)

*Circuito Virtual Permanente (PVC).* Es análogo a una línea telefónica rentada, ya que se asegura que el DTE obtenga una conexión al DTE receptor a través de la red de paquetes. X.25 requiere que un PVC se establezca antes de que comience la sesión. En consecuencia, se debe llegar a un acuerdo previo entre los dos usuarios y la red de paquetes portadora antes de que se establezca la conexión virtual permanente. Por lo tanto, cuando un DTE envía un paquete a la red, la información de identificación en el mismo (un número de canal lógico) indica que el DTE solicitante tiene una conexión de PVC con el DTE receptor. Entonces, se establece la conexión por la red y el DTE receptor sin ningún arbitrio ni negociación de sesión. PVC no requiere inicialización o procedimientos de limpieza, y el canal lógico se encuentra continuamente en un estado de transferencia de datos.

*Llamada Virtual.* También conocida como llamada virtual conmutada, asemeja algunos de los procedimientos asociados con las líneas de llamadas telefónicas. El DTE de origen produce un paquete de solicitud de llamada en la red con un LCN de 11. La red rutea dicho paquete al DTE de destino. Este lo recibe como un paquete de llamada entrante, que le llega desde su nodo de red con un LNC de 16.

La numeración del canal lógico ocurre en cada extremo de la red; el requerimiento principal es mantener la sesión DTE-DTE específica identificada en todo momento con LCN's 11 y 16.

Si el DTE receptor decide acusar recibo y aceptar la llamada, emite un paquete de llamada aceptada. La red entonces transporta este paquete hasta el DTE solicitante en forma de un paquete de llamada conectada. El canal entra en un estado de transferencia de datos después de que se establece la llamada. Para terminar la sesión, una solicitud de limpieza se envía por cualquier DTE. Se recibe como una indicación de limpieza, y se confirma con un paquete de confirmación de limpieza.

*Selección Rápida.* Este mecanismo tiene dos opciones, siendo la primera la llamada de selección rápida. Un DTE puede solicitar este servicio en base a cada llamada al nodo de la red (DCE) por medio de la solicitud adecuada en el encabezado de un paquete. Permite que el paquete de solicitud de llamada contenga hasta 128 bytes de datos de usuario. El DTE que fue llamado contesta con un paquete de aceptación de llamada, que también puede contener información de usuario. Si se transmite un paquete de este tipo, la sesión de X.25 continúa con los procedimientos normales de transferencia de datos y limpieza de una llamada virtual conmutada.

La segunda opción es la *selección rápida con limpieza inmediata*. Al igual que con la opción anterior, una solicitud de llamada contiene datos de usuario. El paquete se transmite a través de la red al DTE receptor que, si acepta la llamada, transmite una solicitud de limpieza que también contiene datos de usuario. Después el procedimiento es el normal.

La idea de la selección rápida es dar soporte a aplicaciones que tienen únicamente una o dos transacciones, tales como transacciones de punto de venta, autorización de crédito y transferencia de fondos. Estas aplicaciones no pueden usar de manera eficiente una llamada virtual conmutada por el recargo de trabajo y el retraso que se requieren en el establecimiento de la conexión. Tampoco pueden tomar ventaja del uso de un PVC por que su uso ocasional no justifica la asignación permanente de recursos.

La selección rápida también se puede utilizar en entradas de trabajos remotos (Remote Job Entries, RJE) y transferencia de archivos muy grandes, ya que, por ejemplo, permitirían al DTE receptor examinar hasta 128 bytes de datos antes de determinar si puede aceptar una sesión muy intensa en cuanto a datos y tiempo de corrida. La

respuesta de aceptación de llamada podría entonces otorgar el permiso, e inclusive tal vez incluir en el paquete las reglas para la transferencia de información entre las aplicaciones de usuario final.

### III.1.7 Otros Tipos de Paquetes.

Además de los paquetes mencionados en el punto anterior, existen otros paquetes que X.25 utiliza, y que se describen a continuación:

**Interrupción.** Permite a un DTE transmitir un paquete no secuenciado a otro DTE sin seguir los procedimientos de flujo de control establecidos. Puede transportar hasta 32 bytes de datos de usuario, y es necesario recibir una confirmación de interrupción antes de poder enviar otro.

Los paquetes de *RR* Y *RNR* se utilizan de manera muy similar a sus comandos homónimos en HDLC. Ambos paquetes tienen un número de secuencia de recepción para indicar cuál es el siguiente paquete que esperan, y cumplen la misma función de control de flujo de tráfico iniciado por el usuario.

El paquete *RNR* se utiliza para solicitar a la estación transmisora que detenga el envío de paquetes y también utiliza el campo del número de secuencia para acusar de recibo cualesquiera paquetes que se hayan recibido con anterioridad.

El paquete de *Rechazo (REJ)* rechaza específicamente la trama recibida. Cuando se utiliza, se solicita la retransmisión de paquetes, empezando con el número que se encuentra en el campo de secuencia de recepción.

El paquete de *Reinicialización (Reset)* se utiliza para reinicializar una llamada virtual conmutada o un circuito virtual permanente. El procedimiento de reinicio elimina en cada sentido entre las dos estaciones todos los datos y paquetes de interrupción que se puedan encontrar en la red. Estos procedimientos pueden ser necesarios cuando ocurren condiciones de error, tal como paquetes perdidos, duplicados o que no pueden ser resecuenciados correctamente. Únicamente puede ocurrir reinicio durante un estado de transferencia de datos.

El procedimiento de *Reinicio (Restart)* se utiliza para inicializar o reinicializar la interfaz DTE/DCE a nivel de paquetes. Se pueden afectar hasta 4095 canales lógicos en un puerto físico. El procedimiento limpia todas las llamadas virtuales y reinicializa todos los circuitos virtuales permanentes al nivel de la interfaz. El reinicio se puede producir como resultado de un problema muy severo, tal como una caída del sistema. Todos los paquetes aún no acusados de recibo se pierden y deben recuperarse por medio de un protocolo de alto nivel.

El paquete de *limpieza (Clear)* se utiliza para una gran variedad de funciones, aunque la principal es para limpiar una sesión DTE-DTE. Otro de sus usos es indicar que una solicitud de llamada no puede ser completada.

El paquete de *diagnóstico* se utiliza por algunas redes X.25 para indicar ciertas condiciones de error que no son cubiertas por otros métodos, tales como la reinicialización y el reinicio. Algunos de estos códigos son:

- paquete no identificable
- paquete muy largo o muy corto
- confirmación de interrupción no autorizada
- tiempo límite expiró
- dirección inválida
- no hay canal lógico disponible
- servicio no disponible

Finalmente, los paquetes de registro se utilizan para invocar o confirmar los servicios de X.25. Se envía una confirmación de registro para informar del estatus de la solicitud.

### III.1.8 Estados de los Canales Lógicos

Los canales lógicos proveen la base para administrar las conexiones DTE/DCE. Por medio del uso de varios tipos de paquetes, el canal lógico puede tomar los siguientes estados:

<i>Número de Estado</i>	<i>Descripción</i>
p1 o d1 o r1	nivel de paquetes listo.
p2	DTE esperando
p3	DCE esperando
p5	colisión de la llamada
p4	transferencia de datos
p6	Solicitud de limpieza del DTE
p7	Indicación de limpieza del DCE
d2	Solicitud de reinicialización del DTE
d3	Indicación de reinicialización del DCE
r2	Solicitud de reinicio del DTE
r3	Indicación de reinicio del DCE

En la tabla 3.1 se muestra en ejemplo de establecimiento de llamada para dar una mejor idea de cómo funcionan los estados del canal.

**Tabla 3.1 Ejemplo de establecimiento de llamada**

Secuencia De eventos	Paquete	Desde	Hasta	Estado del canal desde	Hasta estado del canal
1	Solicitud de llamada	DTE local	DCE local	p1	p2
2	Llamada entrante	DCE remoto	DTE remoto	p1	p3
3	Llamada aceptada	DTE remoto	DCE remoto	p3	p4
4	Llamada conectada	DCE local	DTE local	p2	p4

### III.1.9 Formatos de Paquete

La longitud por omisión es de 128 bytes u octetos, pero X.25 tiene opciones para otras longitudes: 16, 32, 64, 256, 512, 1024, 2048 y 4096 octetos. Si el campo de datos de usuario es más grande que el campo máximo permitido por la red, el DTE receptor reinicializará la llamada virtual emitiendo el paquete correspondiente.

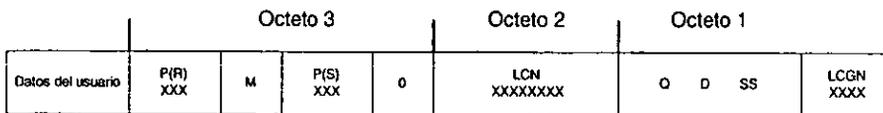


Fig. 3.4 (a) Encabezado de paquete de datos

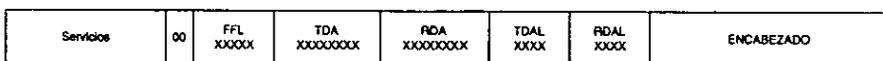


Fig. 3.4 (b) Cuerpo de un paquete de no datos

Cada paquete que se transmite a través de la interfaz DTE/DCE hacia la red, debe tener al menos tres bytes (u octetos), los cuales forman el encabezado del paquete, aunque se pueden usar más octetos para formarlo. El encabezado se muestra en la fig. 3.4. Los primeros cuatro bits del primer octeto del encabezado contienen el número del grupo de canales lógicos. Los últimos cuatro bits contienen el identificador de formato general. Los bits 5 y 6 de éste identificador (SS) se usan para indicar el formato de secuencia para la sesión de paquetes. Dicho formato puede ser de dos tipos, *Módulo 8* y *Módulo 128*. El primero permite números de secuencia de 1 a 7 y el segundo número de 0 a 127. El séptimo bit (o bit D) del identificador de formato general se usa únicamente con algunos tipos de paquetes. El octavo bit se le conoce como bit Q, y se utiliza únicamente en paquetes de tipo dato de usuario final.

El segundo octeto del encabezado contiene el número de canal lógico LCN. este campo de ocho bits, combinado con el número de grupo de canal lógico, provee la identificación completa de 12 bits del canal lógico, lo cual permite hasta 4095 canales lógicos. El LCN 0 está reservado para control (paquetes de diagnóstico y reinicio).

El tercer octeto es el identificador de tipo de paquete en el caso de paquetes que no son de información, y el número de secuencia para paquetes de datos.

La fig. 3.4 (B) ilustra los campos adicionales. Para paquetes de establecimiento de llamada, se incluyen las direcciones de DTE así como las longitudes de las mismas. Los campos de direcciones pueden encontrarse desde el cuarto hasta el decimonoveno octeto del paquete de solicitud de llamada. Estas direcciones se usan para identificar las estaciones al momento de establecer una llamada. Después, la red utiliza el LCN asociado para identificar la sesión DTE-DTE. Adicionalmente, pueden usarse los campos de servicios, y se pueden incluir datos de usuario, hasta un máximo de 16 octetos. Este campo puede ser útil para información de registro tales como contraseñas e información de contabilización de recursos. Para algunas opciones se permiten hasta 128 octetos.

El encabezado del paquete se modifica para facilitar el movimiento de los datos de usuario a través de la red. Como se puede ver en la Fig 3.1.4(a), el tercer octeto del encabezado, normalmente reservado para el identificador del paquete, se separa en cuatro campos diferentes:

<i>Bits</i>	<i>Descripción o Valor</i>
1	0
2-4	Secuencia de envío de paquete P(S)
5	Bit de más datos ( bit M)
6-8	Secuencia de recepción de paquete P(R)

Las funciones de estos campos son como siguen: El primer bit, en 0, identifica al paquete como uno de datos. se asignan tres bits al número de secuencia de envío P(S). Se asigna un bit para la función M (que se explica un poco mas adelante), y los tres bits restantes se asignan al número de secuencia de recepción P(R).

Los números de envío y recepción se usan para coordinar y acusar de recibo las transmisiones entre DTE y DCE. El bit M identifica una secuencia relacionada de paquetes viajando por la red, y ayuda a la red y a los DTEs para conservar la identificación de bloques de datos cuando éstos se dividen en paquetes más pequeños.

### III.1.10 Control de Flujo

X.25 utiliza técnicas de control de flujo muy similares a las de HDLC/LAPB. Como se vio anteriormente, un paquete de datos combina dos números de secuencia (de envío y de recepción) para coordinar el flujo de paquetes entre el DTE y el DCE. En la interfaz DTE/DCE, los paquetes de datos se controlan separadamente para cada dirección, basándose en las autorizaciones provenientes del usuario en la forma de números de secuencia de recepción o de los paquetes de control RR o RNR.

Puede parecer redundante el tener control de flujo en la capa de enlace de datos y en la capa de red o de paquetes. Sin embargo, como X.25 multiplexa varios usuarios en un sólo enlace físico, la emisión de un RNR a nivel enlace afectaría al tráfico de *todas* las conexiones lógicas en el mismo. De esta manera, el control de flujo se puede aplicar mucho más selectivamente. Además, el secuenciar a nivel de interfaz de red agrega un nivel adicional de confiabilidad y seguridad a los datos del usuario.

### III.1.11 Servicios de X.25

A continuación se mencionan, con una breve descripción, algunos de los servicios que ofrece este protocolo:

*Registro de Servicio en Línea.* Permite que el DTE solicite un servicio en cualquier momento, o bien obtener los parámetros de los mismos, como lo entiende el DCE. El diálogo DTE/DCE se lleva a cabo por medio de los paquetes de registro, y éstos indican si el valor del servicio puede ser negociado.

*Retransmisión de Paquetes.* Un DTE puede solicitar la retransmisión de uno o más paquetes de datos del DCE. El DTE especifica el número de canal lógico el valor de P(R) en el paquete de rechazo. El DCE debe entonces retransmitir todos los paquetes desde P(R) hasta el siguiente paquete que transmitirá por primera vez.

*Tamaños por Omisión de Paquetes no Estándares.* Permite la selección de valores por omisión para el tamaño de los paquetes que son soportados por la red. Se pueden usar paquetes de registro para negociar el tamaño de los paquetes.

*Identificación del Usuario de Red.* Este servicio permite que el DTE que realiza la llamada proporcione información de administración, seguridad o contabilidad al DCE en base a llamada. Si dicha información es inválida, la llamada es ignorada.

*Selección e Indicación de Retraso de Tránsito.* Este último servicio permite que un DTE seleccione un tiempo de retraso a través de la red. Esto puede ser muy útil para un usuario.

### **III.2 ISDN ( Integrated Services Digital Network)**

El término ISDN fue definido por el CCITT en 1986. El concepto de ISDN evolucionó a partir de algo denominado la red digital integrada (IDN Integrated Digital Network).

ISDN es una red capaz de transmitir simultáneamente voz, datos, vídeo y gráficos de forma digital. El objetivo de ésta red es ofrecer comunicaciones punto a punto en forma digital mediante un interfaz estándar.

ISDN no necesita instalación de fibra óptica para alcanzar altas velocidades, sino que convierte los cables de cobre en canales digitales (aunque como la fibra óptica permite un mayor flujo de datos, es más recomendable cambiar el cobre). Con ISDN es posible reducir el costo de las comunicaciones de voz y datos. Además de ofrecer un nuevo y amplio espectro de métodos de recuperación de información. ISDN ofrece integración de servicios de voz, datos y vídeo sobre la misma conexión.

ISDN ofrece los beneficios de las comunicaciones digitales, haciendo los servicios disponibles sobre una red integrada, tiene el potencial de proporcionar un alto nivel de control sobre las facilidades de la red. Soportando un amplio rango de información, almacenamiento y servicios de procesamiento.

ISDN es un sistema telefónico que reemplaza todos los servicios analógicos por servicios digitales. Todas las señales son digitales no importando si ellas se originen desde un teléfono, computadora o bien que sean señales portadoras entre ciudades ya

que todas las señales son digitales. Un adaptador ISDN formatea los datos de las líneas de teléfono tomando el lugar de un módem cuando una computadora se conecta al sistema telefónico. Se brinda al usuario el gran beneficio de poder acceder a múltiples servicios a través de un único punto de interconexión, integrado y estandarizado. Se proporciona un mejor aprovechamiento del ancho de banda para multiplexar voz digitalizada, datos, imágenes, fax, sonido Hi-Fi, videotext y teletext, así como servicios desde 144 kbps además de soportar conexiones conmutadas y no conmutadas.

### **III.2.1 Servicios**

Los servicios proporcionados por ISDN se clasifican en: servicios de transporte, servicios de teleservicio y servicios complementarios.

#### **Servicios de transporte**

Proporciona el medio de transmisión de información entre usuarios en tiempo real y sin alterar el contenido del mensaje. Estos servicios corresponden a las tres capas inferiores del modelo OSI.

#### **Servicios de Teleservicio**

Cubre los requerimientos de las aplicaciones de los usuarios finales a través de las funciones corresponden a las capas de la 4ª a la 7ª del modelo OSI. Por ejemplo: telefonía, telex, videotex, teleconferencia, etc.

#### **Servicios complementarios**

Es un grupo de servicios que no pueden usarse solos sino en conjunción con uno o más de los servicios de transporte o teleservicios (servicios básicos).

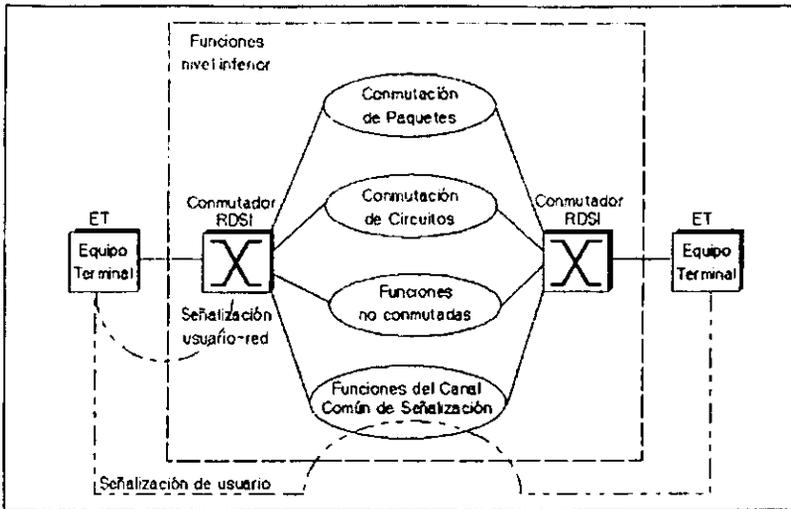


Fig. 3.5 Servicios que proporciona una red ISDN

### III.2.2 Estándares

El CCITT se dio a la tarea de dar las recomendaciones que definen los conceptos y principios del ISDN y especificar sus capacidades de servicios, características de red, interfaces usuario-red, interfaces de interconexión y aspectos de mantenimiento. Lo anterior está contenido en las recomendaciones aprobadas por el CCITT en 1988. Estas recomendaciones se dividen en seis series, que van de la serie I.100 a la serie I.600:

Las series I.100 proporcionan una introducción general a ISDN su terminología, principio de diseño y desarrollo evolutivo.

Las series I.200 contienen una metodología por medio de la cual los servicios (servicios de transporte, teleservicios y servicios complementarios) ofrecidos por ISDN pueden ser clasificados y descritos.

Las series I.300 definen los atributos y topologías de las conexiones de red que pueden ser establecidos sobre el ISDN, los objetivos de desempeño para estas conexiones, su numeración y direccionamiento.

Las series I.400 contienen una descripción detallada de la interface entre el equipo del usuario final y la red.

Las series I.500 se refieren al problema de interconexión entre redes ISDN y otras estructuras de red con el fin de desarrollar un conjunto de funciones estándar que aseguran que los usuarios de redes públicas o privadas puedan ser incorporados en un medio ambiente global de comunicaciones.

Las series I.600 se refieren a servicios de mantenimiento para la interface entre el subscriptor y la red OSI así como para su instalación. Incluye un modelo general de arquitectura de mantenimiento y procedimientos para la supervisión, pruebas internas, detección y localización de fallas.

### **III.2.3 Estructura de la transmisión**

El enlace digital entre la oficina central y el subscriptor ISDN se lleva a cabo mediante canales de comunicación. La estructura de la transmisión de cualquier acceso se constituye por los siguientes tipos de canales:

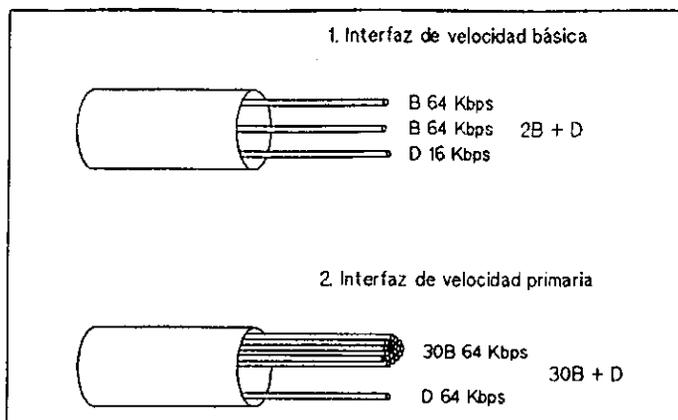
- Canal B (B=bearer ). Es un canal de usuario para transmitir datos digitales, voz digitalizada codificada o una mezcla de ellos.
- Canal D (D=DELTA). Tiene dos propósitos principales: llevar a cabo información de señalización de canales comunes para controlar llamadas conmutadas por circuito y usarse para conmutación por paquetes cuando no hay información por señalización en espera.
- Canales H. Se proporcionan para transmitir información de usuario (teleconferencias, datos en alta velocidad o audio de alta calidad).

Canal	Velocidad de transmisión	Asociación
<b>B</b>	64 kbps	ISDN
<b>D</b>	16 y 64 kbps	ISDN
<b>E</b>	64 kbps	ISDN
<b>H0</b>	384 kbps = 6B	BISDN
<b>H11</b>	1536 kbps = 24B	BISDN
<b>H12</b>	1920 kbps = 30B	BISDN
.		
.		
.		
<b>H4</b>	120 a 140 kbps	BISDN

Fig. 3.6 Velocidad de transmisión de los canales en una red ISDN e ISDN

La capa física del ISDN corresponde a la capa 1 del modelo OSI, en la cual existen dos tipos de interface de usuario:

- BRI ( Basic Rate Interface ) o BRA ( Basic Rate Access ). Servicio básico de ISDN formado por dos canales B que se usan para la información del usuario, cada uno con un promedio de datos de 64 kbps y un canal D que se usa principalmente para el control de las llamadas el cual corre a 16 kbps (2B+D).
- PRI (Primary Rate Interface) o PRA ( Primary Rate Access ). Ofrece 23 canales B a 64 kbps. y un canal D a 64 kbps ( 23B+D ).



**Fig.3.7** Estructura de los canales ISDN

Se estima que en el futuro se utilice una tercera interface de red tipo H+D.

### III.2.4 Grupos Funcionales

El acceso a la red del suscriptor ISDN se descompone en cuatro grupos funcionales que en conjunto describen la capacidad del suscriptor para llevar a cabo la transmisión de información entre el usuario final y la red, los cuales se mencionan a continuación:

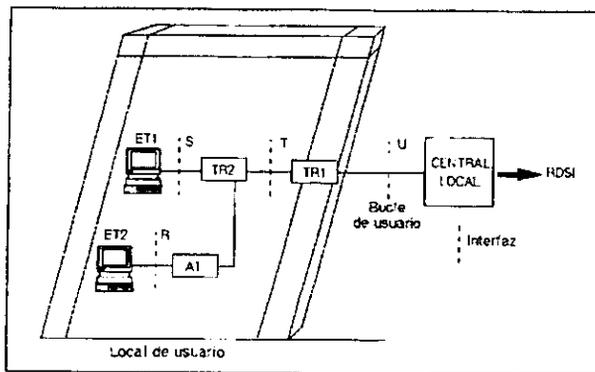
- Terminadores de Red: se subdividen en dos grupos:
  - Terminadores de Red 1 (NT1). Llevan a cabo funciones equivalentes a las del nivel 1 del modelo OSI.
  - Terminadores de Red 2 (NT2). Llevan a cabo funciones equivalentes a las de los niveles 1,2 y 3 del modelo OSI.
- Equipo terminal : se subdividen en dos grupos:
  - Equipo terminal tipo 1 (TE1). Teléfonos digitales, equipos terminales de datos y estaciones de trabajo que integran voz y datos.
  - Equipo terminal tipo 2 (TE2). Equipo terminal con interfaces no ISDN
- Adaptador terminal (TA)
 

Grupo funcional que incluye las funciones para conectar equipo TE2 dentro de ISDN.

- Puntos de Referencia

Son interfaces físicas o virtuales entre los tres grupos funcionales anteriores. Se clasifican en cuatro:

- **R:** Interface funcional entre un grupo TE2 y un TA.
- **T:** Interface entre el equipo NT2 y el NT1.
- **S:** Interface entre equipos de usuario como puede ser los TA o los TE1 y el equipo NT2.
- **U:** Interface del lado de la red del equipo NT1.



**Fig. 3.8** Puntos de referencia y grupos funcionales de una red ISDN

### III.2.5 B-ISDN (Broadband Integrated Service Digital Network)

Es una red de telecomunicaciones capaz de soportar aplicaciones multimedia, y que además posee poderosos sistemas de control de red que permiten operaciones complejas y servicios de administración sofisticados. Un ejemplo de esto es el hecho de poder establecer conexiones no sólo tomando en cuenta el número marcado, sino también evaluando la identidad de la persona que llama, la cantidad de recursos asignados a esa persona, así como el tráfico de la red en el momento de la llamada.

### III.2.5.1 Estándares

El concepto de B-ISDN se introduce por primera vez en 1988 con la recomendación I.121 del CCITT. Para 1990 el Grupo de Estudio XVIII aprueba algunas recomendaciones básicas, entre las que se incluyen aspectos generales de B-ISDN, servicios específicos de Red, características fundamentales de ATM, aplicaciones ATM, operación y mantenimiento de los accesos a B-ISDN.

### III.2.5.2 Características de B-ISDN:

- Un solo canal de transmisión y recepción
- Bajo costo
- Se modula y demodula la señal
- Utilizada por los estándares actuales de redes locales
- Varios canales paralelos
- Multiplexaje por frecuencia
- Conexiones conmutadas por demanda en Broad band
  - Permanentes
  - Semipermanentes
- Aplicaciones
  - Punto a punto
  - Punto a multipunto
- Modo de conmutación
  - Paquetes
  - Circuitos
- Naturaleza de servicios
  - Orientados a conexión
  - No orientados a conexión
- Configuraciones
  - Unidireccionales
  - Bidireccionales
- Tráfico
  - Velocidad constante CBR (Constant Bit Rate).
  - Velocidad variable VBR (Variable Bit Rate).

### III.2.5.3 Servicios

Los servicios de B-ISDN se clasifican en:

- Servicios interactivos. Son aquellos en los cuales hay un intercambio bidireccional de información ya sea entre dos suscriptores o un proveedor de servicios. Estos servicios a su vez se dividen en:

Servicios conversacionales. Proporcionan el medio para una comunicación bidireccional en tiempo real.

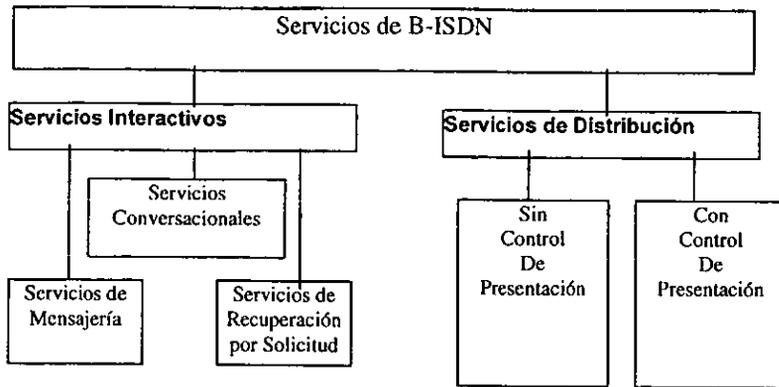
Servicios de mensajería. Ofrecen comunicación suscriptor a suscriptor mediante unidades de almacenamiento en oficina y manejo de mensajes. Este tipo de servicios normalmente no están garantizados.

Servicios de recuperación por solicitud . Proporcionan al usuario la capacidad de obtener cierta información específica.

- Servicios de distribución: Estos servicios se proporcionan sin control o con control de presentación:

Sin control de presentación: Proporcionan un flujo continuo de información que se distribuye desde una fuente central hacia un número ilimitado de receptores conectados a la red. El suscriptor puede acceder a esta información pero no tiene control sobre ella. Un ejemplo análogo de este servicio es la señal de televisión pública. Todos los destinatarios tienen la señal al mismo tiempo.

Con control de presentación: Estos servicios también distribuyen información de una fuente central a un gran número de usuarios, sin embargo la información se envía a una secuencia de entidades de información, con repetición cíclica de tal modo que el usuario tiene la habilidad de acceder y controlar el inicio y orden de la presentación de la información. Un ejemplo es el pago por evento, en donde sólo los usuarios que desean pagar y recibir un determinado programa lo hacen así.



**Fig. 3.9** Servicios que proporciona una red B-ISDN

Se requiere un canal de al menos 150 Mbps para soportar video de alta resolución mientras que para soportar simultáneamente más de un servicio se requiere que el suscriptor tenga una línea de 600 Mbps. La única tecnología que soporta esta tasa de transmisión es la fibra óptica.

## III.3 Frame Relay

Surgió originalmente como protocolo de uso para ISDN propuesto por la CCITT en 1988. Orientado a conexión por conmutación de paquetes fue diseñado para reemplazar el estándar X.25 permitiendo un throughput mucho más alto. Típicamente es usado para interconectar redes LAN de baja velocidad a largas distancias, incrementando hasta el triple la funcionalidad de las redes X.25.

A partir de la creación del foro Frame Relay a cargo de 4 empresas, su crecimiento fue notable, logrando acelerar su introducción al mercado. Este foro nombró extensiones de Frame Relay como Interfaces de Manejo Local, LMI (Local Management Interface).

Los estándares X.25 fueron desarrollados bajo la suposición de que el medio de transmisión es propenso a errores, y para asegurar la calidad en un enlace extremo a extremo se efectúa una administración de errores en cada nodo por medio del protocolo HDLC. La detección de errores y las funciones de recuperación se ejecutan enlace por enlace, lo que causa un tiempo de retraso, entorpeciendo a una red que opere a altas velocidades.

En Frame Relay, las funciones de corrección de errores y de control de flujo se manejan en el equipo del usuario o CPE (Customer Premises Equipment) para incrementar la eficiencia.

El protocolo de Frame Relay soporta tasas desde 64 kbps a 2 Mbps y sus aplicaciones incluyen:

- Aplicaciones de bloques de datos interactivos.- Aplicaciones que requieren bajos tiempos de retardo y gran volumen.
- Transferencia de archivos.- Aplicaciones que requieren gran volumen y corto tiempo de respuesta.
- Multiplexado de baja tasa de bits.- Aplicaciones que requieren las capacidades de multiplexación del protocolo de la capa 2.
- Tráfico con carácter interactivo.- Aplicaciones que requieren tramas cortas, retardos de tiempos bajos y volumen pequeño.

Sin embargo, Frame Relay, no es fácilmente aplicable para voz o para flujo de tráfico estacionario, el cual requiere procesamiento en tiempo real.

### III.3.1 Arquitectura de Frame Relay

El modelo de referencia para Frame Relay sigue la estructura del modelo de referencia OSI para ISDN. Como en otras áreas de ISDN se necesitan considerar dos planos separados de operación: el plano de control C, el cual esta relacionado con el establecimiento y terminación de conexiones lógicas y un plano de usuario U, el cual es responsable de la transferencia de los datos de usuario entre los suscriptores. Los protocolos del plano C están entre un usuario y la red mientras que los protocolos del plano U proporcionan una funcionalidad de extremo a extremo.

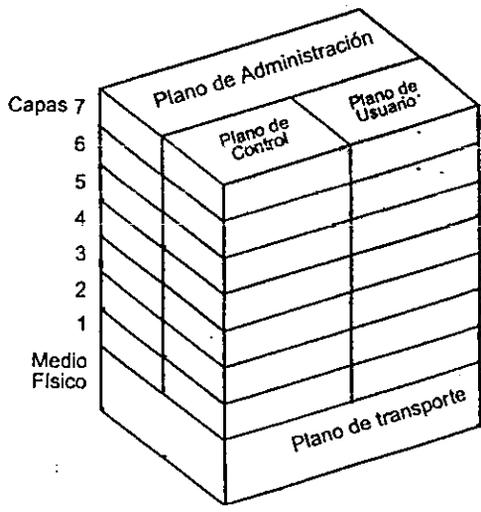


Fig. 3.10 Modelo de referencia para ISDN

Para la transferencia de información entre usuarios finales, el protocolo del plano U es el protocolo Q.922. Este protocolo es una recomendación que fue establecida por primera vez en 1991, la cual es una versión ampliada de LAPD (1.441/Q921) solamente las siguientes funciones de Q.922 son utilizadas por Frame Relay:

- Delimitación, alineamiento y transparencia de tramas.
- Multiplexación/Demultiplexación de tramas usando el campo de dirección.
- Inspección de la trama para asegurarse que esta consiste de un número entero de octetos anterior a la inserción del bit cero o después de la extracción del bit cero.
  - Inspección de la trama para asegurarse de que esta no sea muy larga ni muy corta.
  - Detección de errores de transmisión.
  - Funciones de control de congestión.

Estas funciones constituyen una subcapa de la capa de enlace de datos. Estas proveen el servicio de tramas de enlace de transferencia de datos de un suscriptor a otro, sin control de flujo ni control de errores. Antes de esto, el usuario puede escoger entre seleccionar un enlace de datos adicional o funciones de capa de red de extremo a extremo. Estas no son parte del servicio de ISDN. Basado en las funciones principales, ISDN ofrece el relevo de tramas como un servicio de capa de enlace orientado a conexión con las siguientes propiedades:

- Preservación del orden de la trama transferida de un extremo de la red a otro.
- No duplicación de tramas.
- Una pequeña probabilidad de pérdida de tramas.

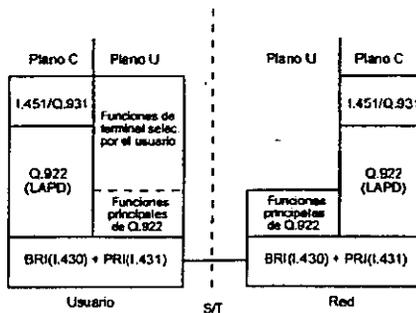


Fig. 3.11 Arquitectura del protocolo de Frame Relay

En el plano de control, Q.922 se utiliza para proveer un servicio de control confiable de enlace de datos, con control de errores y control de flujo, para el envío de mensajes 1.451/Q.931.

Como se puede observar, esta arquitectura reduce al mínimo el trabajo realizado por la red. Los datos de usuario son transmitidos en tramas casi sin ningún procesamiento por los nodos intermedios de la red, dado que solamente se hacen las verificaciones de errores y del enrutamiento basado en el número de conexión. Una trama con error es desechada simplemente, dejando, la recuperación de errores a las capas superiores.

### **Interfaz de la capa física**

La especificación de Frame Relay no establece un tipo específico de cable físico o conector. Dado que Frame Relay fue desarrollado como parte de ISDN, los servicios de Frame Relay pueden ser proporcionados por un cable común UTP (al menos para las tasas bajas de datos).

Típicamente, una unidad DSU/CSU (Data Service Unit/Channel Service Unit) conecta directamente a los cuatro hilos de pares trenzados traídos sobre las premisas por la compañía telefónica. Un ruteador está típicamente conectado a la unidad DSU/CSU por una conexión V.35 o por una conexión estilo RS-232 de alta velocidad. Dependiendo del modelo específico, el ruteador proporciona uno o más puertos los cuales pueden ser directamente conectados a virtualmente cualquier tipo de LAN.

### **III.3.2 Formato de la trama de Frame Relay**

El protocolo principal está basado en la implementación de los acuerdos desarrollados por el comité técnico del Foro de Frame Relay y aceptado por todos los miembros en enero de 1992.

Todos los protocolos bit-síncronos usan una trama como la base en su estructura de transmisión. Los protocolos tales como X.25 y SNA usan derivaciones del procedimiento HDLC o del SDLC (Synchronous Data Link Control) como formato base. El

LAPD es el derivado de HDLC usado en ISDN sobre el cual se basa la trama de Frame Relay.

Dado que Frame Relay no proporciona todas las funciones del protocolo HDLC, varios de los elementos de la trama son innecesarios y se han omitido del formato básico de Frame Relay. El formato de Frame Relay fusiona los campos de direcciones y de control en un simple campo de encabezado, también llamado campo de direcciones. El encabezado de la trama básica de Frame Relay se muestra en la fig. 3.11. Los campos dentro de la trama de Frame Relay son: bandera, dirección CR, EA, FECN, BECN, DE, FCS y campo de información.

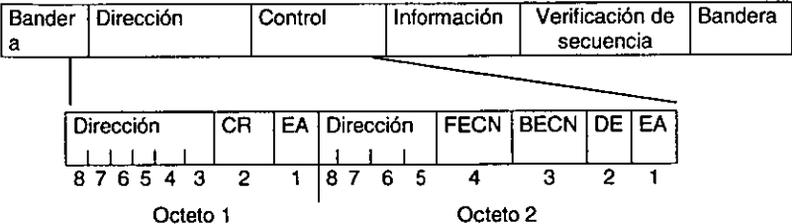


Fig. 3.12 - Encabezado de la trama de Frame Relay

Como ya se mencionó, la trama del protocolo definido para usarse en Frame Relay esta basado sobre el protocolo del acceso al enlace D, LAP-D (Link Access Protocol D), el cual esta definido para ISDN. Bajo Frame Relay, las tramas también son llamadas Unidades de Protocolo de Datos PDU's (Protocol Data Units).

**Bandera**

Utiliza la misma bandera que se explicó en la sección de X.25.

**Dirección**

La dirección en la trama de Frame Relay, consiste de los seis bits más significativos del primer octeto y de los cuatro bits más significativos del segundo octeto del encabezado de la trama. Estos bits están concatenados para producir una dirección de 10 bits.

Esta dirección puede ser de 2, 3 ó 4 bytes de longitud. Representa la dirección de un usuario de Frame Relay y normalmente se refiere como un identificador de conexión de enlace de datos DLCI (Data Link connection identifier). El DLCI denota el puerto donde se localiza el destino.

La mayor parte de la dirección consiste del identificador de la conexión del enlace de datos DLCI (Data Link Connection identifier). El DLCI es equivalente al identificador del circuito virtual VCI (Virtual Circuit identifier) usado en las redes X.25. La dirección completa de 23 bits sirve como un modo de dirección global. La mayoría de los modos de direccionamiento compacto sirven para limitar el encabezado de la trama cuando el usuario no necesita direccionamiento global, por ejemplo, cuando un usuario sólo se conecta con otro usuario local dentro de una organización. Esto es análogo al uso de extensiones telefónicas.

#### Bit de indicación comando/respuesta (CR)

El bit CR (Command/Response) se define en paquetes LAP-D, pero no se usa en Frame Relay, sin embargo, puede ser usado por el usuario pasando transparente a través de la red Frame Relay.

#### Bit de dirección extendida (EA)

El encabezado de la trama básica de Frame Relay consiste de dos octetos que contienen un DLCI de 10 bits. Sin embargo, es posible extender el campo del encabezado para soportar direcciones de más de 10 bits. El bit EA (Extended Address) indica si el octeto en cuestión es el último en el campo del encabezado. Así, para un encabezado de dos octetos, el bit EA se pondrá en "0" en el primer octeto y en "1" en el segundo. El Foro de Frame Relay, recomienda el uso de dos octetos.

#### Bit de notificación de congestión hacia adelante (FECN)

Para notificar al usuario que hay congestión de tráfico en la dirección del octeto que contiene dicho bit, la red le asigna un "1". El bit FECN es controlado por la red, no por el usuario que está transmitiendo y no hay obligación para el sistema final de tomar ninguna consideración de él.

#### Bit de notificación de congestión hacia atrás (BECN)

Este bit es usado por la red para notificar al usuario que se puede presentar congestión para el tráfico de datos, en la dirección opuesta del octeto que lleva el bit BECN. El bit es controlado por la red y no hay obligación para el sistema final tomar ninguna consideración de él.

#### Bit de elegibilidad de desecho (DE)

El bit Discard Eligibility es importante en situaciones de congestión, e indica que la trama deberá ser descartada dando preferencia a otras tramas que no tengan el bit activado. Este bit puede ser activado por la red o por el usuario. Las redes no están restringidas a desechar únicamente tramas con el bit DE activado.

#### Bit indicador de control (DC)

El bit indicador de control DC de DLCI (DLCI/Control Indicator) determina si los seis bits menos significativos van a ser interpretados como los bits menos significativos de DLCI ó como bits de control.

#### Campo de información

El campo de información contiene la información del usuario y consiste de un número entero de octetos. El máximo tamaño de éste campo dependerá de la red, pero el foro Frame Relay recomienda un máximo de 1600 octetos. El tamaño mínimo es de un octeto. El contenido del campo de información pasa sin ser modificado a través de la red y no es interpretado por el protocolo Frame Relay.

#### Verificación de la secuencia de tramas (FCS)

La verificación de la secuencia de trama se utiliza para verificar que la trama se ha recibido sin error y consiste de un campo de dos octetos conteniendo un CRC usando el polinomial para verificación de errores de CCITT  $x^{16} + x^{12} + x^5 + 1$ , que se mencionó a detalle en la sección correspondiente a X.25.

El FCS opera sobre todos los bits de la trama, excluyendo a los de la bandera y del FCS mismo, así como cualquier bit stuffing que se haya colocado. El polinomial generador de FCS es exactamente el mismo que el utilizado por HDLC.

Todos los campos anteriores deberán estar presentes en cada trama de Frame Relay que se esté transmitiendo entre los dos sistemas de los usuarios. Es importante notar que dentro del protocolo de Frame Relay no hay mecanismos para que los usuarios pasen mensajes de señalización entre ellos.

Frame Relay contiene información de señalización, pero está contenida dentro de un canal de administración separado, (una dirección separada o DLCI) y tiene solamente un significado local (del usuario a la red). Esta se conoce como señalización fuera de banda.

Otra importante diferencia entre Frame Relay y HDLC es la omisión de cualquier numeración secuencial de las tramas. Frame Relay no contiene mecanismos para reconocimiento de transmisión de usuario así que no requiere números secuenciales o control de mensajes para confirmar la recepción.

### **Comportamiento del protocolo**

El DLCI permite que los datos que llegan a un nodo Frame Relay sean enviados a través de la red usando un proceso muy simple:

1. Verificar la integridad de la trama usando el FCS, si indica un error se desecha la trama.
2. Consulta el DLCI en una tabla, si no está definido para este enlace, entonces desecha la trama.
3. Reenvía la trama hacia su destino por el puerto o enlace especificado en la tabla.

Cabe mencionar que un nodo Frame Relay no lleva a cabo la enorme cantidad de procesos que ejecuta X.25.

En Frame Relay hay una regla simple: Si existe algún problema, desecha la trama. Las causas más comunes por las que se desechan las tramas son:

- Error de bits
- Congestión en la red.

## **Error de bits**

Cuando ocurre un error en una trama, causado por ruido en la línea, este podría ser detectado usando FCS. A diferencia de otros protocolos como X.25, el nodo que detecta el error no solicita a quien lo envió que corrija el error retransmitiendo la trama: El nodo simplemente descarta la trama y se alista para recibir la siguiente trama. Este descansa en la "inteligencia" del dispositivo (PC o workstation) que originó la trama para reconocer que un error se ha dado y reenvíe la trama.

Si las líneas en la red fueran muy ruidosas, generando gran cantidad de errores, esto implicaría que las capas superiores estarían siendo ocupadas para recuperar tramas, el costo sería elevado y la eficiencia de la red sería desastrosa. Sin embargo, el uso de fibras ópticas con bajos niveles de error hace que la frecuencia de los errores por ruido sea muy espaciada, lo cual no significa ningún problema.

En consecuencia, Frame Relay es útil sólo en líneas limpias; X.25 se desempeña muy bien en líneas con altos niveles de errores.

### **III.3.3 Congestión de red**

La causa más significativa para descartar tramas es la congestión en la red. La congestión ocurre siempre y cuando un nodo de red este recibiendo más tramas de las que puede procesar o cuando éste desea enviar más tramas sobre una línea de las que le permite la velocidad de la misma (line congestion).

En cualquier caso, los buffers de los nodos (memoria temporal para tramas que entran y esperan a ser procesadas o tramas que salen y están en cola para ser enviadas) se saturan y el nodo debe desechar tramas para liberar espacio en los buffers.

Dado que el tráfico en una LAN es extremadamente explosivo o en ráfagas, la probabilidad de que se presente una congestión ocasional es alta. Como resultado, es muy importante que la red Frame Relay tenga un excelente control de congestión para minimizar la ocurrencia de congestión severa y minimizar el efecto de desechar tramas sólo cuando sea requerido.

## Señalización de control

Las redes deben tratar el problema de congestión, un problema que típicamente es controlado en la capa de red. Muchas redes imponen reglas de transmisión que incluyen acuerdos sobre cuanto tráfico puede ser enviado a la red antes de que el flujo de tráfico sea regulado (control de flujo). El control de flujo es un elemento esencial para prevenir la congestión en una red. El congestionamiento es un problema que es evitado por los administradores de red porque ocasiona una severa degradación de la red, tanto en el throughput como en el tiempo de respuesta.

La teoría de colas demuestra que la carga ofrecida para la red puede incrementarse linealmente resultando también un incremento del throughput pero solo en un punto. Sin embargo, se puede alcanzar un punto en donde la carga del tráfico de red alcance un nivel que resulta una rápida caída del throughput, debido al serio congestionamiento y las colas resultantes de los nodos de la red.

### III.3.4 Protocolo LMI

Dado que el protocolo de Frame Relay ha sido definido extremadamente simple, hay varias omisiones desde la especificación básica del protocolo que son consideradas obligatorias para otros protocolos de conmutación de paquetes. Algunas de estas características tales como el control de flujo de datos se pueden omitir sin impactar severamente sobre las operaciones de la red, pero algunas son esenciales para la correcta operación de cualquier red. Estas son las características esenciales que están contenidas dentro de la interfaz de administración local LMI (Local Management Interface).

El protocolo LMI se usa para controlar la conexión entre el usuario y la red siendo responsable de:

- Asegurar que el enlace entre el usuario y la red esté activo.
- Notificar la adición y borrado de PVC's.
- Enviar mensajes de estado para proporcionar la disponibilidad de los circuitos.

Como el protocolo de Frame Relay no esta posibilitado para manejar este tipo de información, un circuito virtual separado se establece entre el usuario y la red sobre el cual pasa esta información conocida como fuera de banda. El LMI también contiene varios procedimientos opcionales los cuales pueden ser utilizados por los proveedores en particular.

El LMI opera como un protocolo de sondeo (polling) entre el usuario y la red. Un mensaje de sondeo y uno de reconocimiento se intercambian a intervalos regulares. Cada vez se intercambia normalmente un mensaje de estado, proporcionando una visión completa del estado actual de los PVC,s, si están activos, inactivos, nuevos o borrados.

Ya que el protocolo de Frame Relay esta basado en PVC no necesita procedimientos para conexión y desconexión de circuitos. Tampoco hay procedimientos para acciones de control de flujo y recuperación por errores. No permite ningún control o administración de la interfaz, ni hay una manera para que el sistema final determine el estado de su conexión. Un aspecto importante en el protocolo de señalización es que ellos están diseñados solamente como complementos del protocolo base de Frame Relay.

Es posible implementar una interfaz de Frame Relay y pasar datos sin el mecanismo de señalización, estos simplemente permiten al usuario obtener mas información sobre el estado de la red y son considerados opcionales. Por esta razón, los mensajes de administración de la información son enviados por un DLCI diferente a los usados por los sistemas extremos para la transferencia de datos. El DLCI número 0 es el que se usa para los mensajes LMI.

El objetivo principal del LMI es proporcionar al usuario el estado y la información de la configuración relacionada a los PVC's operando sobre la interfaz de Frame Relay. El LMI es solamente aplicable a UNI (User-Network Interface). En la fig. 3.12 se muestra la aplicabilidad de LMI en una red de Frame Relay.

## Capítulo IV

### TECNOLOGIA ATM

#### IV.1 Definición y Conceptos

ATM (*Asynchronous Transfer Mode*, o Modo de Transferencia Asíncrono) es una de las más modernas técnicas de conmutación para telecomunicaciones, altamente eficiente, que se puede aplicar a diferentes tipos de información y a diferentes velocidades de transmisión. No es una técnica limitada a redes de telefonía o de datos, sino que permite que una red se utilice para la transferencia de diferentes tipos de señales, de manera simultánea (p. ej. teléfono, datos y video). Es, por lo tanto, la técnica integrada de conmutación que formará la base de la Red Digital de Servicios Integrados de Banda Ancha, B-ISDN (*Broadband Integrated Services Digital Network*). Se considera a ATM como un subconjunto de B-ISDN.

ATM está diseñado para ser flexible, eficiente y tiene la capacidad de soportar las siguientes demandas:

- Utilización del canal o la red por múltiples usuarios simultáneamente.
- Cada usuario con necesidades de telecomunicación diferentes (p. ej. teléfono, transmisión de datos, interconexión a LANs, transmisión de video, etc.) y
- Cada aplicación corriendo a diferentes velocidades de transmisión, es decir, cada aplicación tiene diferentes necesidades de ancho de banda.

Aunque estas capacidades las ofrecen también tecnologías predecesoras (anteriores tecnologías), la diferencia con ATM es que ATM es capaz de hacer ajustes *en cada instante* en la asignación de recursos de red disponibles entre los diferentes usuarios compitiendo por su uso. En lugar de asignar una capacidad fija entre las dos partes que se están comunicando, por el período de una sesión o llamada, ATM se asegura que la capacidad de la línea se utilice de manera óptima, al transportar únicamente la información útil o que se necesita. Por ejemplo, las pausas o silencios en una conversación telefónica no necesitan transmitirse, y en su lugar se pueden enviar pequeños paquetes de datos. Esta asignación dinámica de recursos se logra mediante una tecnología llamada *cell relay switching* (*conmutación de retransmisión de celdas*)

#### IV.1.1 Multiplexaje Estadístico y Cell Relay Switching

ATM se basa en una técnica de multiplexaje estadístico llamada *conmutación de retransmisión de celdas* (cell relay switching). El multiplexaje estadístico es una forma de multiplicar la capacidad efectiva de una red o línea de transmisión, al tomar ventaja de la naturaleza estadística de las ocasiones en que se necesita transportar información. Con este método, es posible suprimir los periodos de silencio para que no se transmitan por la línea. Mientras tanto, las palabras de otras conversaciones pueden transmitirse en esos espacios. Este concepto se aplica también a la transmisión de datos, y de hecho se hace de una manera mas eficiente, ya que se pueden entrelazar los caracteres separados de diferentes textos, o bien transmitir diferentes archivos de datos rápidamente uno detrás de otro.

En la fig. 4.1, se ilustra la técnica del multiplexaje estadístico. Tres usuarios separados (representados por A, B y C) se comunican a través de la misma línea de transmisión. Los tres diferentes circuitos fuentes se conectan al multiplexor y este a su vez a un demultiplexor al otro extremo de la línea.

Lo único que hace este multiplexor es enviar todo lo que recibe de cualquiera de los circuitos directamente a la línea de transmisión. La razón por la que se le llama *estadístico* es porque depende de la probabilidad estadística de que los tres circuitos no quieran transmitir al mismo tiempo. De hecho, el multiplexor está diseñado para poder atender transmisiones simultáneas de todas las fuentes, por periodos cortos de tiempo. Si el tiempo es largo, los espacios de almacenamiento temporal (buffers) se llenan y se desbordan.

Para prevenir la pérdida de información, el sistema debe planearse para que la suma de los *promedios* de flujo de cada canal sea menor que la capacidad máxima de la línea de transmisión. En realidad, la capacidad de la línea debe ser de 1.5 a 2 veces la suma de los flujos (A+B+C) para que el multiplexaje estadístico funcione de manera confiable. De otro modo, se presentan congestionamientos, seguidos algunas veces de largos periodos de holganza del sistema.

Las primeras realizaciones prácticas de este multiplexaje fueron los protocolos de redes de datos, y es el principio sobre el cual están contruidos SNA (Systems Network Architecture, Arquitectura de redes de Sistemas) de IBM y X.25

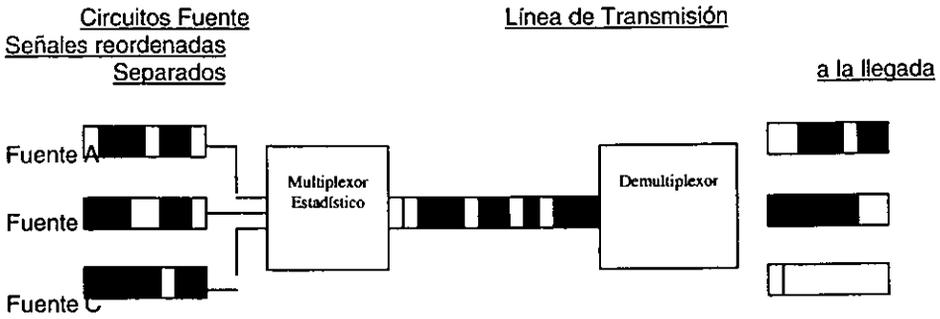


Fig. 4.1. El Principio del Multiplexaje Estadístico

Las redes públicas de voz, a diferencia de las redes de datos, no utilizan este multiplexaje, sino que utilizan la conmutación de circuitos.

*Cell relay* es una forma de multiplexaje estadístico similar en varios aspectos a la conmutación de paquetes, sólo que en lugar de *paquetes* se les llama *celdas* a las unidades básicas de información. ATM tiene un tamaño fijo de celda de 48 octetos mas un encabezado de 5 octetos, dando un total de 53 octetos. Debido a las velocidades que maneja ATM y el corto tamaño de la celda, la duración de la transmisión de la celda también es muy pequeño, lo que permite aplicar un esquema de prioridades para que las aplicaciones muy sensibles a los retrasos (como el video o la voz) tengan acceso a la siguiente ranura de celda disponible. Esto ocasiona una reducción en el *jitter* de la señal. En cambio, las aplicaciones en las cuales no importan las variaciones en el retraso de propagación de la señal, se les puede asignar únicamente las ranuras de celda de baja prioridad (Fig. 4.2)



Fig. 4.2 Las celdas y las ranuras de ATM

#### **IV.1.2 Modos de Transferencia**

Un modo de transferencia indica la manera en la cual la información puede ser transferida (conmutada y transportada) de un lado de la red a otro. Existen tres técnicas:

*Modo de Transferencia Síncrona (STM, Synchronous Transfer Mode).* Este método se utiliza en sistemas de transmisión de alta velocidad. Bajo este esquema, la capacidad de la línea (bitrate) se encuentra estructurada en un patrón estrictamente regular y repetitivo. Por ejemplo, una línea de 155 Mbit/s, en realidad se encuentra formada por una trama de 2430 bytes u octetos, repetida 8000 veces por segundo. No existen espacios libres entre tramas, así que se puede esperar la misma parte de la trama en el mismo lugar cada 125 microsegundos, lo cual hace que el sistema sea síncrono.

*Modo de Transferencia Plesiócrona (Plesiochronous Transfer Mode)* En este caso el sistema no es del todo síncrono, pero pretende que sí lo es. Para minimizar el efecto de los errores que inevitablemente ocurren por la falta de sincronía, parte de la capacidad de la línea se desperdicia a propósito para que exista una pequeña holgura en el sistema, y de esta manera el usuario final no sufra de las consecuencias del comportamiento errático.

*Modo de Transferencia Asíncrono.* Sólo se envían tramas de información (celdas), cuando se necesitan. Por ejemplo, sólo se transmiten los caracteres que se introducen desde una terminal cuando se presiona una tecla. Mientras tanto no se envía nada. En contraste, los sistemas síncronos envían tramas todo el tiempo, inclusive tramas vacías.

#### **IV.1.3 Interfaces de una Red ATM**

En una red ATM existen principalmente dos tipos de interfaces, la interfaz red-usuario y la interfaz red-red. Algunos autores consideran una tercera interfaz, que sería algo así como un puente o gateway entre dos redes ATM diferentes, sin embargo, aquí consideraremos únicamente las dos primeras:

- **ATM UNI (User-Network Interface).** Es la especificación técnica que permite a diferentes equipos de usuario, de diferentes fabricantes, se comuniquen a través de

una red de aún otro fabricante. Es la interfaz que se utiliza entre el equipo ATM del usuario y un switch, crossconnect o multiplexor ATM.

- ATM NNI (Network-network Interface). Es la interfaz que se usa entre nodos dentro de la misma red, o entre diferentes subredes. La NNI tiene la finalidad de estandarizar el cómo nodos de diferentes fabricantes pueden comunicarse entre sí, de manera que se pueda formar una red ATM a partir de nodos individuales.

## IV.2 Canal Virtual y Ruta Virtual

A la conexión que establece ATM entre dos usuarios finales, a través de la red, se le conoce como *canal*. A diferencia de la red telefónica y otras basadas en la conmutación de circuitos, los canales ATM comparten la misma conexión física y el mismo ancho de banda, por medio de la técnica de multiplexaje estadístico. De esta manera, los usuarios ven como si tuvieran un canal físico dedicado sólo a ellos. Por esta razón se les conoce como *canales virtuales (VC)* o algunas veces como canales lógicos.

Un canal virtual que se extienda a través de toda la red (en la capa ATM) es en realidad una *conexión de canal virtual (VCC)*. Esta conexión se puede formar de varios *enlaces de canal virtual* más pequeños, que se van conectando entre sí para formar el VCC completo. Además, comparte los mismos puntos iniciales, finales y comparte también una *conexión de ruta virtual (VPC)*. El concepto de ruta virtual (VP) es fundamental en el diseño de redes ATM, y su función es como la de un saco de cartas. De la misma manera como el saco ayuda a manejar un conjunto de cartas que tienen un destino similar, así ayuda la *ruta virtual* a reducir la carga de los nodos ATM al permitir que se agrupen los *enlaces de canal virtual*. Por lo tanto, una *ruta virtual (VP)* transporta varios enlaces, que por su lado pueden concatenarse a otros enlaces de canal virtual para formar un VCC.

Al igual que los canales virtuales, las rutas virtuales pueden clasificarse en *conexiones de ruta virtual (VPC)* y enlaces de ruta virtual, donde un VPC se compone de la concatenación de uno o más enlaces de ruta virtuales. Estos últimos se derivan directamente de una ruta física de transmisión.

Todos los canales virtuales de una red ATM, ya sean VCCs o VPCs, se pueden clasificar de acuerdo a si son *circuitos virtuales permanentes* o *conmutados* (PVC o SVC). Un circuito virtual permanente (PVC) normalmente sólo se establece por medio de un operador humano, con comandos manuales, y es un circuito permanentemente conectado entre dos o más puntos finales. En cambio, un circuito virtual conmutado (SVC) se establece cada vez que se solicita una nueva llamada o conexión.

#### **IV.2.1 Establecimiento de la Conexión de Canal Virtual (VCC)**

Las conexiones de circuito virtual y las de ruta virtual pueden usarse tanto para transportar información de usuario como para llevar información de señalización referente a la propia red. Cuando es este último caso, a las conexiones se les llama *canales virtuales de señalización* (SVC también, o Signalling VC para no confundirlos con los circuitos virtuales conmutados). Un ejemplo de mensaje de señalización podría ser 'establecer conexión virtual número 1 entre los usuarios A y B', o bien podría ser 'limpiar la conexión entre A y B'.

Como se mencionó anteriormente, los PVCs se establecen por medio de un operador humano, y son conexiones que están definidas por configuración de la red y siempre existirán entre dos o más puntos finales.

Cuando se establece un SVC, en cambio, primero se lleva a cabo una negociación entre el equipo del usuario y la red a través del *canal virtual de señalización UNI*. Esta negociación establece los puntos finales de la conexión, las características técnicas que se requieren (p.ej. tipo de conexión, tasa de transmisión, prioridad y calidad de conexión). Durante la negociación, se establecen rutas virtuales y conexiones entre los diferentes nodos, y los números de referencia de estas conexiones, la combinación de *identificadores de ruta virtual* (VPIs) y los *identificadores de conexión virtual* (VCIs) se confirman a través del canal de señalización. Entonces estos valores (Los VPI y los VCI) se colocan en el encabezado de todas las celdas que se envían a través de la conexión final.

## IV.2.2 Identificadores de Canal Virtual (VCIs) e Identificadores de Ruta Virtual (VPis)

En la fig. 4.3 se muestra cómo se puede subdividir una conexión física en varias rutas virtuales diferentes, cada una con un VPI único. Cada una de estas rutas virtuales puede subdividirse a su vez en distintos canales virtuales, cada uno con su identificador VCI. Para poder especificar un canal virtual dentro de una conexión física en particular, se debe proporcionar tanto el VPI como el VCI. Esto es porque, mientras que los VPis son únicos para cada interfaz, los VCIs no. Para cada ruta virtual, la numeración de los canales virtuales puede comenzar en '1'. La combinación VPI/VCI sí es única y suficiente para identificar cualquier conexión activa en la interfaz.

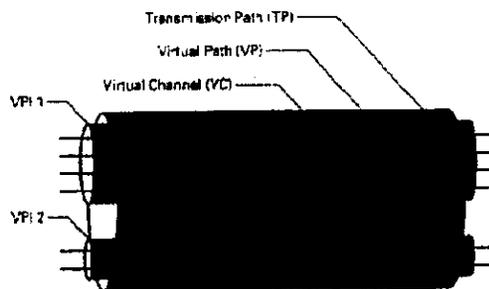


Fig. 4.3 Rutas y Canales Virtuales

Un multiplexor ATM permite que varios canales virtuales de diferentes rutas virtuales se junten en una sola. Un crossconnect ATM permite que se reordenen las rutas virtuales sin que se afecten los canales virtuales que contienen. Un switch ATM completo tiene la capacidad no sólo de interconectar rutas virtuales, sino también de conmutar canales virtuales de diferentes rutas virtuales.

## IV.3 Formato de la Celda ATM

El modo de transferencia asíncrono utiliza celdas de tamaño fijo, que consisten de un encabezado de 5 octetos y un campo de información de 48 octetos (fig. 4.4). El hecho de que las celdas sean de un tamaño constante tiene varias ventajas, de las cuales las más importantes son que el tamaño pequeño de estas celdas reduce el tiempo de



*Formato del Encabezado:* La fig. 4.4(a) muestra el formato del encabezado en la interfaz de usuario-red (UNI), mientras que la fig. 4.4(b) muestra el formato de la celda interno para uso de la red (NNI). Para uso interno no es necesario proveer control de extremo a extremo, no se tiene el campo de control genérico de flujo. En lugar de eso, se expande el campo identificador de la ruta virtual de 8 a 12 bits, para manejar el tráfico generado tanto por los usuarios como por la administración de la red.

El *Control Genérico de Flujo* (GFC) únicamente aparece en el formato de encabezado de la interfaz usuario-red. Este campo puede servir para ayudar al cliente a controlar el flujo de tráfico para diferentes calidades de servicio (QOS), y puede utilizarse en una de dos maneras, para aliviar condiciones pico de sobrecarga en la red. En la primera, para configuraciones punto a punto, el GFC puede controlar el flujo desde un TE individual. En la segunda, para configuraciones punto a multipunto, el GFC proporciona control de flujo adicional al ya existente. Sin embargo, este campo también puede utilizarse como control de acceso al medio cuando se tienen múltiples terminales a nivel de interfaz usuario-red.

La recomendación I.150 lista como requerimiento que el mecanismo de GFC permita a todas las terminales trabajar a sus capacidades aseguradas. Esto incluye tanto a terminales de tasa de bits fija (CBR) como a las de tasa de bits variable (VBR), que tengan un elemento de capacidad garantizada.

El *Identificador de Ruta Virtual* (VPI) es un campo de ruteo para la red. Como ya se ha mencionado, tiene 8 bits en la interfaz usuario-red (UNI) y 12 bits en la interfaz red-red (NNI), lo que permite que se soporten más rutas virtuales para uso interno de la red.

El *Identificador de Canal Virtual* (VCI) se utiliza para ruteo desde y hasta el usuario final.

El campo de tipo de *Tipo de Carga* indica qué tipo de información se está transportando en el campo respectivo. En la tabla 4.3.1 se muestra el significado de los bits de este campo (también se les conoce como bits PT, por Payload Type). Un cero en el primer bit indica que se tiene información de usuario, es decir información de la siguiente capa más alta. En este caso, el segundo bit indica si es que se experimentó

congestión en algún nodo, y el tercer bit, conocido como el bit indicador de usuario-ATM a usuario-ATM (AAU) se considera como un campo donde puede transportarse información entre usuarios finales. También se utiliza en la capa de adaptación de ATM (AAL).

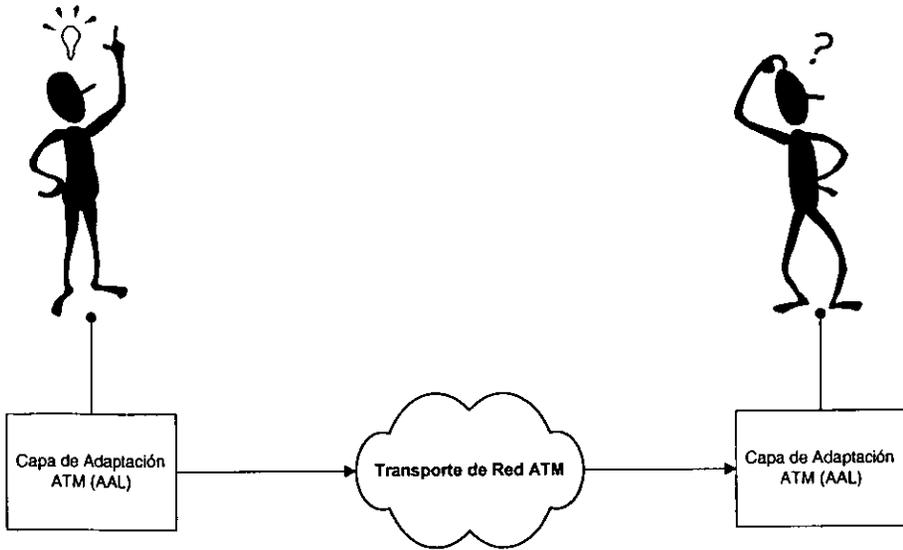
Si tenemos un valor de 1 en el primer bit indica que la celda contiene información de administración o mantenimiento. este indicador permite que se inserten celdas de control en un canal virtual de un usuario, sin que se afecte su proceso de transferencia de información. Por lo tanto, puede proveer control dentro del mismo ancho de banda.

La *Prioridad de Pérdida de Celda (CLP)* se utiliza para ayudar a la red a decidir qué hacer en caso de congestión. Un valor de 0 indica que la celda es de relativamente mayor prioridad, y que no debe descartarse a menos que no quede otra alternativa. Un valor de 1 indica que esta celda se puede eliminar por la misma red. Por medio de este indicador se puede insertar información adicional en la red, si colocamos el CLP en 1. esto indicaría que la información se transportará sólo si no hay congestión. la red también puede colocar este bit en 1 si la celda esta violando algún acuerdo de tráfico. En este caso, lo que hace el conmutador ATM es que, cuando se da cuenta que esto sucede, pero que puede hacerse cargo, procesa la celda y le cambia el estatus del CLP. Más adelante en la red, si se vuelve a encontrar una congestión, la celda ya esta marcada para eliminarse y se le da preferencia a celdas que si cumplen con los límites de tráfico preestablecidos.

#### **IV. 4 Capas de Adaptación AAL**

La capa de adaptación AAL es la más importante parte funcional de ATM, esta capa proporciona la conversión de información dentro de un formato que pueda viajar a lo largo de la red ATM.

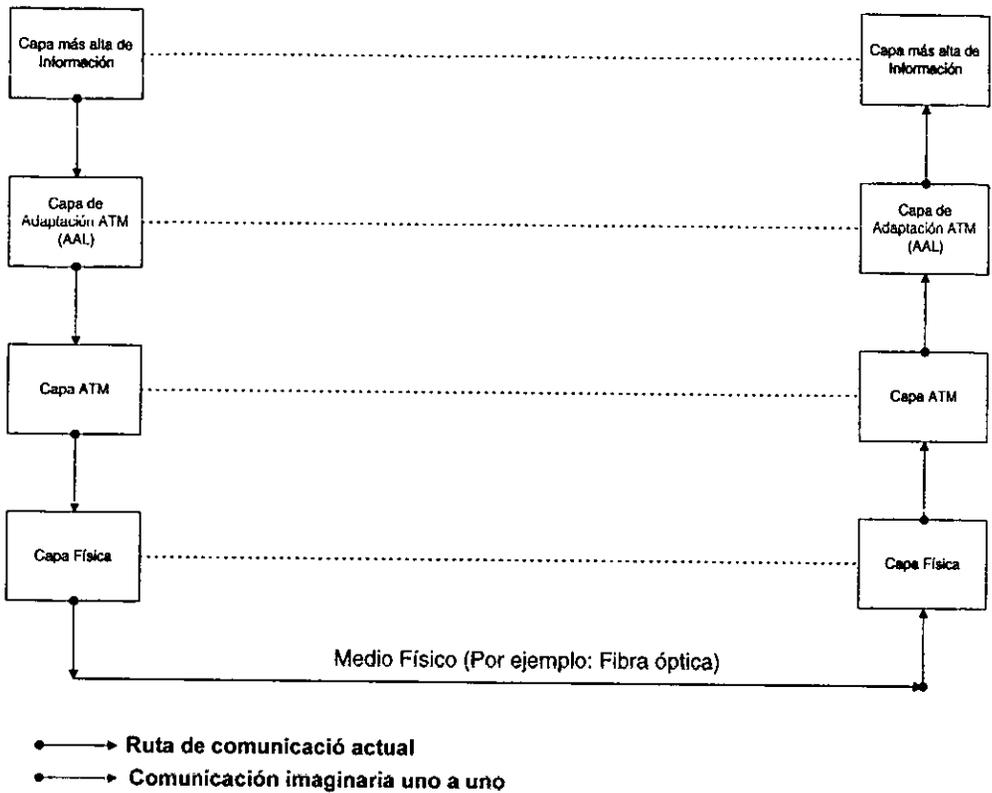
La funcionalidad de AAL es proporcionada en lugar del transporte de red ATM, que podemos observar en la figura IV.4.1 Este proporciona (en el envío final) para la conversión de un teléfono, datos o bien otras señales de comunicación dentro del formato de celda ATM. Para la recepción final, AAL invierte la conversión, regresando las celdas dentro de la señal original.



**Fig. 4.5** Función de la Capa de Adaptación de ATM (AAL)

En la fig. 4.5 notamos esta situación pero en la forma de los modelos en niveles de protocolo. El más alto nivel de información es pasado hacia la capa ATM de adaptación (AAL) que convierte esto dentro de una forma en la cual el transporte de red ATM pueda trabajar con él.

Por otro lado la capa de adaptación ATM ejecuta conversiones de las capas más altas de información dentro de celdas para la reconstrucción de la señal original. AAL debe asegurarse que todas las celdas están recibiendo, están en el orden correcto y que la tasa de error en las celdas recibidas es aceptable, especificando la naturaleza de la información que provee el usuario. Para las señales de información que son sensibles a las variaciones en los retrasos de celdas (CDV), la AAL proporciona funciones de buffer y reloj a fin de asegurarse que las señales enviadas a los dispositivos destino están libres de CDV. Este CDV para el caso de señales telefónicas se manifiesta con problemas de jitter.



**Fig. 4.6** Modelo de Referencia de Protocolo de la Capa de Adaptación ATM (AAL)

Por otro lado ATM requiere transferir información entre protocolos que no están basados en ATM. Dos ejemplos son: PCM (Modulación por Código de Pulsos, Pulse – Code Modulation) para voz y LAPD ( Link Access Procedure on the D Channel). PCM para voz es un aplicación que produce una cadena de bits para una señal de voz. Para poder ejecutar esta aplicación sobre ATM se requiere ensamblar los bits PCM dentro de las celdas, de manera que se puedan transmitir y leer los datos fuera de línea para permitir un flujo de bits constante hacia el receptor. LAPD es el protocolo estandar para el control del enlace de datos en ISDN y B-ISDN. Es necesario segmentar una estructura LAPD dentro de varias celdas durante la transmisión y reensamblar la estructura original que se encuentra en las celda al momento de recibirlas.

Es posible mediante el uso de la capa AAL diferenciar y manejar diferentes tipos de información.

#### **IV.4.1 Servicios**

La ITU-T en su norma I.362 proporciona la siguiente lista con ejemplos generales de servicios que brinda AAL:

- Manejo de transmisión de errores
- Segmentación y re-ensamblado , para habilitar bloques grandes de información que son proporcionados en el campo de información de las celdas ATM
- Manejo de pérdidas y condiciones de error en la inserción de celdas
- Control de flujo de datos y de tiempos

Para disminuir el número de diferentes protocolos AAL especificados que satisfacen diversas necesidades, la ITU-T definió cuatro clases de servicios que cubren un amplio rango de requerimientos (fig. 4.7). Esta clasificación esta basada en las siguientes necesidades: sincronización entre la fuente y el destino, una tasa constante de bits, y si la transferencia es orientada. Un ejemplo de un servicio de clase A es la emulación de circuitos (circuit emulation). En este caso se utiliza una tasa de bits constante que requiere el mantener una sincronización (entre la fuente y el destino) así como una trasferencia orientada a conexión. Un ejemplo de servicio clase B es el video con tasa de bits variable, como puede utilizarse en una videoconferencia. Aquí la aplicación es orientada a conexión y la sincronía en la transmisión es muy importante, pero la variación en el flujo de bits depende de la actividad en la escena. Las clases C y D corresponden a las aplicaciones que transfieren datos, en ambos casos el flujo de bits puede variar y no se requiere una sincronía en las transmisiones. Las diferencias en los flujos de datos son manejadas por los sistemas finales usando buffers. Las transferencias de datos pueden ser orientadas a conexión (Clase C) o no orientadas a conexión (clase D).

	Clase A	Clase B	Clase C	Clase D
Sincronización entre la Fuente y el Destino	Requerida	Requerida	No requerida	No requerida
Tasa de Bits	Constante	Variable	Variable	Variable
Modo de Conexión	Orientada a Conexión	Orientada a Conexión	Orientada a Conexión	No orientada a conexión
Protocolo AAL	Tipo 1	Tipo 2	Tipo 3, Tipo 5	Tipo 3/4

**Fig. 4.7** Clasificación de Servicios para AAL

#### IV.4.2 Protocolos AAL

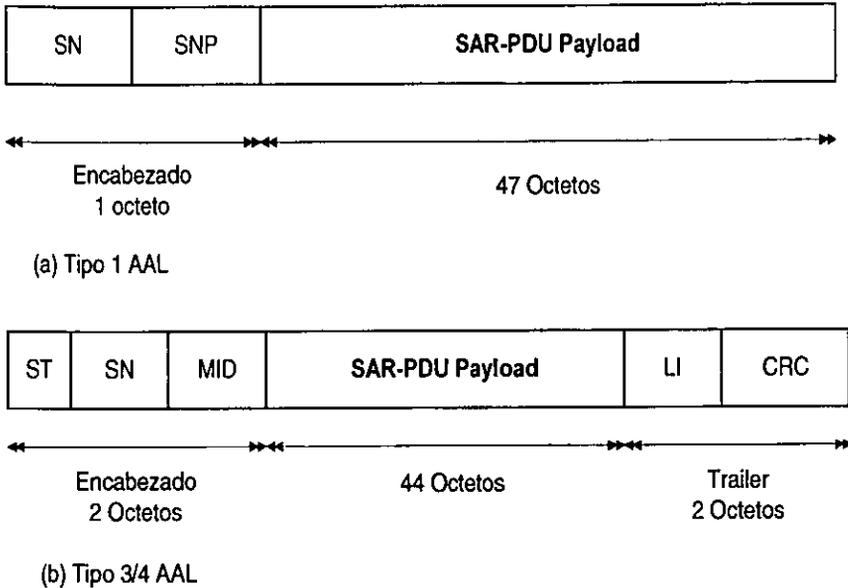
Para soportar este tipo de servicios, un conjunto de protocolos debe ser definido en el nivel AAL. La capa AAL se encuentra organizada en dos subcapas lógicas: la subcapa de convergencia (CS) y la subcapa de segmentación y reensamblaje (SAR).

La subcapa de convergencia provee las funciones necesarias para soportar aplicaciones específicas usando AAL, donde cada aplicación se agrega al AAL en un punto de acceso a servicio (SAP), que es simplemente la dirección de la aplicación. Esta subcapa es dependiente del servicio. El SAR es responsable de empaquetar la información recibida de la CS dentro de las celdas a transmitir y de desempacar la información en el extremo final.

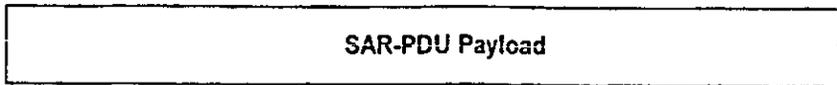
Para la capa AAL, cada celda consta de un encabezado de cinco octetos y un campo de información con cuarenta y ocho octetos. Sin embargo la SAR debe encapsular sus encabezados y sus trailers además de la información de la subcapa CS dentro de bloques de cuarenta y ocho octetos.

Inicialmente, ITU-T define un tipo de protocolo para cada clase de servicio ( tipo 1, tipo 2, tipo 3 y tipo 4). Actualmente cada tipo de protocolo esta formado por dos

protocolos, uno en la subcapa CS y uno en la subcapa SAR. Recientemente los tipos 3 y 4 se unieron, dando como resultado la definición de el tipo 3/4, y un nuevo tipo, el tipo 5. La fig. 4.7 muestra que servicios soporta cada tipo de protocolo, la fig. 4.8 muestra los formatos de la Unidad de Datos de Protocolo (PDUs) en el nivel SAR, excepto para el tipo 2 que aún no se define y la tabla IV.4.2.2 lista los detalles de las definiciones funcionales actuales de los cuatro tipos de protocolos AAL.



**Fig 4.8** Formatos de la Unidad de Datos de Protocolo



(c) Tipo 5 AAL

48 Octetos

SN = Número de secuencia (4bits)

SNP= Protección de número de secuencia (4bits)

ST = Tipo de Segmento (2 bits)

MID = Identificador de Multiplexaje (10bits)

LI = Indicador de Longitud (6bits)

CRC- Verificador de Redundancia Cíclica (10bits)

**AAL Tipo 1.-** Para la operación del tipo 1, se manejan tasas de bits constantes. En este caso la única responsabilidad del protocolo SAR es empaquetar los bits dentro de celdas para su posterior transmisión y desempaque en la recepción. Cada bloque de bits es acompañado por un número de secuencia de manera que los PDUs con error puedan ser rastreados. El campo de protección de número de secuencia representa un código de error para la detección de errores y posiblemente realiza correcciones en el campo de número de secuencia.

No han sido definidos CS PDU para el tipo 1. Las funciones de la subcapa CS para el tipo 1 principalmente tiene que ver con reloj y sincronización, y no es necesario un encabezado CS separado.

**AAL Tipo 2.-** El tipo 2 es diseñado para aplicaciones análogas como video y audio, que requieren información en tiempos determinados pero no requieren una tasa constante de bits.

**AAL Tipo 3/4.-** Las especificaciones iniciales del tipo 3 y 4 de AAL fueron muy similares en términos del formato PDU y funcionalmente. En base a esto se decide con la colaboración de ITU-T combinar ambos tipos y formar solo una especificación de protocolo para las capas SAR y CS, este tipo es conocido como tipo 3/4.

Los tipos de servicios proporcionados por el tipo 3 de AAL se caracterizan por lo siguientes puntos:

1. El servicio puede ser orientado a conexión o bien orientado a no conexión, dependiendo del caso, cada bloque de datos presentado en la capa SAR (SAR, services data units o SDU) se trata de forma independiente. Para el caso de orientado a conexión es posible definir múltiples conexiones lógicas SAR sobre una sola conexión ATM.
2. El servicio puede ser modo-mensaje o modo-flujo. El servicio de modo-mensaje transfiere tramas de datos de modo que cualquier protocolos OSI y aplicaciones que se encuentren dentro de estas categorías, en particular LAPD o Frame Relay puedan ser modo-mensaje. Un solo bloque de datos de una capa superior de AAL se transfiere en una o más celdas.

El servicio de modo-flujo soporta transferencias continuas de datos de baja velocidad con bajos retardos. La información se presenta a la AAL en bloques de tamaño constante, que puede ser tan pequeño como un octeto. Cada bloque se transfiere en una celda.

El tipo 3 de AAL proporciona estos servicios de transferencia de datos aceptando bloques de datos desde la siguiente capa más alta y transmitiendo cada bloque hacia el usuarios AAL destino. Dado que la capa ATM limita la transferencia de datos a un tamaño de 48 octetos, la capa AAL debe proporcionar al menos las funciones de segmentación y reensamblado.

Cada bloque de datos de la capa superior se encapsula en un PDU de la subcapa CS.

**Tipo 5 AAL.-** El protocolo de más reciente ingreso a las especificaciones AAL es el protocolo tipo 5. Este protocolo se introduce para proporcionar las facilidades de transporte para protocolos de capas superiores que son orientados a conexión. Si se asume que las capas superiores cuidan del manejo en las conexiones y que la capa

ATM produce mínimos errores , entonces la mayoría de los campos del SAR y de CPCS PDUs no son necesarios.

El tipo 5 fue adicionado para:

- Reducir sobrecargas en los procesos de protocolos
- Reducir sobrecargas en las transmisiones
- Asegurar compatibilidad para los protocolos de transporte existentes.

	<b>Servicios que ofrece</b>	<b>Funciones</b>	<b>Funciones SAR</b>	<b>Funciones CS</b>
Tipo 1	Transferencia del SDU con un rango constante de bits. Transferencia de la información por tiempo entre la fuente y el destino. Indicación de error ó información errónea no recuperada por el tipo-1.	Segmentación Reensamblaje. Manejo de la variación retardo de celda. Manejo de pérdidas de celdas. Monitoreo de la información de usuario para errores de bits y una posible corrección.	Mapeos entre PDU CS y PDU SAR. Indica la existencia de la función CS. Numeración de secuencia. Protección a errores.	Manejo de variaciones en retrasos con celdas. Manejo en pérdidas y celdas mal insertadas. Para algunos servicios, recuperación de reloj para el receptor. Transferencia de la estructura de la información. Envío de corrección de errores para una buena calidad en video y audio. Reporte de estatus de desempeño extremo a extremo.

	Servicios que ofrece	Funciones	Funciones SAR	Funciones CS
Tipo 2	Transferencia del SDU con un rango variable de bits (VBR). Transferencia del tiempo de información entre fuente y destino. Indicación de información errónea o perdida no recuperada por el tipo-2.	Segmentación Reensamblaje. Manejo de la variación de retardo de celdas. Manejo de pérdidas de celdas. Monitoreo de la información de usuario para errores de bits y una posible corrección.	En estudio	En estudio
Tipos 4	Servicio de modo de mensaje. Servicio de modo de flujo. Operación no asegurada.		Segmentación Reensamblaje Detección de errores. Integridad en la secuencia. Multiplexaje.	Detección y manejo de errores. Indicación de tamaño de buffer.
Tipo 5	Modo de conexión orientada. Flujo de bits variable.	No requiere relación coordinada entre la fuente y el destino.	Manejo con información de congestión. Manejo de información con pérdida de prioridad	Detección de errores y "reellenos". Manejo de información de congestión. Manejo de información con pérdida de prioridad.

**Tabla 4.1**

#### **IV.5 Control de Tráfico y Congestión**

El control de tráfico es un tema de estudio muy importante para cualquier red de comunicaciones que tenga recursos compartidos. Si no se tiene control sobre los requerimientos de estos recursos (buffer, ancho de banda, o incluso procesadores) la eficiencia y tasa de transmisión de la red se ve degradada seriamente. El control de tráfico es necesario tanto para garantizar la calidad de servicio requerida por los usuarios como para asegurar la utilización eficiente de los recursos de la red. Los mecanismos de este

tipo de control se deben implementar dentro de los sistemas de conmutación y en los protocolos de las capas más altas de la red.

Existe gran conciencia del problema de tráfico en ATM, y prueba de ello es la recomendación I.371 de la ITU-T, que es un intento de formular un lineamiento general de los principios y funciones del control de tráfico, y la investigación sobre este tema continúa en el grupo de administración de tráfico del foro ATM. Lo que se presenta aquí se deriva precisamente de la recomendación de la ITU-T y las especificaciones del foro.

#### **IV.5.1 Conceptos generales**

Para poder comprender el marco de referencia donde actúa el control de tráfico, es necesario primero comprender los principios que rodean los siguientes conceptos:

- Calidad del Servicio (QOS)
- Compartición estadística de recursos vs. aislamiento
- Niveles de Control
- Controles reactivos y preventivos.

Las funciones específicas de control de tráfico son las siguientes:

- Control de admisión de conexión
- Control de parámetros de uso y de la red
- Control de Congestión

#### **Calidad de Servicio**

Como ya se ha mencionado, el servicio básico de ATM es el transporte secuencial de celdas de extremo a extremo. El servicio se inicia por una petición de usuario de una conexión virtual, la cual puede admitirse o rechazarse por la red. El Grado de Servicio (GOS) tiene que ver con el tráfico *ofrecido* en términos de la probabilidad de bloqueo al nivel de admisiones o rechazo de conexión. Después de que se acepta una conexión, las celdas que se transportan pueden experimentar dos tipos básicos de deterioro o daño en la red: retraso y pérdida. En cambio, la Calidad del Servicio (QOS) se refiere al conjunto de parámetros tal como retraso de celdas, variación de retraso y la tasa de pérdida de celdas, los cuales pertenecen a los deterioros que experimenta el tráfico que se *transporta*

por la red. Estos parámetros tienen que ver con la percepción del usuario del servicio de la red.

Mientras que el QOS tiene significado desde la perspectiva de los usuarios en el punto de acceso al servicio, el desempeño de la red se define desde el punto de vista del proveedor de la red para diferentes puntos dentro de la misma. A nivel de llamada, los parámetros para medir este desempeño pueden ser el retraso en el establecimiento de la conexión, el retraso en la liberación de la conexión, y la probabilidad de bloqueo. A nivel de la celda, los parámetros pueden incluir la tasa de errores en las celdas, tasa de pérdida, tasa de inserción errónea, retraso de la celda de extremo a extremo, y variación del retraso de la celda.

En ATM, el rendimiento de la red también puede verse afectado por la contención de recursos limitados. Las consecuencias de una congestión no controlada se muestra en la fig. 4.8.1. Como ATM es tanto orientada a conexión como orientada a paquete, este tipo de redes pueden tener problemas de congestión tanto a nivel de conexiones como a nivel de celdas. A nivel de conexiones, los procesadores de llamadas se preocupan por intentos fallidos de establecimiento de llamada. A nivel de celdas, los enlaces de transmisión se saturan con tráfico y los buffers se desbordan. Por lo tanto, la congestión se hace patente por medio de un incremento dramático en el bloqueo de celdas, retrasos, y aumento de la tasa de pérdida. El control de congestión intenta detectar y reaccionar para minimizar la intensidad, alcance y duración de estos efectos.

### **Compartición Estadística de Recursos Vs. Aislamiento**

El control de tráfico es difícil en ATM porque existe una contraposición natural entre dos objetivos mutuamente excluyentes: la compartición estadística de recursos para aumentar la eficiencia y el aislamiento entre flujos de tráfico para la protección del QOS. Se puede conseguir un aumento en la eficiencia al multiplexar de manera estadística conexiones VBR en las cuales la tasa total de pico excede la tasa de transmisión del enlace físico, siempre y cuando la tasa total promedio sea menor que la del enlace. Si se tienen muchos flujos de tráfico de manera independiente, entonces la probabilidad de que su tasa total instantánea exceda la del enlace, será muy pequeña. Es deseable entonces

mantener un alto factor de actualización y maximizar el grado de compartición estadística de los recursos de la red.

El problema que ocasiona la compartición estadística es la posibilidad de que el QOS de una conexión se vea degradada por el tráfico existente en otras conexiones. Por ejemplo, una ráfaga repentina en un determinado flujo pudiera llenar el buffer del multiplexor y por lo tanto incrementar los retrasos de celda para todos los demás flujos. El problema de desbordamiento de buffer y retrasos excesivos en el encolamiento se vuelve más grande en cuanto aumenta la carga de la red. Por lo tanto, es preferible mantener un factor de utilización bajo o proveer aislamiento entre flujos de tráfico para aminorar el efecto de las ráfagas mencionadas anteriormente. Como se puede observar, esta última conclusión es totalmente contraria a la de compartición estadística de recursos.

Para intentar romper esta contradicción, se pueden manejar prioridades. Las prioridades de retraso dictan el orden en el cual las celdas que están encoladas se deben programar para transmitirse por un enlace compartido; las prioridades de pérdida especifican la utilización de buffers compartidos. Esto trae como consecuencia que el aumento de tráfico de baja prioridad no afecta mayormente al de alta prioridad. Sin embargo, un aumento de tráfico en el de alta prioridad, sí trae como consecuencia un aumento muy grande de los tiempos de retraso del tráfico de baja prioridad. Se debe entonces decidir qué clase de servicio se debe ver beneficiado a costa de los demás.

La red debe operar necesariamente en un punto intermedio entre la utilización alta y baja, dependiendo de la importancia relativa de utilización eficiente vs. protección del QOS. El punto de operación también depende de la predictibilidad y número de veces que ocurren ráfagas. Entre más impredecible sea el tráfico y más ráfagas tenga, se debe disminuir más el factor de utilización.

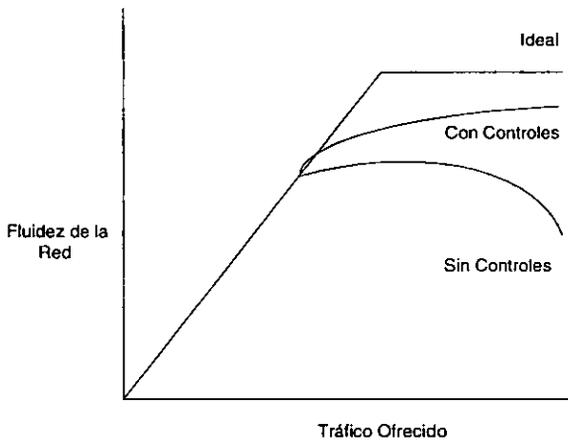
### **Niveles de Control**

El flujo de tráfico en ATM se puede analizar a diferentes niveles:

- Llamada (posiblemente con conexiones múltiples)
- Conexiones de Ruta Virtual

- Conexiones de Canal Virtual
- Ráfagas (que consisten de celdas consecutivas)
- Celdas Individuales

El control de tráfico consiste de un conjunto de mecanismos que se pueden aplicara diferentes entidades de tráfico al mismo nivel. Cada mecanismo tiene una escala de tiempo característica, como se muestra en la fig. 4.9 Los que operan en celdas individuales son los más instantáneos porque las decisiones de control dependen únicamente de las condiciones locales dentro de un switch. Por ejemplo, la eliminación selectiva de celdas depende del nivel de congestión en los buffers del switch. Por el contrario, otros mecanismos operan a través de la red en la escala de tiempo de retrasos de propagación de extremo a extremo. Este tipo de mecanismos involucran el paso de información en un solo sentido entre dos puntos a lo largo de una conexión virtual. Un ejemplo es el algoritmo EFCL que se verá en el control de congestión. Existen otros mecanismos que operan en escalas de tiempo aún más grandes, donde se involucra el intercambio bidireccional de mensajes y respuestas. Un ejemplo es el Control de Admisiones de Conexión (CAC).



**Fig. 4.9.** Efectos de la Congestión sin Control de Tráfico

## **Controles Reactivos y Preventivos**

A pesar de que ATM se puede comportar tanto como una técnica orientada a paquetes como una orientada a conexión, los mecanismos convencionales de retroalimentación que se utilizan en las redes orientadas a paquetes no se pueden aplicar aquí, por dos razones principales: Primero, la retroalimentación no es apropiada para fuentes de tráfico de tiempo real, que en general no se controlan por la red, y segundo, la eficiencia del control por retroalimentación está limitada por el tiempo de propagación. En una red ATM, el tiempo necesario para transmitir una celda es mucho menor que el tiempo que toma detectar una congestión y notificar a la fuente, para que ésta reaccione y tome las medidas pertinentes.

Por las razones anteriores, las redes ATM deben poseer controles preventivos, que aseguren que cada conexión permanezca dentro de los límites que utilizó la red para asignar recursos durante el establecimiento de la misma. Los métodos preventivos tienen principalmente dos funciones: el control de admisión de conexión y el control de los parámetros de uso (UPC) para regular la cantidad de tráfico que entra a la red. Incluyen la eliminación selectiva de celdas, EFCI, y reconfiguración dinámica de ruteo.

### **IV.5.2 Control de Admisión de Conexión (CAC)**

CAC junto con UPC, es de las funciones principales del control preventivo de tráfico en ATM. Al igual que en una red telefónica conmutada por circuitos, el trabajo de CAC consiste en:

- Negociar con los usuarios un nuevo requerimiento de conexión.
- Decidir la admisión o el rechazo de la nueva conexión.
- Asignar los recursos de la red que sean apropiados.

Puesto que una llamada de B-ISDN puede involucrar una o más conexiones virtuales, se determina la admisión o el rechazo por cada conexión virtual. Las solicitudes de conexión (y la renegociación de los parámetros) se hacen a través del intercambio de información de señalización.

Sólo se admite una nueva conexión si se estima que ésta se puede establecer con el QOS solicitado sin degradar el QOS de conexiones ya existentes. Para poder determinar esto, la solicitud de la nueva conexión se transmite a lo largo de toda la ruta. Cada nodo decide entonces si puede asignar los recursos necesarios. La solicitud se acepta sólo si es aceptada por cada nodo. La aceptación de la nueva conexión implica que se está de acuerdo con un contrato de tráfico que especifica las obligaciones entre el usuario y la red. Una vez que se establece, los parámetros de una conexión virtual sólo se pueden cambiar a través de una renegociación entre el usuario y la red.

### **Contrato de Tráfico**

El punto de entrada para este contrato es la descripción del tráfico. Un *descriptor de tráfico* en ATM es un conjunto de parámetros que se pueden usar para caracterizar una conexión. Estos parámetros pueden ser, por ejemplo, la tasa pico, la tasa promedio, y la longitud máxima de ráfaga a la tasa pico. Un *descriptor de fuente de tráfico* es un subconjunto del descriptor de tráfico que se utiliza durante el establecimiento de la conexión para caracterizarla. Un *descriptor de conexión* caracteriza la conexión a nivel UNI, y consiste de un descriptor de fuente de tráfico, tolerancia en la variación del retraso de la celda, y definición de conformidad. Este descriptor de conexión se utiliza por la red durante el establecimiento de la conexión para asignar recursos y derivar parámetros para UPC. La definición de conformidad se utiliza por UPC para distinguir claramente entre celdas conformantes y no conformantes.

Un contrato de tráfico consiste de:

- Descriptor de conexión.
- Clase QOS que se solicita.
- Definición de una conexión adecuada (compliant connection).

Se determina una compliant connection por el proveedor de la red y difiere de la definición de conformidad que se aplica a celdas individuales. Por ejemplo, una compliant connection puede permitir un cierto número de celdas no conformantes.

Algunos de los parámetros que han sido propuestos para el descriptor de fuente de tráfico son:

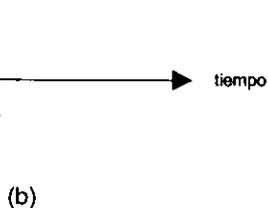
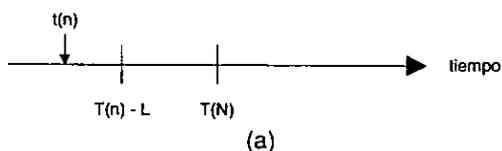
- Tasa pico de celdas y tolerancia de variación en el retraso de celda
- Tasa sustentable de celdas y tolerancia a ráfagas
- Tiempo mínimo de llegada entre celdas
- Mínimo del promedio de tiempo de llegada entre celdas en un intervalo específico
- Tasa promedio
- Longitud promedio y máxima de ráfaga

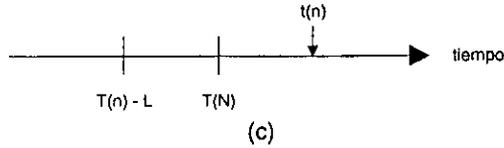
### Tasa Pico de Celda y Variación de Retraso de Celda

Aunque originalmente se definió la tasa pico de celda como el recíproco del tiempo mínimo de llegada entre dos celdas consecutivas, esta definición pronto se volvió obsoleta porque en un enlace ranurado, donde las celdas solo se transmiten en ranuras fijas de tiempo a una tasa de  $N$  bps, este parámetro sólo arroja valores  $N$ ,  $N/2$ ,  $N/3$  y así consecutivamente. Por lo tanto, el foro ATM ha propuesto una definición basada en el Algoritmo de Tasa Genérica de Celda (GCRA) y el concepto de terminal equivalente.

#### Algoritmo de Tasa Genérica de Celda (GCRA)

El GCRA involucra dos parámetros, un incremento  $I$  y un límite  $L$ , por lo que el algoritmo se denota de manera completa como  $GCRA(I,L)$ . Se puede explicar de dos maneras equivalentes: Un algoritmo de *virtual scheduling* o un algoritmo de 'cubeta con fugas' de estado continuo (continuous-state leaky bucket).

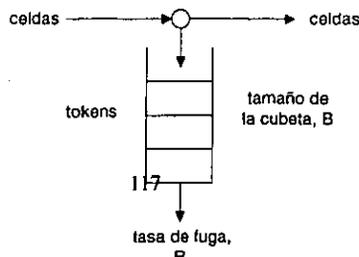




**Fig. 10** Algoritmo de Virtual Scheduling: (a) La celda llegó demasiado pronto y es no conformante; (b) La celda llegó anticipada pero conformante, y entonces  $T(n+1) = T(n) + l$ ; (c) La celda es conformante, y  $T(n+1) = t(n) + l$ .

En el algoritmo de virtual scheduling de la fig. 4.10, el tiempo de llegada real de la celda  $n$ ,  $t(n)$ , se compara con el tiempo de llegada teórico  $T(n)$ , que es el tiempo de llegada esperado asumiendo que las celdas se encuentran igualmente espaciadas en el tiempo con una distancia  $l$ . El algoritmo intenta garantizar que la tasa de celda no sea mas grande de  $1/l$  en promedio, con una tolerancia dependiente de  $L$ ; esto quiere decir que la celda no debe llegar mucho tiempo antes que el tiempo de llegada teórico. Se dice que la celda es conformante si  $t(n) > T(n) - L$ ; de otra manera se dice que es no conformante. El tiempo de llegada teórico para la siguiente celda,  $T(n + 1)$ , se calcula como una función de  $t(n)$ . Si la  $n$ -ésima celda es conformante y  $t(n) < T(n)$ , entonces el siguiente tiempo de llegada teórico se establece como  $T(n + 1) = T(n) + l$ . Si la celda es conformante y  $t(n) \geq T(n)$ , entonces el siguiente tiempo de llegada teórico se establece como  $T(n + 1) = t(n) + l$ . Las celdas no conformantes no se toman en cuenta para actualizar los valores del tiempo de llegada teórico.

El algoritmo básico de leaky bucket se presenta en la fig. 4.11, como un esquema de encolamiento de tokens. Un buffer (o cubeta de tokens) de tamaño  $B$  que contiene tokens se drena a una tasa constante de fuga  $R$ . Una celda que va llegando intenta agregar un token al buffer, y se le permite el paso si la cubeta aún no está llena. En caso contrario, la celda se descarta. Conceptualmente, los tokens pueden ser vistos como llegadas a una cola de capacidad finita con un solo servidor, con tiempos de servicio determinísticos. Este algoritmo refuerza la tasa promedio  $R$  y permite ráfagas temporales



por arriba de la tasa  $R$  dependiendo del tamaño del buffer  $B$ .

**Fig. 4.11** Algoritmo 'leaky bucket'

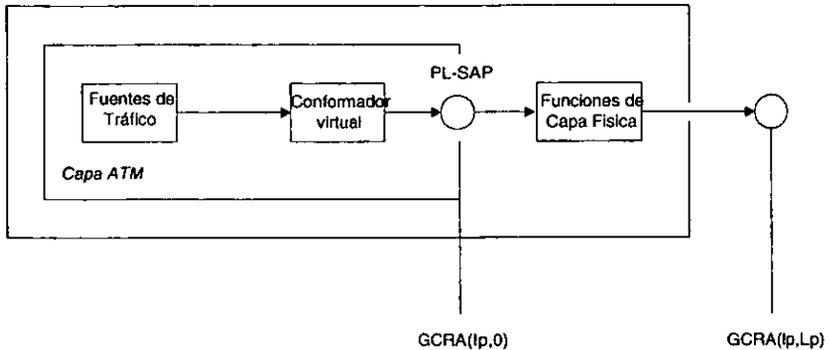
En lugar de descartar las celdas cuando el buffer está lleno, se puede tener un buffer de entrada para que se encolen ahí las celdas que van llegando; también se puede marcar una celda (esto es, disminuir su prioridad de pérdida, CLP) y dejarla pasar para que se pueda descartar posteriormente si es necesario.

Bajo el esquema básico, los únicos parámetros ajustables son  $R$  y  $B$ . Si  $B$  es demasiado pequeño, existe poca tolerancia para variaciones en los tiempos de llegada entre celdas, y se pueden descartar por equivocación celdas que sí son conformantes. Por otro lado, si  $B$  es muy grande, se convierte en un mecanismo poco efectivo porque permite desviaciones muy grandes de  $R$ .

Como se dijo anteriormente, el GCRA( $I,L$ ) es funcionalmente equivalente a un leaky bucket de estado continuo. La cubeta se drena continuamente a una tasa de 1 por unidad de tiempo y se llena con un incremento  $I$  para cada llegada de una celda conformante. Se dice que una celda es conformante sólo si el contenido del buffer es menor que el límite  $L$  a la llegada de la celda, de otra manera, se considera no conformante. La capacidad del buffer es  $L + I$ .

#### *Terminal Equivalente.*

En la fig. 4.12 se muestran las funciones de una terminal equivalente, que es un modelo conceptual para representar la generación de un flujo de celdas del usuario. Esto no significa que la terminal del usuario lleve a cabo las funciones representadas, sino que el flujo de celdas que cruza el UNI parece como si hubiera sido generado por una terminal equivalente. Las celdas se generan en la capa ATM y se conforman (es decir, que se introducen en buffers para separarlas en el tiempo) de tal manera que cumplan con un GCRA( $I_p,0$ ) en el punto de acceso a servicio de la capa física (PL-SAP), que es un punto conceptual donde las celdas de la capa ATM se presentan a la capa física para su transmisión. La *tasa pico de celda* se define entonces como el inverso  $R_p = 1/I_p$ .



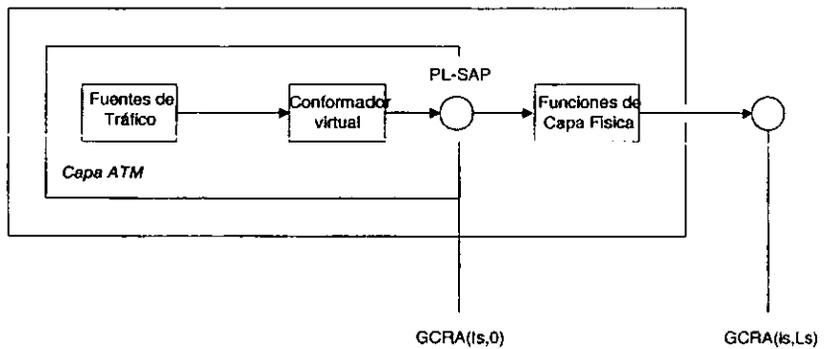
**Fig. 4.12** Modelo de Terminal Equivalente para la tasa pico de celda y la tolerancia a variación de retraso de celda.

La tolerancia de variación de retraso de celda va mano con mano con la tasa pico de celda. Después de que la capa ATM presenta celdas en el PL-SAP para su transmisión, se introduce cierta aleatoriedad en el espaciamiento del flujo de celdas, debido a causas como el multiplexaje, inserción de celdas OAM, o espera por ranuras de tiempo. Entonces, puede ser que este flujo ya no se conforme a un  $GCRA(lp,0)$ . El límite superior de la distorsión en el flujo de celdas es la tolerancia de variación de retraso de celda. Si denotamos esta tolerancia como  $Lp$ , el flujo de celdas que se genera por la terminal equivalente se conforma a un  $GCRA(lp,Lp)$  a la salida de la terminal.

### Tasa Sustentable de Celdas y Tolerancia a Ráfagas

Para una fuente CBR, los parámetros anteriores son suficientes para la asignación de recursos. Sin embargo, para las fuentes VBR no son suficientes porque no dan ninguna indicación sobre las posibles ráfagas que se pueden presentar. Para fuentes

VBR, se necesita también especificar la tasa promedio (si se conoce) para poder asignar los recursos.



**Fig. 4.13** Modelo de Terminal Equivalente para la Tasa Sustentable de Celda y la Tolerancia a Ráfaga

La tasa sustentable de celda y la tolerancia a ráfagas son el límite superior de la tasa promedio y el límite superior de la desviación permisible de esta tasa promedio, respectivamente. Estos parámetros también se pueden definir utilizando el modelo de terminal equivalente, como se muestra en la fig. 4.13. En la capa ATM, las celdas se generan y pasan a la capa física a intervalos iguales  $I_s$ . La tasa sustentable se define como  $R_s = 1 / I_s$ .  $I_s$  sólo tiene sentido si  $I_s > I_p$ . En el punto PL-SAP, el flujo se conforma a  $GCRA(I_s,0)$

Antes de la transmisión, operaciones en la capa física introducirán desviaciones en el espaciamiento del flujo de celdas. Si la tolerancia a ráfagas es el límite superior de estas desviaciones y se denota con  $L_s$ , entonces el flujo de celdas que se genera a la salida de la terminal equivalente se conforma a  $GCRA(I_s,L_s)$ . Se tiene entonces que la máxima longitud de una ráfaga es  $1 + \lceil L_s / (I_s - I_p) \rceil$

## Protocolo de Reservación Rápida

Para algunas aplicaciones de datos, tales como transferencias de LAN a LAN en forma de ráfagas, la fuente de tráfico se caracteriza únicamente por ráfagas a una tasa pico separadas por periodos de inactividad. La tasa pico es entonces el único parámetro conocido, y los demás parámetros no aplican. Para este tipo de tráfico, no es necesario seguir un establecimiento de conexión largo para negociar un contrato de tráfico detallado. Una mejor aproximación es negociar una tasa al principio de cada ráfaga, siguiendo un procedimiento simplificado llamado *protocolo de reservación rápida*.

Bajo este esquema, una celda especial precede a la ráfaga, para solicitar los recursos de la red, con lo que cada ráfaga puede ser admitida o rechazada individualmente. Si es aceptada, los recursos asignados a esta son inmediatamente liberados cuando concluye, lo que reduce el tiempo de señalización y asegura el transporte confiable de celdas correlacionadas que pertenecen a una unidad de datos más grande. Es una alternativa viable para servicios que no requieren un QOS garantizado, que son más sensitivos a la pérdida de celdas que a su retraso, y que tienen características de tráfico impredecibles.

### IV.5.3 Control de Parámetros de Uso y de Red

El control de parámetros de uso (UPC) se necesita para monitorear y regular que los flujos de tráfico entrante al UNI cumplan con los contratos de tráfico establecidos. Eso mismo, pero a nivel de NNI, se llama *control de parámetros de red (NPC)*. El objetivo de estos mecanismos es proteger a la red de desviaciones (intencionales o no) de los parámetros de tráfico negociados que puedan afectar de manera negativa el QOS de otras conexiones que sí se adhieren al contrato. Ciertas tareas específicas verifican continuamente la validez de los valores VPI/VCI y que las tasas del tráfico entrante de VPCs/VCCs activas se conformen a los parámetros establecidos.

Un mecanismo UPC/NPC debe tener las siguientes características:

- Ser sencillo de implementar y entendible por el usuario
- Responder rápidamente a violaciones

- Permitir un cierto margen de tolerancia debido a indeterminaciones prácticas
- Ser transparente si la fuente es conformante.

Aunque aún no se ha estandarizado un mecanismo UPC/NPC en particular, el Foro ATM especificó el algoritmo GCRA de leaky bucket. El UPC utiliza el marcado de celdas para cumplir con su función.

## Marcado de Celdas

Es responsabilidad del usuario el conformarse a los parámetros del contrato de tráfico. Para las celdas que están en violación, el UPC puede marcar las celdas con prioridad de pérdida alta cambiando dicha prioridad a  $CLP = 1$ , o bien puede descartarlas. Si se utiliza la opción de marcarlas, las celdas indicadas (ahora con  $CLP = 1$ ) se mezclan con otras celdas con  $CLP = 1$  antes de que entren al mecanismo UPC para flujos  $CLP = 1$  o  $CLP = 0 + 1$ . Dentro de la red, las celdas con  $CLP = 1$  se descartan si se encuentra congestión.

La técnica de marcar celdas es conveniente si existe una probabilidad significativa de que el tráfico marcado se pueda transportar por la red sin afectar su desempeño (p. ej. cuando hay tráfico ligero). Puede ser apropiado para servicios que no son muy exigentes en cuanto al QOS.

Si la probabilidad de transportar exitosamente al tráfico marcado es baja, (p. ej. cuando la red tiene cargas pesadas), es preferible evitar el marcado de celdas, porque éstas utilizan recursos de red valiosos e incrementan el nivel de congestión. Es preferible entonces descartar el exceso de tráfico en el UPC para evita desperdiciar recursos de red.

### IV.5.4 Control de Congestión

Mientras que CAC y UPC son funciones para prevenir la congestión, hay la probabilidad de que esta exista a causa de sobrecarga temporal de buffers dentro de la red. El propósito del control de congestión es la detección y la reacción para minimizar la velocidad, efectos y duración de la misma. Por simplicidad y rapidez, el protocolo ATM no incluye controles de flujo convencionales a nivel de enlace, que son apropiados únicamente para el tráfico tolerante a retrasos. En ATM, las acciones de control de congestión incluyen el descartamiento selectivo de celdas y el *explicit forward congestion indication (EFCI)*.

## Prioridades de Retraso y Pérdida

El descartamiento o eliminación selectiva de celdas depende de las prioridades de pérdida de la celda. ATM permite que estas prioridades se asignen específicamente a celdas individuales por medio del bit CLP del encabezado de la misma. Cuando ocurre congestión y no se puede evitar el descartar celdas, las celdas de baja prioridad (CLP = 1) se descartan antes que las celdas con CLP = 0. Para que una celda tenga CLP = 1 es porque o no se conforma al contrato de tráfico (marcada por la red) o porque contiene datos de usuario no indispensables (marcada por el usuario).

Existen dos implementaciones para el descartamiento selectivo: el esquema *push-out* y el *partial-buffer-sharing*. En el primer esquema, una celda que llega con CLP = 0 puede encolarse en un buffer lleno eliminando una celda con CLP = 1 que se encuentre en el mismo. Las celdas que llegan con CLP = 1 no pueden encolarse. En el segundo, cuando el buffer llega a un cierto valor límite (aún sin estar lleno) únicamente se aceptan celdas con CLP = 0 y se rechazan aquellas con CLP = 1. El esquema *push-out* tiene un desempeño óptimo, pero el *partial-buffer-sharing* tiene una implementación mucho más simple y puede llegar a tener un rendimiento muy cercano al del *push-out*.

Las prioridades de retraso son útiles para reducir los retrasos de extremo a extremo y el jitter de tráfico para el cual el tiempo es crítico. ATM permite que este tipo de prioridades se asignen implícitamente por cada VPC/VCC; es decir, las celdas que pertenezcan al mismo VPC/VCC tendrán la misma prioridad de retraso asociada con su VPI/VCI en una tabla.

Las prioridades de retraso afectan el orden en que las celdas almacenadas se programan para transmisión en un enlace compartido. Esta programación se puede decidir en base a celdas individuales o a ciclos. Cuando se programa por celdas, se escoge para transmisión la celda que tiene un periodo de latencia mas próximo a expirar, para evitar que se descarte.

Cuando se programa por ciclo, las decisiones se toman únicamente al comienzo de ese ciclo. Por ejemplo, para cada ciclo, las ranuras de tiempo se pueden asignar primero a un número mínimo de celdas de tiempo real encoladas que no pueden ser

retrasadas hasta el siguiente ciclo sin que expire su tiempo de latencia. El resto del ciclo se llena después con celdas que no sean de tiempo real.

### **Explicit Forward Congestion Indication (EFCI)**

Mientras que las prioridades de retraso y de pérdida se utilizan en acciones de control de tráfico dentro de un switch, EFCI es un mecanismo para la comunicación de información de congestión de la red hacia el usuario para habilitar acciones de control de extremo a extremo. Si un nodo de la red experimenta congestión, le puede informar tanto a los nodos que siguen en la ruta como al destino cambiando el campo PT en el encabezado de las celdas. El usuario destino leerá entonces los indicadores de congestión y le dirá a la fuente indicada que ajuste su tasa, si es que el flujo de tráfico de esa fuente puede ajustarse o modificarse.

Este mecanismo ayuda a disminuir la tasa de pérdida de celdas durante periodos de congestión persistentes, con una duración de al menos un orden de magnitud mayor que el tiempo de propagación.

### **IV.6 Switch ATM**

Un switch o conmutador ATM es una matriz de conmutación construida con elementos de conmutación binarios. Las celdas pasan a través de las matrices de conmutación a una alta velocidad controladas por un circuito de tiempo el cual sincroniza y administra al switch.

Un switch ATM recibe tráfico desde muchos usuarios diferentes y multiplexa las celdas al siguiente switch sobre una o más conexiones físicas. Cuando un switch recibe una celda, ve cual es la dirección de destino para enrutarla. Para esto, se ha establecido previamente una conexión hacia la estación de destino. Cuando varias estaciones deseen usar el ancho de banda disponible, tendrán que dividirlo entre ellas.

En un switch ATM se tiene varios bloques funcionales:

### **Módulo de entrada.**

Se usa para recibir celdas de entrada y prepararlas para rutearlas a través del CSF (cell switch fabric o arquitectura del switch de celda). En cada puerto de entrada, la primera función es la terminación de señales de entrada SONET y extracción de las celdas ATM, esto involucra: conversión de señales ópticas a eléctricas, recuperación del flujo digital, procesamiento del SONET más alto, delineación de celdas, separación promedio de celdas (descartando celdas vacías).

Las celdas deben de estar preparadas para rutear a través del CSF, esto requiere de las siguientes funciones en cada celda: chequeo de errores en la cabeza de la celda usando el campo HEC, validación y conversión de valores VPI/VCI, determinación del puerto de salida, posible ordenamiento de celdas de señalización y ruteo hacia el CAC, posible ordenamiento de celdas de administración y ruteo hacia el CM, control de parámetros de uso/red para cada VPC/VCC y adición de una etiqueta interna.

Una etiqueta interna puede ser añadida a cada celda en los módulos de entrada y removida en los módulos de salida. Puede contener dos tipos de información ruteo interno y ruteo general.

Para el ruteo interno la etiqueta puede contener campos relativos al puerto de salida, disminución de tolerancia, retaso de prioridad, impresión de la hora, retaso o identificador de conexiones broad cast/multicast.

Para propósitos generales por ejemplo monitoreo del movimiento interno, la etiqueta puede contener campos para identificar el usuario fuente, número de secuencia de la celda, tipo de celda o chequeo de errores.

### **Módulo de Salida.**

Es empleado para preparar celdas de salida para la transmisión. Sus principales funciones son: remover y procesar las etiquetas internas de cada celda, posible conversión de valores VPI/VCI, generación de campo HEC e inclusión dentro de los header de la celda, posible mezcla de señales de CAC y celdas de administración de

SM sin celdas de datos del usuario de salida, separación de celdas promedio(agregando celdas vacías), mapeo de celdas dentro de cargas SONET, generación del SONET de arriba, conversión del flujo digital en una señal óptica.

### **Arquitectura del switch de celda.**

Permite rutear celdas de datos del usuario de los puertos de entrada hacia los puertos de salida y rutear señalización y administración de celdas entre los otros bloques funcionales en el switch. Su función principal es transferir celdas entre los otros bloques funcionales del switch en particular celdas de datos del usuario deben ser ruteados de los módulos de entrada a los módulos de salida. Es posible usarlo para rutear celdas de señalización y administración hacia el CAC o el SM, manejo del buffer de las celdas, concentración del tráfico y multiplexaje, redundancia para tolerancia a fallas, multicasting o broadcasting, asignación en secuencia de celdas basado en prioridades de retraso, depuración selectiva de celdas basado en prioridades más bajas, monitoreo de congestión y activación de EFCI.

### **Control de admisión de conexiones.**

Su función es procesar e interpretar información de señalización y decidir acerca de admitir o rechazar información. Sus funciones son relativas al establecimiento, modificación y terminación de conexiones en los niveles de rutas virtuales y canales virtuales. Sus funciones principales son: protocolos de señalización de capas altas, funciones de señalización AAL para interpretar o generar celdas de señalización, interfase de una red de señalización, negociación de aspectos de tráfico con usuarios requiriendo nuevos VPC y VCC incluyendo selección de ruteo, decisiones de admisión o rechazo para VPC y UCC solicitados, generación de parámetros UPC/NPC.

### **Sistema de administración.**

Se usa para realizar todas las funciones de administración y control de tráfico que aseguren la operación correcta y eficiente del switch. Sus principales funciones en la capa física y en la capa ATM son: administración de la configuración de los componentes del

switch, control de seguridad para la base de datos del switch, medición del uso de recursos del switch, manejo de tráfico, administración de la información básica, administración cliente/red, interfase con sistemas de operación o TMN y soporte de manejo de red

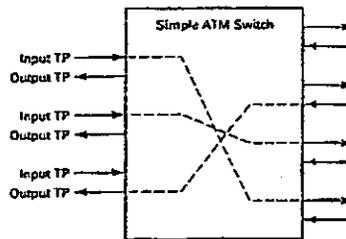


Fig. 4.14 Switch ATM simple

Los switches ATM pueden ser clasificados en dos principales categorías switches ATM públicos y switches ATM privados.

Switches ATM públicos: Son parte de una red pública proveedora de servicios de telecomunicaciones y es referida en los estándares ATM como un network node (NN). Estos switches son vendidos a la industria de las telecomunicaciones por los mismos vendedores quienes proveen POTS convencionales y equipo de transmisión y conmutación.

Switches ATM privados: Son adquiridos y mantenidos por una organización de usuarios y son referidos en los estándares ATM como un customer premises node (CPN). Los switches públicos ATM son vendidos a organizaciones de usuarios por los mismos vendedores de infraestructura de red quienes proveen tarjetas de red, concentradores, etc.

Algunos tópicos usados para el diseño de un switch ATM son:

### Throughput

Mide el promedio en el cual los datos pasan a través del switch. Refleja el procesamiento interno del switch y los promedios de transmisión así como el grado de

paralelismo dentro del switch. Los switch ATM pueden ser diseñados para procesar celdas de velocidades cercanas a los 2 Gbps. Es interesante notar que a un promedio de datos de 2 Gbps el switch necesita ser capaz de recibir y transmitir celdas en un promedio de 4 millones de celdas por segundo sobre cada ruta de transmisión activa.

### **Resolución de contención**

En el diseño de todo switch hay lugares donde la contención de los recursos puede ocurrir. Los buffers pueden ser usados para detener celdas hasta que la contención es resuelta, pero a veces la capacidad del buffer puede ser excedida. El diseño del switch incluye el tamaño y colocación de buffer también como métodos para esquivar o manejar congestión.

### **Escalabilidad**

Algunos diseños de switch trabajan bien con números más bajos de rutas de transmisión pero no pueden retener niveles aceptables de rendimiento o costo cuando el número de rutas de transmisión llega a ser grande.

### **Costo**

La complejidad del diseño y el costo relativo de diferentes tecnologías empleadas en implementar un switch pueden afectar su costo total.

## **IV.6.1 Tipos de Switches.**

Existen diferentes tipos de diseño para un switch ATM:

- Arquitectura de switch crosspoint.
- Arquitectura de switch de medios de transmisión compartidos.
- Arquitectura de switch de memoria compartida.
- Arquitectura de switch multi-etapa.

### Arquitectura de switch crosspoint.

Fue desarrollado principalmente para soportar aplicaciones telefónicas, a veces es llamado un switch de división de espacios, usa rutas paralelas de datos para conectar vías de transmisión de entrada-salida. Las rutas paralelas de datos hacen a este switch eficiente y su estructura relativamente simple hace barata su construcción. Sin embargo problemas en la escalabilidad pueden presentarse cuando el número de rutas de transmisión conectadas al switch es muy grande.

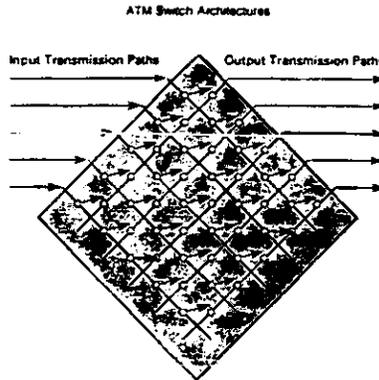


Fig. 4.15 Switch ATM Crosspoint

### Arquitectura de switch de medios de transmisión compartidos.

Estos switch toman la forma de un backplane o de estructura de anillo. Las celdas que arriban de las vías de transmisión de entrada son transmitidas sobre un medio de transmisión compartido y son entonces enviados hacia afuera sobre las rutas de transmisión de salidas apropiadas. Operaciones broadcast multicast pueden ser manejadas en un switch de este tipo colocando en el medio compartido múltiples copias de la celda, cada una de las cuales tiene diferentes direcciones de vías de transmisión de salida asociadas a ella.

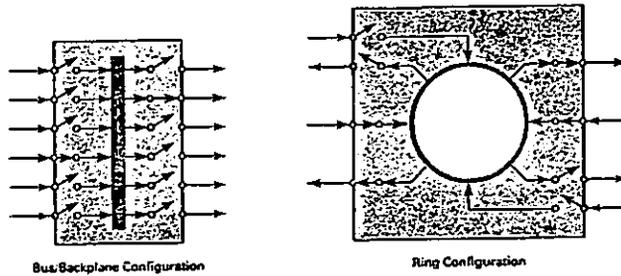


Fig. 4.16 Switch ATM de medios de transmisión compartidos

**Arquitectura de switch de memoria compartida.**

Con un switch de este tipo las celdas arribando sobre rutas de transmisión de entrada son temporalmente escritas a una memoria compartida. Las celdas son entonces aceptadas de la memoria compartida para su transmisión de salida. La memoria compartida implementa colas de salida en las cuales las celdas son temporalmente retenidas hasta que el switch pueda transmitir las.

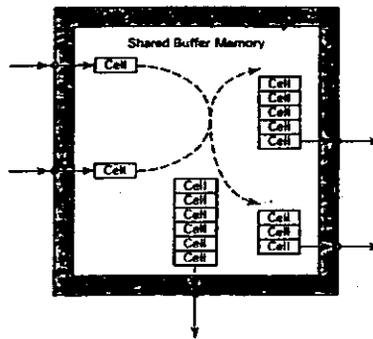


Fig. 4.17 Switch ATM de memoria compartida

**Arquitectura de switch multi-etapa.**

Frecuentemente es llamado un switch Banyan. Consiste de un número de elementos de conmutación individuales que son conectados por vías de transmisión

interinas. Una celda pasa a través de una serie de estos elementos de conmutación para alcanzar su ruta de transmisión de salida basada en una dirección asociada con esa vía de transmisión con elemento de conmutación tiene dos entradas y dos salidas y las interconexiones entre ellos forman una estructura tal que cada vía de transmisión de salida puede ser alcanzada desde cada vía de transmisión de entrada.

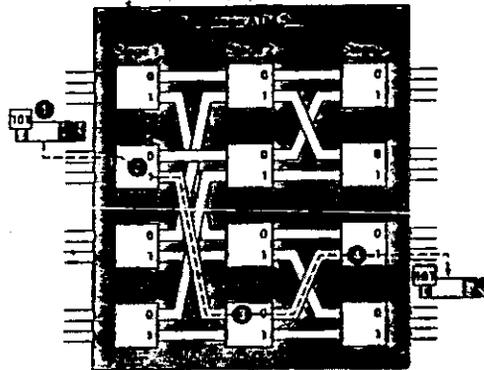


Fig. 4.18 Switch ATM multietapa

#### IV.7 Emulación de Redes Lan

Actualmente la interoperabilidad de los sistemas finales que se encuentran en una gran variedad de redes LAN interconectadas representan un punto sumamente importante. Los sistemas finales conectados a una LAN normalizada forman la capa MAC (Control de Acceso al Medio) apropiado para este tipo de LAN. Por otro lado, los sistemas finales conectados directamente a una red ATM implementan los protocolos ATM y AAL.

A fin de utilizar las aplicaciones de software basadas en Redes de Area Local, se presenta la necesidad de definir un servicio ATM denominado LAN Emulation (LANE), Emulación de redes de área local, el cual se encarga de emular servicios de LAN existentes a través de una red ATM y puede soportar sistemas finales por medio de su capa de software.

Como el servicio de LANE es proporcionado por una red ATM, entonces los sistemas finales (estaciones de trabajo, servidores, etc.) pueden conectarse a una red

ATM mientras las aplicaciones de software interactúan como si estuvieran corriendo en su ambiente original de LAN. Esto permite la interoperabilidad entre aplicaciones de software residentes en sistemas finales ATM y en los sistemas finales tradicionales de LAN.

La solución general para este problema es el uso de dispositivos de enrutamiento. Básicamente, un dispositivo de enrutamiento funciona en el nivel del protocolo de internet (IP). Todos los sistemas finales implementan IP y todas las redes se interconectan mediante dispositivos de enrutamiento. A pesar de que esta aproximación es efectiva, introduce un cierto volumen de procesamiento suplementario y retardo en cada nodo que pueden llegar a ser importantes para interconexiones de redes muy grandes.

En respuesta a esta necesidad de convivencia, el Foro ATM ha creado la especificación para la coexistencia de LAN normalizadas y redes LAN ATM, conocida como Emulación de Redes LAN ATM. El objetivo en este tipo de emulación de redes LAN ATM es el permitir la coexistencia de nodos LAN de medio compartido para interoperar a través de una red ATM y con dispositivos que conectan directamente con switches ATM.

#### Redes LAN ATM Emuladas (LANE)

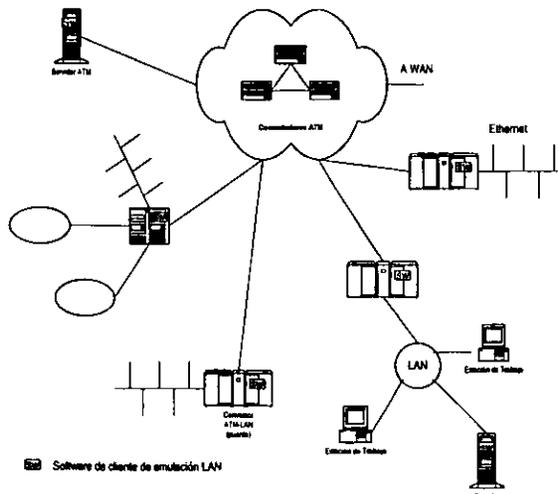


Fig. 4.19 Ejemplo de configuración de Emulación LAN ATM

La arquitectura del protocolo involucrado en la emulación de redes LAN ATM así como la interacción existente de un sistema de conexión ATM con un sistema final conectado a una LAN tradicional puede observarse en la figura 4.20.

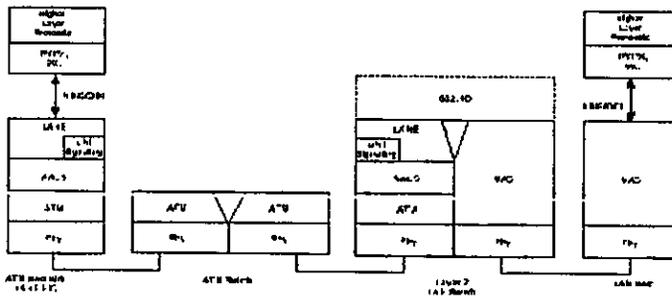


Fig. 4.20 Arquitectura del protocolo LANE.

Observamos que el sistema final conectado a la LAN tradicional no se ve afectado, es posible hacer uso del conjunto de protocolos normalmente utilizados, incluyendo el protocolo MAC específico de esta LAN y LLC existente sobre MAC.

La LANE define cómo pueden ejecutarse sin modificación sobre una red ATM las aplicaciones y sistemas operativos de red con base Ethernet o Token Ring. LANE funciona permitiendo que el sistema operativo y todos los protocolos de la capa dos (de transmisión de datos) y superiores operen de forma transparente con ATM. Un adaptador ATM que emplee controladores LANE basados en la Network Driver Interface Specification (NDIS) o bien la Open Data-Link Interface (ODI) aparece ante el sistema operativo de red y la pila de protocolos del servidor como si fuera un adaptador Ethernet o Token Ring. La clave de este diagrama es el uso de un puente conocido como conversor ATM-LAN.

El puente lógico debe ser capaz de convertir tramas MAC en celdas ATM y viceversa. Esta es una de las funciones clave de la emulación de redes LAN ATM. La

especificación del Foro ATM hace uso de AAL 5 para segmentar tramas MAC en celdas ATM, y agrupar celdas ATM entrantes en tramas MAC. Para celdas ATM de salida, los conversores ATM-LAN se conectan de la forma usual a un conmutador ATM como parte de una red ATM.

En la figura 4.19 se muestra el caso en que una estación en una LAN tradicional intercambia datos con una estación conectada directamente a una red ATM. Para hacer posible este intercambio la estación ATM debe incluir un módulo de emulación ATM que acepte tramas MAC de AAL y pase el contenido a una capa LLC. Así la estación emula, verdaderamente a una LAN, ya que puede recibir y transmitir tramas MAC con el mismo formato de la MAC lejana. Desde el punto de vista de los sistemas finales en la LAN tradicional, la estación ATM es sólo otro sistema final con una estación MAC. El proceso de emulación de la LAN es transparente a los sistemas existentes que implementan LLC y MAC.

### **Clientes y Servidores en Emulación de Redes LAN**

Existen ciertas reflexiones hacia cuestiones fundamentales que vale la pena mencionar:

1. Los dispositivos conectados directamente a switches ATM y los sistemas conversores ATM-LAN hacen uso de direcciones ATM, es decir, se lleva a cabo una traducción entre éstas y las direcciones MAC.
2. ATM hace uso de un protocolo orientado a conexión mediante canales y caminos virtuales, esto es , se acepta un protocolo MAC no orientado a conexión dentro de un esquema orientado a conexión.
3. La gestión de direcciones multidestino y de difusión es fácil de conseguir en una LAN de medio compartido.

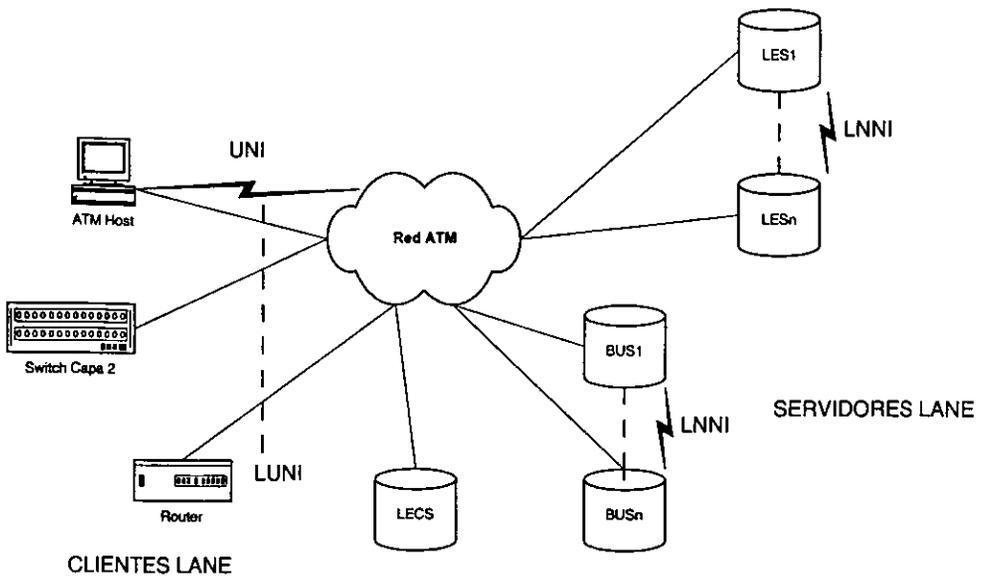
Para tratar estas cuestiones nuevamente el Foro ATM desarrolló un procedimiento en base a una aproximación cliente/servidor que describimos a continuación.

La emulación de redes LAN ATM requiere dos tipos de componentes:

**Cliente y Servidor** . Los clientes operan en base a dispositivos conectados a LAN tradicionales que hacen uso de direcciones MAC. **El cliente** es responsable de añadir entidades MAC a la configuración global y de abordar las tareas asociadas con la conversión de direcciones MAC en direcciones ATM. Generalmente, un cliente puede existir en un dispositivo de enrutamiento o en un servidor ATM. **Los servidores** se conocen como servicios de emulación de LAN, estos servicios absorben tareas como indicar qué tipo de LAN se está emulando, mantener una tabla de todas las estaciones finales de la LANE y manejar las tareas de difusión, como mensajes Netware RIP y SAP y consultas de nombres NetBios.

Entidad	Descripción
Cliente de Emulación LAN (LEC)	Establece conexiones de control con servidores de emulación LAN; establece conexiones de datos con otros clientes; transforma direcciones MAC a direcciones ATM.
Servidor de Configuración de Emulación LAN (LECS)	Ayuda al cliente a seleccionar un LES
Servidor de Emulación LAN (LES)	Realiza transformación de direcciones inicial; acepta clientes
Servidor de Difusión y Servidor Desconocido (BUS)	Realiza multidestino

El servicio de emulación LAN comprende realmente tres tipos de servidores que realizan tareas separadas: el servidor de configuración de emulación LAN (LECS, "Lan Emulation Configuration Server"), el servidor de emulación LAN (LES, "Lan Emulation Server") y el servidor de difusión y desconocido (BUS, "Broadcast and Unknown Server"). El motivo de dividir el servidor en tres módulos es que un gestor puede decidir disponer de más servidores de un tipo que de otro para un funcionamiento eficiente, y puede decidir distribuirlos físicamente con el fin de minimizar la tarea de comunicación.



**Fig. 4.21** Configuración de las Interfaces del Protocolo LANE.

El cliente puede establecer conexiones en base a canales virtuales, llamadas conexiones de control, con el LECS y el LES. El enlace con el LECS se usa por un LES para conseguir el acceso a una LAN Emulada y localizar un LES. El LES es responsable de registrar nuevos clientes y sus direcciones MAC en la LAN emulada y de la conversión entre direcciones MAC y direcciones ATM.

Una vez que un cliente y sus sistemas finales se han incorporado a una LAN emulada, la mayor parte del trabajo se realiza a través de las conexiones de canal virtual, llamadas conexiones de datos. Las tramas MAC, segmentadas en celdas ATM, se transmiten a través de conexiones de datos entre sistemas finales en la misma LAN emulada. Para una transmisión dirigida a una única estación destino se configura una conexión de canal virtual entre dos clientes; es el protocolo de configuración visto en la fig. 4.19. Por último, la conexión de datos entre un cliente y un BUS, transporta

transmisiones de difusión o multidestino y se usa también para gestionar transmisiones en las que el cliente emisor no conoce la dirección del cliente receptor.

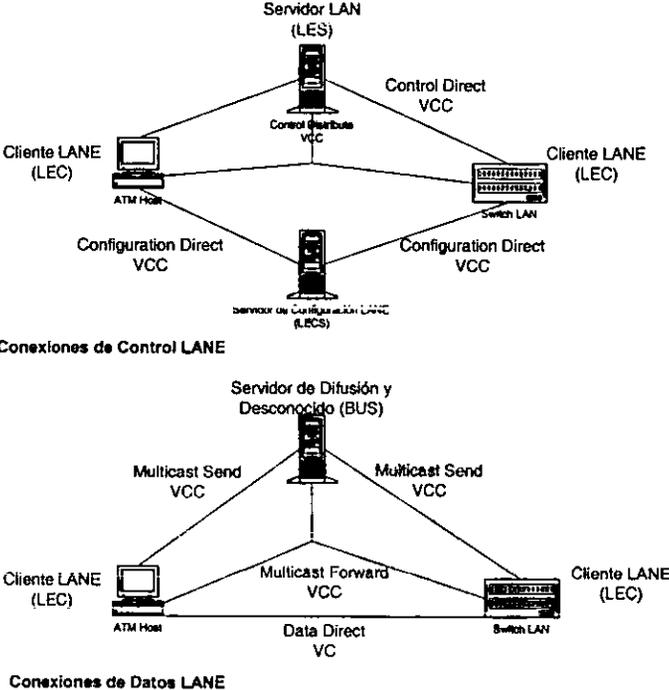


Fig. 4.22 Conexiones de Control y de Datos en una LANE .

**Tolerancia a Fallas**

Con la versión 1.0 de la especificación LANE, no es posible la redundancia de hardware en la LAN Emulada. Si falla el LES o el BUS, los usuarios no se pueden conectar con la red troncal ATM. Para afrontar el problema de la unicidad de los puntos de avería, diversos vendedores independientes han intentado implementar soluciones que proporcionen tolerancia a fallos en las redes ATM. Cisco Systems ha desarrollado Simple Server Redundancy Protocol (SSRP), que replica la información de configuración en los

LANE Servers, por ejemplo. La información básica de configuración sobre las LAN emuladas se comparte entre el dispositivo primario y hasta tres dispositivos LECS de respaldo.

Si falla el LES/BUS, se cortan las conexiones con los LEC acoplados. El cliente al percibir la avería en la red, intenta conectarse con la LAN emulada, el LECS lo dirigirá hacia un LES/BUS de respaldo operativo en otro dispositivo de red. Olicom ha completado esta solución mediante el software Dynamic Connection Redundancy o DCR, el cual permite que un cliente busque automáticamente la localización del nuevo LES/BUS en la red ATM a través del LECS.

#### **IV.8 Operación y Mantenimiento**

La calidad de servicio ofrecido por una red de telecomunicaciones depende en gran parte de la viabilidad de los componentes individuales, pero lo más importante es el diseño de la red como un todo. Una de las tareas más importantes del administrador de la red es la operación y mantenimiento de la misma.

Los estándares ATM definen 5 niveles de operación y mantenimiento de una red ATM denominados desde F1 hasta F5. Los cuales se describen a continuación:

- **Nivel F1:** nivel regenerador de secciones. Este nivel comprende dos funciones:

**Detección de señales:** esta función asegura que la sección regeneradora permanezca funcionando. Si no se recibe una señal en un punto dado un AIS (señal de indicación de alarma) es transmitida hacia los demás puntos receptores en la conexión y un RDI (indicación remota de defectos) será retornada para notificar el fin del envío.

**Alineación de frames:** la pérdida de alineación de frames (LOF) en la medida que se detecta en un regenerador intermedio también resultará en una señal AIS que será enviada hacia puntos a lo largo de la vía de transmisión y retornará un RDI .

- **Nivel F2:** nivel de sección digital: su función es el monitoreo de la sección de errores. Puede detectarse un BER (error promedio de bits) en una sección digital y entonces señales AIS y RDI son generadas.
- **Nivel F3:** nivel de ruta de transmisión. Este nivel tiene cinco funciones que son:

Cell rate decoupling(desacoplamiento de tasa de celda): es la falla en la inserción o supresión de capas físicas de celdas inactivas siendo transmitidas a la capa ATM. Las celdas inactivas utilizan la línea digital cuando no hay celdas de capa ATM esperando ser enviadas. La reacción apropiada para este estado aún no esta totalmente definida.

Reconocimiento de celdas PL-OAM (capa física de operación y mantenimiento ): en el caso de que celdas PL-OAM no sean detectadas una señal RDI será enviada al transmisor. La generación periódica de celdas PL-OAM es una obligación del emisor.

Delineación de celdas: si la delineación de celdas se pierde entonces la señal RDI es usada para notificar al emisor.

Monitoreo de estatus CN: cuando el emisor no monitoreo como ok entonces el receptor es informado por medio de AIS.

Operación AU (administrative pointer): El AU es un requerimiento de sistemas en línea basados en SDH. Cuando esta ausente el emisor es informado por medio de la señal RDI.

- **Nivel F4:** Nivel de ruta virtual: Comprende dos funciones:

Monitoreo de disponibilidad de rutas: cuando una interrupción en una ruta virtual es detectada por la capa ATM (mediante la interpretación de indicaciones de falla pasadas a la capa AM por la capa física) entonces otros puntos a lo largo del VP son notificados por medio de señales VP-AIS y VP-RDI. Esto habilita la capa ATM si es necesario para restablecer el VP usando una ruta física alternativa.

Monitoreo de performance: se efectúa enviando en forma periódica celdas de monitoreo de performance después de cada bloque de celdas de usuario. Estas son usadas para asegurarse que el performance del VP permanezca dentro de valores límites aceptables.

- **Nivel F5:** Canales virtuales. Tienen dos funciones:

Monitoreo de disponibilidad de canales: señales VC-AIS y VC-RDI son enviadas hacia puntos finales de envío y recepción de un VC para notificar condiciones de falla que rebasen la falla de conexión a un promedio nominal de una por segundo hasta que la condición de falla subsista. Estas señales en principio notifican los puntos finales ATM VCC de la falla de conexión. La respuesta puede ser ya sea intentar una conexión alternativa o esperar hasta que se recupere.

Monitoreo de performance: esta función del nivel VC de la capa ATM opera enviando celdas de monitoreo de performance en una base fin a fin después de cada bloque de n celdas de usuario. Esta función puede ser usada para monitorear bloques de errores fin a fin, inserciones no efectuadas, retraso de transferencia de celdas y otros parámetros de performance en una conexión específica.

#### **IV.9 Administración en ATM**

La administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada, bien planeada y debidamente documentada. Los objetivos de la administración son:

- Mejorar la continuidad en la operación de la red usando mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red, con una mejor utilización de los recursos.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura protegiéndola contra el acceso no autorizado haciendo imposible que personas ajenas puedan entender la información que circula en la red.

- Controlar cambios y actualizaciones en la red de modo que ocasionen las menores interrupciones en el servicio. Esto incluye cambios en hardware, en software, en aplicaciones y en procedimientos.

La administración de red se hace más crítica y complicada si se consideran los elementos que componen a las redes actuales como los tipos de señales, voz, datos y video, interconexión de varios tipos de redes, WAN, LAN y MAN, los múltiples medios de comunicación, pares de hilos trenzados, cable coaxial, fibra óptica, satélite, láser, infrarrojo, microondas, diferentes métodos de compresión, varios códigos de línea, distintos mecanismos de control de error, etc.

El sistema de administración de red opera bajo los siguientes pasos básicos:

1. Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir eventos, atributos y acciones operativas.
2. Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
3. Transportación, para hacer llegar la información del equipo monitoreado al centro de control.
4. Almacenamiento para guardar los datos coleccionados en el centro de control.
5. Análisis para correlacionar parámetros y obtener conclusiones que permitan deducir rápidamente lo que está pasando en la red.
6. Toma de decisiones para generar acciones rápidas y automáticas en respuesta previniendo una falla mayor.

La característica fundamental de un sistema de administración de red moderno es ser un sistema abierto, capaz de manejar varios protocolos y soportar varias arquitecturas de red.

### **Elementos incluidos en el manejo de la red.**

De acuerdo al modelo OSI, los elementos involucrados en la administración de red son los siguientes:

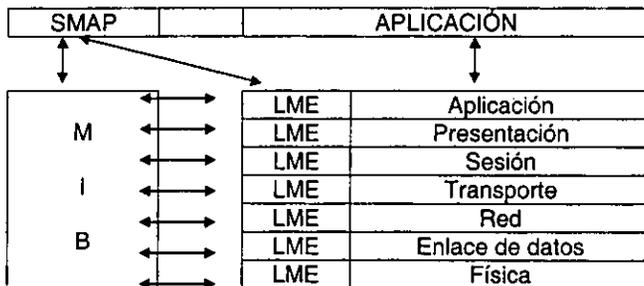
**Objetos.** Son los elementos de más bajo nivel y constituyen los dispositivos administrados.

**Agentes.** Un agente es un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente efectúa el grado de administración apropiado a ese nivel y retransmite información al administrador central de la red.

**Administración del sistema.** Es un conjunto de programas ubicados en un punto central al cual son dirigidos los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

**Modelo de administración de red en el modelo OSI**

El LME (Layer Management Entity) es un modelo conceptual para funciones internas del sistema y puede ser opcionalmente asociado con cada capa de OSI, como se muestra en la figura IV.11.1. El LME incluye colección de información de administración, reporte asíncrono de eventos, cambio de parámetros operacionales y cambio de estado de operación de la capa correspondiente.



**Fig. 4.23** Modelo de administración en OSI

El MIB (Management Information Base), es una base de datos de los objetos y atributos administrados en una red. Un agente almacena información en el MIB de todos los objetos en la red sobre los que es responsable y que puede operar.

El SMAP (System Management Application Process), es la interfaz de un MIB con el mundo exterior. Se comunica con los SMAP de otros nodos.

### **Funciones de administración definidas por el modelo OSI**

OSI define las cinco funciones de administración básicas siguientes:

- Configuración
- Fallas
- Contabilidad
- Desempeño
- Seguridad

La administración de configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

La administración de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.

La administración de contabilidad permite el establecimiento de cargos a los usuarios por uso de los recursos de la red.

La administración de desempeño se encarga de mantener el funcionamiento de la red en niveles aceptables.

La administración de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

El modelo OSI incluye cinco componentes claves en la administración de red:

CMIS (Common Management Information Services).- Es el servicio para la colección y la transmisión de información de administración de red a las entidades de red que lo soliciten.

CMIP (Common Management Information Protocol).- Es el protocolo de OSI que soporta a CMIS y que proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.

SMIS (Specific Management Information Services).- Este componente define los servicios específicos de administración de red a ser implementados.

MIB (Management Information Base).- Contiene información del estado del dispositivo, estadísticas del desempeño y parámetros de configuración.

## **SNMP**

Una interfaz temporal de administración de red, ILMI (Interim Local Management Interface), ha sido definida para el uso en redes ATM hasta que el estándar completo de administración en ATM haya sido completado. ILMI está basado en un protocolo de administración de red llamado SNMP (Simple Network Management Protocol) el cual fue diseñado originalmente para la administración de redes en ambiente TCP/IP.

ILMI define la información a ser coleccionada por los agentes llamadas UMES, (User/Network Interface Management Entities). La información que UMES usa es almacenada en el SNMP MIB.

### **Mensajes SNMP**

El administrador de red de la estación de control y los agentes instalados en los dispositivos manejados, se comunican enviando mensaje SNMP. Sólo existen cinco mensajes:

**Get request:** Contiene una lista de variables que el administrador desea leer de una MIB, esto es, el administrador pregunta sobre el estado de un objeto.

**Get Next Request:** Provee un modo de leer secuencialmente de una MIB.

**Set Request:** Lo usa el administrador para ordenar un cambio en el valor de una o más variables.

**Get Response:** Lo envía el agente como réplica a un mensaje de Get Request, Get Next Request o Set Request.

**Trap:** Este mensaje lo usa el agente para reportar que ha ocurrido un evento significativo como falla de un enlace local, enlace restablecido o mensajes recibidos con autenticación incorrecta.

## Capítulo V

### ATM CONTRA X.25 y OTRAS TECNOLOGIAS

#### V.1 ATM contra X.25

La conmutación de paquetes X.25 fue el primer sistema universal que permitió interconectar cualquier tipo de dispositivo de comunicaciones en una sola red conmutada de datos. X.25 fue diseñado para velocidades de transmisión muy inferiores a las actuales y para líneas digitales con una calidad muy inferior a las modernas. Como resultado de esto, las redes X.25 son muy robustas contra la mala calidad de las líneas, y son capaces de soportar e incluso recuperarse de errores de bits masivos. El problema consiste en que las velocidades de transmisión son muy limitadas y en cierta ineficiencia en la utilización de la línea cuando se tienen líneas de transmisión de buena calidad.

El principal problema de X.25 cuando se tienen altas velocidades de transmisión se debe a la técnica de *ventanas* que utiliza para evitar errores. Para ejemplificar el problema, se considera una línea de 2Mbps con X.25 en una distancia de 1000 Km.

En una línea de alta velocidad de transmisión de datos, siempre hay una gran cantidad de bits en tránsito en cualquier punto del tiempo, debido a su longitud; en este ejemplo existen alrededor de 20 000 bits o 2500 bytes, si tomamos en cuenta la fórmula: (longitud de línea x tasa de bits)/ velocidad de la luz. Siempre se deben considerar estos bits en tránsito cuando se diseñan redes de datos de alta velocidad.

X.25 le da mucha importancia al hecho de poder recibir los bits en el orden correcto y sin errores, mientras que ATM confía más en el chequeo que realizan las capas superiores. Uno de los métodos que emplea X.25 es el de las *ventanas* de acuse de recibo. Sólo se pueden enviar cierto número de paquetes (lo que define el tamaño de la ventana, típicamente 7) antes de que se obtenga un acuse de recibo que indique que los bits llegaron a salvo. Puesto que el tamaño máximo típico es de 256 bytes, sólo se pueden transmitir alrededor de 1800 bits (256 x 7) antes de que se reciba el acuse de recibo correspondiente. Por lo tanto, la *ventana* restringe la eficiencia de la línea a un máximo de 1800/2500 (máximos bits permitidos en tránsito / bits disponibles en tránsito), es decir, una eficiencia de alrededor del 70 %.

Se podría pensar que este problema se puede resolver incrementando el tamaño de la ventana; sin embargo, esto sólo crea más problemas. Primero, el dispositivo receptor necesita tener *buffers* de almacenamiento mucho más grandes para poder retener la información que aún no se acusa de recibo. Segundo, puesto que el tamaño de la ventana es más grande, también la probabilidad de encontrar errores en una ventana es más grande, y por tanto también se incrementa la probabilidad de necesidad de retransmisión, junto con el tiempo necesario para llevarla a cabo.

X.25 mantiene su importancia por su gran potencial de interconectar computadoras y otros dispositivos de muchos tipos y manufacturas diferentes, y por su gran presencia en el mercado. Sin embargo, no es apropiado para aplicaciones o dispositivos que necesiten tasas de bits mayores a 64 kbit/s.

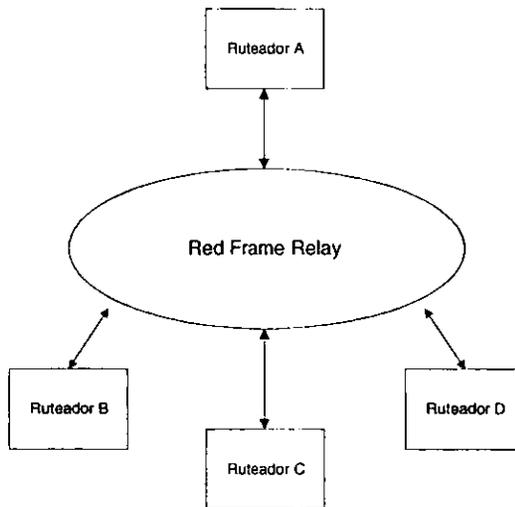
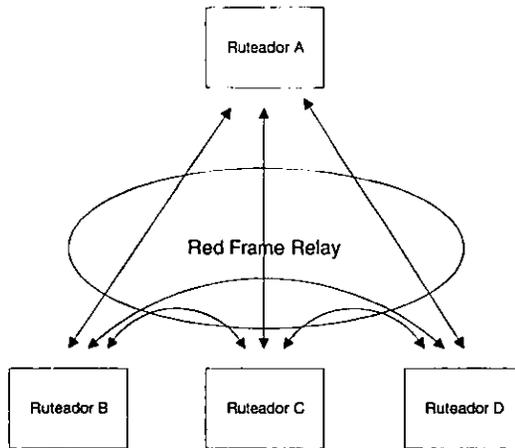
## V.2 ATM Contra Frame Relay

El protocolo *Frame Relay* se desarrolló como resultado de los problemas de desempeño de X.25, y se basa fundamentalmente en él. *Frame Relay* es una forma simplificada de X.25 en la cual la mayoría de las responsabilidades de detección y corrección de errores se transfirieron de los dispositivos intermedios a los dispositivos finales de la red. La alta calidad de las redes modernas han hecho que muchas de las funciones de control de errores de X.25 sean redundantes. Al reducir estas funciones, se reduce el overhead producido por la trama, lo que ha aumentado en gran medida la eficiencia y tasa de transmisión de la línea.

Aunque *Frame Relay* es un estándar *de facto* para la interconexión de redes LAN en diferentes lugares geográficos por medio de ruteadores de alta velocidad, tiene varias desventajas:

- La incapacidad de conmutar conexiones, siendo capaz únicamente de soportar conexiones punto a punto (PVC's, o circuitos virtuales permanentes)
- La incapacidad de soportar conexiones de muy alta velocidad, especialmente aquellas que requieren un desempeño con *jitter* bajo, tales como vídeo o que involucren imágenes con movimiento.

La limitación de soportar únicamente conexiones PVC tiene como consecuencia que las redes Frame Relay tiene que seguir topologías muy rígidas, sin la flexibilidad de poder establecer conexiones directas con dispositivos remotos tal como se puede hacer en una red conmutada.



- a) Conexión de Dispositivos PVC
- b) Conexión de Dispositivos SVC

**Fig. 5.1 Comparación de Servicios PVC y SVC en Frame Relay**

En 1994 surgieron los estándares de SVC (circuito virtual conmutado) para Frame Relay. En la fig. 5.1(a) se muestran cuatro LAN interconectadas utilizando ruteadores y una topología de malla de seis conexiones Frame Relay PVC. Esta configuración requiere un solo puerto lógico en cada uno de los ruteadores y tres canales lógicos separados para cada puerto. Si se necesitan más PVC's para la conexión de malla (p ej. más de 1024), también se pueden necesitar puertos físicos adicionales.

En contraste, en la fig. 5.1(b), los mismos dispositivos se encuentran conectados utilizando Frame Relay SVC. En este caso, cualquiera de los ruteadores puede establecer conexiones conmutadas con base en solicitudes de los demás. En lo que concierne a los ruteadores, ellos piensan que están interconectados con una topología tipo malla; sin embargo, el trabajo de administrar la topología de la red es más sencillo (se tienen muchas menos conexiones permanentes que mantener y reconfigurar cuando la topología de la red cambia) y si uno de los ruteadores llegara a fallar, se puede establecer una nueva ruta a un dispositivo de respaldo.

ATM no se encuentra preparado para competir con Frame Relay a tasas menores de 2 Mbps debido al tamaño fijo de la celda ATM de 53 bytes, que es demasiado inflexible para ser efectivo a velocidades bajas. Por ejemplo, la duración de la celda a 512 kbps es de un milisegundo, comparada con 12 microsegundos a 34 Mbps, por lo que hay un riesgo más grande de que exista un retraso inaceptable en las celdas que están esperando a transmitirse. Además, el sobrecarga extra causado por el formato de la celda se suma al retraso global y daña la tasa de transmisión de la red.

Al reconocer las potencialidades y fuerza que tienen Frame Relay y ATM para diferentes velocidades de transmisión, se han creado estándares que los complementan al especificar interconexiones ATM/Frame Relay, y algunos fabricantes están desarrollando dispositivos de conmutación de redes que soportan tanto Frame Relay como ATM.

### V.3 ATM Contra ISDN

ISDN es una tecnología que se basa en la red telefónica, pero capaz de ofrecer *servicios integrados*. Este tipo de red permite que una compañía optimice su red de telecomunicaciones al compartir las mismas líneas para diferentes propósitos. ISDN fue diseñado para permitir que datos de computadora y transmisión de video relativamente sencilla se puedan transportar a través de las redes telefónicas digitales de hoy en día. Para poder lograrlo, los teléfonos ISDN deben ser capaces de señalizar a la red no sólo el número destino de la llamada, sino también el tipo de conexión que se requiere. La pulsación tradicional de dígitos marcados individualmente ya no proveen suficiente información para el establecimiento de la llamada y se ha desarrollado un sistema de señalización mucho más evolucionado.

ISDN también tiene capacidad de ofrecer ciertos servicios adicionales, tales como la identificación del número que hace la llamada aún antes de contestar, la capacidad de notificar cuando el número deseado se encuentra libre y las llamadas de conferencia tripartita.

Sin embargo, ISDN está limitado por la red telefónica en sí. El problema con las redes telefónicas tradicionales e ISDN es que todas las conexiones de red tienen la misma capacidad (64 kbps) que se necesita para una llamada telefónica. Para algunas aplicaciones es una capacidad muy sobrada, mientras para otras, tales como algunos de los métodos más recientes de interconexión de PCs y LAN y aplicaciones de video, la capacidad es muy pequeña. Por lo tanto, ISDN tiene que dividir o fragmentar la señal para la transmisión y luego reensamblarla en la recepción.

ATM no tiene estas dificultades. En lugar de tener una capacidad fija, puede conmutar conexiones de casi cualquier tasa de bits. Por lo tanto, puede soportar simultáneamente conexiones telefónicas, de LAN o de video. Haciendo una analogía con una carretera, ATM sería una carretera muy ancha (el medio de transmisión), donde las conexiones entre carreteras serían los switches ATM y el tráfico en la carretera representaría los diferentes tipos de tráfico de telecomunicaciones. En una red ISDN, solo

pueden circular por la carretera transportes de un tamaño determinado. Si el tamaño es muy grande, entonces los vehículos viajan semi-vacíos, en caso contrario, la carga debe repartirse entre varios vehículos. Por otro lado, en una red ATM hay varios tamaños de vehículos disponibles, y el usuario decide qué tamaño de vehículo utilizar de acuerdo a sus necesidades.

Puesto que en ATM el usuario puede seleccionar sus necesidades exactas de capacidad antes de la llamada, se maximiza la eficiencia de la red y se mantiene la congestión en un mínimo.

Los servicios complementarios de ISDN también serán soportados por ATM, porque la señalización de acceso a la red Q.2931 a nivel ATM UNI, se basa en la señalización usuario-red de ISDN ( recomendación Q.931 de la ITU-T)

#### **V.4 ATM Contra Gigabit Ethernet**

En un principio, el Modo de Transferencia Asíncrono se veía como la solución para todos los problemas de las redes. Sin embargo, con las mejoras que se le han hecho a TCP/IP y las arquitecturas Ethernet, pareciera ser que hoy existe más de una opción y una opinión en contra de utilizar ATM. Sin embargo, hay varios puntos en los cuales estas nuevas tecnologías (tales como Gigabit Ethernet) aún no pueden competir contra ATM.

##### **V.4.1 Calidad de Servicio (QoS)**

Con Gigabit Ethernet (y soportado por el Protocolo de Reservación de Servicios, RSVP), la transferencia de datos para asegurar la entrega garantizada de información depende de implementaciones específicas de los fabricantes, lo que impide que se pueda tener interoperabilidad y garantía de servicio a través de una plataforma con diferentes equipos. Eso, aunado a la falta de un mecanismo que asegure la reservación de servicios y recursos de manera eficiente, producen áreas de congestión en el núcleo de la red.

En cambio, con ATM, y aunque existen diferencias entre las arquitecturas de switches de diferentes fabricantes, todos tienen capacidades de administración de congestión y de QoS. El uso de protocolos estándar de señalización asegura un grado

muy alto de interoperabilidad tanto a nivel físico como lógico. Además, el QoS ha ido pasando de configuraciones estáticas a protocolos de señalización dinámicos, lo que permite que se adopten diferentes políticas de administración en la red.

#### **V.4.2 Escalabilidad de Ancho de Banda**

Hay gente que opina que la migración de Ethernet de 10 Mbps a Fast Ethernet (100 Mbps), y de ahí a Gigabit Ethernet, es una prueba de la escalabilidad de esa arquitectura. Sin embargo, el hecho de escalar Ethernet a velocidades de gigabits, es un problema no trivial que ha ocasionado la definición de un estándar Gigabit Ethernet que lo único que tiene en común con el resto de la familia Ethernet es el esquema de las tramas. Este estándar aún está sufriendo muchos cambios para poder soportar esas velocidades y proveer control de flujo rudimentario y capacidades de asignación de prioridades.

ATM, por otro lado, fue diseñado para proveer un gran rango de velocidades de conexión. Los estándares soportan desde conexiones a nivel E1 hasta OC-12 (622 Mbps), y se están esperando las ratificaciones para OC-48 (2.4 Gbps) y OC-192 (10 Gbps). Toda la señalización y los protocolos ATM de mayor nivel son completamente compatibles a través de todas las velocidades de las interfaces.

#### **V.4.3 Redes Virtuales y Ruteo**

La migración a un ancho de banda dedicado y conmutado se hizo en respuesta a los tiempos de respuesta cada vez más lentos de las aplicaciones de red; sin embargo, en instalaciones muy grandes el aspecto del ruteo entre subredes todavía es un cuello de botella. Aunque existe una cierta variedad de implementaciones particulares de fabricantes para definir redes lógicas (LAN virtuales, o VLAN) y el ruteo entre ellas, en realidad no existe estándar para VLAN u opciones de conmutación/ruteo de la capa 3.

El estándar IEEE 802.1q solamente resuelve parte del problema, pues todavía debe definir un método estándar para identificar las VLAN; y aunque requiere que asegure la interoperatividad entre los conmutadores y otros dispositivos de red (p.ej. ruteadores y servidores), hay algunos productos que ya eclipsan el trabajo en este estándar. Los conmutadores LAN ahora proveen capacidades de control de puertos y de acceso al

medio, así como de protocolos VLAN. Además, el estándar 802.1q no incluye ninguna de las capacidades que acaban de ser ratificadas en el Multiprotocolo sobre ATM (MPOA), con lo que ahora ATM tiene mecanismos bien definidos para LAN lógicas (LAN Emulation) y capacidades completas de ruteo embebidas en la infraestructura del switch.

#### **V.4.4 Costo**

La familia Ethernet tiene una clara ventaja sobre ATM en cuanto a costo del equipo. Esta ventaja, junto con una gran base instalada, impone una barrera para el desarrollo de instalaciones ATM para escritorio, excepto para algunas aplicaciones específicas. Sin embargo, en cuanto al costo total de migrar hacia una arquitectura de red conmutada, el sobreprecio de instalar ATM en el núcleo es de solamente 20%. Por esta pequeña diferencia, las empresas pueden tomar ventaja de un backbone totalmente interoperante con capacidad adicional de ancho de banda, ruteo muy eficiente integrado, y acceso a calidad de servicio (QoS) a través de toda la red empresarial.

En términos de evaluación, Ethernet-TCP/IP es superior cuando:

- Hay una gran base instalada a considerar
- El costo es el criterio dominante

ATM es superior cuando:

- La escalabilidad y una red robusta es lo importante
- Se requiere calidad de servicio
- Existen múltiples tipos de datos a ser transportados por la red
- Se requiere ruteo conmutado basado en estándares, por desempeño
- Se quieren evitar soluciones propietarias

#### **V.5 IP + ATM**

IP y ATM son dos tecnologías radicalmente diferentes. ATM (orientado a conexión), proporciona un camino predefinido al establecer circuitos a través de una red antes de enviar tráfico. Utilizando celdas de longitud fija y capacidades de QoS (Quality of Service), cada circuito tiene su propio QoS de acuerdo a sus requerimientos. ATM

también tiene su propio protocolo de ruteo, el PNNI (Redes Privadas hacia interfaces de red) basado en conceptos usados por el ruteo IP, donde cada nodo construye una vista completa de la topología de la red y determina el mejor camino con base en esta información y en parámetros de QoS propio de ATM. Mediante esquemas de direccionamiento los nodos pueden ser asociados en grupos, cada uno de estos grupos puede ser representado como una entidad simple en la capa inmediata superior del mecanismo de ruteo.

IP es una tecnología no orientada a conexión, se basa en su capacidad para utilizar cualquier tipo de capa 2 (ethernet, token ring, etc.) y de medio físico (par trenzado, fibra óptica, etc.). Cada nodo (punto de ruteo) dentro de una red IP implica una decisión acerca del siguiente destino que formará la ruta.

Las redes ruteadas se dividen en sistemas autónomos (AS). En grandes redes IP normalmente se utiliza OSPF (abre primero la ruta más corta) o el IS-IS (Sistema Intermediario hacia Sistema Intermediario) los cuales permiten la comunicación sin exponer la información de ruteo interno, esta es una capacidad importante si el tráfico esta fluyendo a través de varios "carriers" o ISPs. Ambos OSPF e IS-IS, son protocolos dinámicos de estado de enlace, donde cada ruteador construye una topología completa de la red y calcula el camino más corto para cada destino en dicha red, normalmente utilizando un algoritmo "Dijkstra". Estos cálculos se colocan en tablas de distribución que se usan para determinar el siguiente salto de un paquete con base en su dirección destino. El resultado consiste en un mecanismo de mejor esfuerzo que no contempla el concepto de QoS o caminos alternos en redes congestionadas.

### **V.5.1 Redes IP - ATM**

A medida que el tráfico fluye el desempeño puede verse afectado por el número de saltos que los paquetes deben dar entre el origen y destino. Un problema realmente grande es el fuerte incremento de cálculos para identificar al camino más corto.

Para lidiar con esto, los proveedores de servicios han adoptado una red en donde los ruteadores rodean un *backbone* ATM y los ruteadores se conectan directamente uno con otro por medio de un circuito de conexión virtual (VCC). Actualmente un gran

número de redes adopta configuraciones híbridas, las cuales permiten obtener lo mejor de ruteo "salto a salto" así como del formato VCC.

### **Tecnología MPLS**

La solución de MPLS (Multiprotocol Label Switching), consiste de una serie de módulos de red así como aplicaciones con servicios de control. Es un sistema para control de red el cual define y monitorea servicios VPN (Virtual Private Network) para proveedores de servicios. Es una tecnología que forma parte de los estándares en comunicación, la cual comienza a surgir y esta basada en swicheo.

MPLS es una tecnología que se desarrolló para obtener las ventajas de tecnologías de Capa 2 como ATM y las de Capa 3 como IP.

### **Tecnología MPLS VPN**

La solución MPLS permite manejar redes privadas virtuales internas y externas (internet y extranet). El producto proporciona el control a la operación del flow-through suministrado, servicios de auditoría y servicios para dimensionar SLA (Service Level Agreement) sobre ambientes IP.

Esta solución es escalable, enfoca sus capacidades hacia tecnologías VPN; suministra y controla servicios IP VPN, esto de acuerdo con el SLA establecido. Este producto complementa la solución de algunas compañías dedicadas a implementaciones y asesorías para la Arquitectura y el Diseño de Redes como CISCO para soluciones sobre VPN basadas en MPLS que simplifica el suministro, la garantía en el servicio así como los procesos de billing, por esto reduce costos para el desarrollo y operación de servicios VPN.

Utilizando la solución de software para MPLS VPN, los servicios que podrían proporcionarse son los siguientes:

- Proporcionar servicios IP utilizando MPLS VPN
- Generación de reportes de auditorías por cada solicitud de servicio

- Llevar a cabo recopilación de datos que permiten medir el desempeño para el SLA
- Evaluación del uso en el servicio por cada VPN

### **Ventajas**

- Una plataforma para el desarrollo acelerado de servicios IP de valor agregado, incluyendo intranets, extranets, voz, multimedia y comercio electrónico
- Privacidad y seguridad igual a la Capa 2 VPNs, ya que distribuye las rutas de un VPN solo hacia los routers que son miembros de esta VPN y por medio del uso de MPLS para efectuar forwarding.
- Facilidad para crear redes virtuales
- IP Class of Service (CoS) con soporte para múltiples clases de servicio dentro de una VPN, así como prioridades a lo largo de las VPNs
- Fácil control de los miembros de la VPN y rápido desarrollo de nuevas VPNs
- Escalable conectividad cualesquiera con cualesquiera para extensas intranets y extranets abarcando múltiples negocios

### **QoS / CoS (Quality of Service / Class of Service)**

CoS se refiere a los métodos que proporcionan servicio diferenciado, en donde la red entrega una clase de servicio basada en la clase de servicio por cada paquete. CoS proporciona categorías específicas de servicio como Gold, Silver y Best-Effort (clases de servicio).

Para el apropiado desarrollo en el servicio deben aplicarse las medidas y políticas QoS a través de la red, desde el primer dispositivo internetwork forwarding (de la Capa 2, un switch o un router) hasta el último dispositivo que tiene la última IP en una estación destino.

La clave de QoS en VPNs en gran escala consiste en la implementación de controles sobre un grupo de clases de servicio que cuentan con aplicaciones agrupadas dentro de ellas. Por ejemplo un proveedor de servicio de red puede implementar tres clases de servicio: High-priority, low latency "clase premium"; un guaranteed-delivery "clase mission-critical"; y low-priority "clase best effort". Cada clase de servicio es

estimado y cotizado apropiadamente y los usuarios pueden adquirir una mezcla de ellos en base a sus necesidades. Por ejemplo usuarios de voz y video-conferencias pueden adquirir servicios de best-effort para el tráfico de correo electrónico y grandes transferencias de archivos.

### **Paquete CISCO IOS QoS/CoS**

El software de CISCO IOS incluye diferentes características de la capa 3 QoS que son particularmente aplicadas a los controles y suministros de una VPN. MPLS habilita la red para utilizar las siguientes características CISCO IOS QoS y construir una arquitectura punto a punto QoS:

- Precedencia IP
- Committed Access Rate (CAR)
- Weighted Random Early Detection (WRED)
- Weighted Fair Queuing (WFQ)
- Generic Traffic Shaping

Las versiones que maneja son IPv4 e IPv6

### **Utilidad de MPLS**

La importancia de una mayor integración entre IP y ATM ha sido ampliamente reconocida, los estándares básicos están ya listos para permitir el desarrollo de redes MPLS de gran escala.

MPLS refuerza muchas capacidades de las tecnologías orientadas a conexión incluyendo ATM, para realzar los mecanismos de mejor esfuerzo de IP. MPLS cuenta con mecanismos de señalización, de esta forma los datagramas IP no necesitan ser interrogados en cada salto a lo largo del trayecto; ellos son simplemente conmutados usando etiquetas. Los protocolos de señalización de MPLS proveen parámetros adicionales para seleccionar la ruta incluyendo por ejemplo ancho de banda.

Mucho del poder de MPLS viene de la forma en que los flujos de IP se mapean hacia LSPs. Con ATM, cada conexión es única, llevando tráfico del punto A al punto B con base en el esquema apropiado de direccionamiento. MPLS provee un mapeo altamente flexible de direcciones IP a LSPs basado en el concepto de clases equivalentes de transporte FEC.

### **Retos en Aplicaciones**

MPLS promete ayudar en dos áreas críticas para los proveedores de servicio: Ingeniería de Tráfico y nuevos servicios generadores de ganancias. Las capacidades de QoS inherentes al estándar son la llave para su éxito.

Los primeros desarrollos de MPLS se han enfocado en la ingeniería de tráfico y solamente para el tráfico de mejor esfuerzo.

Uno de los mayores retos de MPLS es obtener la información relevante de QoS y desarrollar el control dinámico de admisión de conexiones (CAC) y capacidades de ingeniería de tráfico que ya se encuentran presentes y bien entendidas en ATM.

### **V.6 Voz sobre ATM**

Dadas las presiones comerciales que enfrenta cualquier operador de red, ha existido un esfuerzo constante para reducir los costos operativos e incrementar la eficiencia. ATM es una de las herramientas principales en el arsenal del diseñador de redes, para lograr este objetivo. ATM permite el multiplexaje estadístico del tráfico sobre cualquier recurso de la red. Este multiplexaje elimina la necesidad de reservar de antemano recursos para un usuario, puesto que los reserva conforme se van necesitando, dando a los usuarios exclusivamente el ancho de banda que necesitan y cuando lo necesitan. Esto permite que la red soporte más usuarios (típicamente el doble que una red TDM).

Sin embargo, para que una red ATM tenga éxito, debe ser capaz de integrar tráfico de todos los tipos en un sólo flujo multiplexado estadísticamente. Esto implica poder transportar el más demandante de todos los tráficos: Voz. El transporte de voz presenta

un gran número de retos técnicos que deben ser resueltos efectivamente si la red va a proveer un mecanismo efectivo para hacerlo.

Hoy, a través del foro ATM y sus miembros, estos temas han sido tratados y es posible construir y operar una red ATM que satisfaga las necesidades de varios tipos de aplicaciones de voz.

### **Dificultad en la transmisión de voz**

Tal vez es difícil porque la voz y el video están tan íntimamente relacionados con nuestras experiencias diarias, proveen una prueba muy severa de cualquier tecnología de red, y ATM no es diferente en este respecto.

Cualquier aproximación de conmutación de paquetes al transporte de voz enfrenta una serie de retos tecnológicos, los cuales son iguales para cualquier tecnología, sea x.25, Frame Relay, IP o X.25. Estos retos surgen por la naturaleza interactiva y de tiempo real del tráfico de voz. Para entender cómo estos problemas han sido enfrentados por la tecnología ATM actual, primero debemos entender cuáles son esos retos y cómo surgen.

### **Retraso**

El primer tema es el retraso. Para poder mantener una conversación interactiva de extremo a extremo a través de la red, el retraso debe mantenerse al mínimo para asegurar que los subscriptores reciban una calidad de servicio aceptable. Existen dos límites significativos, que se cruzan o rompen cuando el retraso de la red se incrementa.

El primero de estos límites existe por un problema de la red telefónica mundial. Los aparatos telefónicos utilizan 4 cables para conectarse a la red. Sin embargo, la red de larga distancia únicamente utiliza un par de cables para transportar la llamada telefónica. Esta transición de operación de 2 a 4 cables se lleva a cabo por un dispositivo conocido como el 'híbrido', en cada extremo de la red. Sin embargo, los híbridos causan una reflexión de la señal, debido a un desacoplamiento de impedancias irresoluble. El efecto de esto, es que parte de la señal de voz se refleja hacia atrás por cada híbrido y llega al receptor del aparato telefónico. Normalmente esto es imperceptible, puesto que es casi

como escuchar la voz propia a través del aire de la habitación. Sin embargo, si existe un retraso en la red, la señal reflejada se presenta como un eco. El eco es más pronunciado conforme se aumenta el retraso.

A los 30 milisegundos de retraso, el eco es tan significativo que hace muy difícil llevar una conversación normal. Por tanto, una vez que el retraso de un circuito de voz excede este límite, se deben incluir canceladores de eco en la red. Estos dispositivos son caros y complejos. Aún más, estos dispositivos funcionan mejor cuando el retraso es constante, lo cual no es el caso de una red de conmutación de paquetes.

Una vez colocados, los sistemas de cancelación de eco permiten que los retrasos de la red alcancen aproximadamente los 150 milisegundos antes de que se experimente una nueva degradación de la voz. Cuando se excede este nuevo límite, emerge un nuevo problema. A este nivel de retraso, se comienzan a tener problemas significativos para tener una conversación normal. Los patrones de conversación demandan que algunas respuestas del receptor sean recibidas antes de 200 milisegundos, ya que los retrasos mayores causan conversaciones entrecortadas y que ambas partes de la conversación intenten hablar al mismo tiempo. Este tipo de problema se encuentra comúnmente en los enlaces satelitales.

Por estas razones, las redes de alta calidad requieren que el retraso de extremo a extremo para el tráfico de voz sea menor a 25 milisegundos en llamadas nacionales y de 100 milisegundos en llamadas internacionales.

No es inmediatamente obvio el porqué utilizar ATM conlleva problemas de retraso, si después de todo ATM es muy rápido. La dificultad surge de tres áreas:

- Retraso en la formación de paquetes
- Retraso de buffer
- Retraso de codificación

Aún más, estos tres retrasos son comunes a todas las redes de conmutación de paquetes, independientemente de la velocidad de transmisión.

## **Retraso de Construcción de la Celda**

Este retraso es causado por el tiempo que se necesita para llenar un paquete o celda antes de ser transmitirse. Las muestras de voz se reciben a una tasa correspondiente al nivel de compresión de la señal. Por tanto, la voz codificada en PCM llega a una velocidad de 64Kbps. La voz comprimida llegará a tasas aún más bajas (2Kbps, 16Kbps y 8Kbps). Se induce un retraso mientras se espera a que lleven suficientes datos codificados para que se pueda enviar una celda con la menor longitud posible. Mientras que en algunos esquemas de conmutación de paquetes es posible enviar tramas muy pequeñas, esto es poco atractivo por que la eficiencia de cualquier esquema baja conforme la proporción entre la carga y la longitud de los encabezados baja. En el caso de ATM, el tamaño fijo de la celda determina que el retraso es directamente proporcional al nivel de compresión de voz utilizado - a mayor compresión, mayor retraso.

Para ver un ejemplo práctico, si estamos utilizando una compresión de 8kbps y llenando celdas AAL1 de ATM, una celda se llena cada 47 milisegundos. Puesto que la celda no se puede transmitir hasta que esté llena, ya hemos roto nuestro primer límite del tráfico de voz aún antes de haber insertado dicho tráfico en la red. Este problema se puede resolver ya sea con celdas únicamente parcialmente llenas (lo cual es ineficiente) o multiplexando varias llamadas de voz en un sólo VCC de ATM.

La segunda área de retraso proviene de la necesidad de mantener la entrega del tráfico de voz en tiempo real, a través de la red. Cuando se inserta el tráfico a la red, primero debe partirse este tráfico en unidades pequeñas (tramas, paquetes o celdas) para su transmisión. En el destino, estas unidades deben reensamblarse en una copia de la llamada original (el circuito emulado). En el caso de la voz, el tráfico debe reensamblarse en tiempo real sin distorsión temporal.

## **Retraso de Buffer**

Para operar correctamente, la función de reensamble de cualquier tasa constante de bits (CBR) o flujo de datos de tiempo real, requiere que los datos necesarios para reconstruir el tráfico transportado se encuentre disponible en la destinación en el momento correcto en el tiempo. Si una celda se retrasa en el tránsito, la función de

reensamblaje (SAR) puede no tener datos que procesar, lo cual resulta en brechas o espacios vacíos en la conversación.

Para prevenir que esto ocurra, la función SAR acumulará un buffer de información antes de comenzar la reconstrucción del tráfico a partir de las celdas recibidas. El tamaño de este buffer debe exceder el retraso máximo pronosticado propagado por la red para que no ocurran los silencios en la conversación. Sin embargo, el tamaño del buffer se traduce en aún mas retraso, ya que cada celda debe avanzar en el buffer cuando llega.

La implicación de esto es que la Variación de Retraso de la Celda dentro de la red ATM necesita ser estrictamente controlada para poder configurar el tamaño de buffer mínimo, y por lo tanto minimizar el retraso. Por esta razón, es importante ver que esta Variación es el criterio más importante en el diseño del equipo ATM, ya que tiene un impacto muy grande en la red.

### **Retraso de Codificación**

La tercera fuente de retraso ocurre en la codificación de la señal analógica a digital. El deseo de comprimir el tráfico de voz a la tasa de bits mínima mientras se mantiene la calidad, resulta en un retraso de procesamiento. Típicamente, esto se vuelve más significativo en las tasas de bits mas bajas. La familia de algoritmos de Código de Predicción Linear de bajo Retraso (Low Delay Code Excited Linear Prediction, o LD-CELP) son muy populares hoy en día y permiten codificación de alta calidad a tasas de muestreo tan bajas como 16Kbps, con retrasos menores a 10 milisegundos. Sin embargo, como hemos visto, esto puede representar el 50% de nuestro presupuesto.

### **Soporte a la Señalización**

El segundo conjunto de temas se refiere a la utilización eficiente de recursos, la transferencia de control y la información de señalización. Una llamada consiste de dos partes: las muestras de voz y la información de señalización. Esta información incluye el número marcado, el estatus de la llamada e información diversa de ruteo y control. Esta señalización puede ser codificada de diferentes maneras, y puede ser enviada como canal común, canal asociado o DTMF.

Normalmente, varios canales de voz se combinan en un solo circuito. Por ejemplo, un enlace E1 a 2Mbps contiene 30 canales de voz discreta, mientras que un enlace T1 a 1.5Mbps contiene 24. La información de señalización se puede embeber en cada canal discreto de voz (lo que se conoce como señalización por canal asociado) o enviarse por un sólo canal, que contendrá toda la señalización de todos los canales (señalización de canal común).

En el caso más simple, donde el tráfico de voz simplemente es transportado tal cual por la red ATM, podemos únicamente transferir la señalización de un extremo a otro. Sin embargo, en casos más complejos que utilicen señalización de canal común, donde el tráfico de un sitio debe ser conmutado y entregado a más de un destino, las aproximaciones sencillas no funcionan. En estos casos, los canales de señalización deben cerrarse e interpretarse en el switch ATM para que la información correcta pueda pasar al punto final correspondiente. Dado el hecho de que existen muchos mecanismos de señalización, tanto estandarizados como propietarios, la red ATM debe poder entender muchos protocolos de señalización diferentes.

## **Sincronización**

También se debe discutir la sincronización del tráfico. ATM, como su nombre le implica, es asíncrono por naturaleza, pero el transporte de voz requiere que los datos estén sincronizados para mantener la relación temporal entre el que habla y el que escucha. Con aplicaciones sencillas de punto a punto, ambos extremos pueden sincronizarse por medio de dos mecanismo estándares: Adaptive Clocking o Synchronous Residual Time Stamping (SRTS). Estos métodos ajustan el reloj en un extremo del circuito en base al reloj del otro extremo. Adaptive Clocking logra esto monitoreando el tamaño de los buffers SAR de recepción. Entonces ajusta el reloj del extremo 'esclavo' para mantener un tamaño de buffer apropiado.

SRTS monitorea la línea del reloj del extremo 'maestro' del circuito, con respecto a un reloj estándar. La diferencia entre ambos relojes se codifica y transmite como parte del flujo de datos. En el extremo 'esclavo', esta señal de diferencia se extrae y se utiliza para ajustar el reloj esclavo con referencia al reloj estándar.

Sin embargo, ninguno de estos dos mecanismos pueden operar cuando entran en operación servicios multipunto. Por ejemplo, en el caso de SRTS, es claro que no es posible para un extremo esclavo 'A' el ajustar su reloj en respuesta a dos señales diferenciales que se reciben de dos diferentes extremos maestros. Tampoco, en el caso adaptativo, puede un esclavo ajustar su línea de reloj en respuesta a cambios en el tamaño del buffer de dos fuentes diferentes de datos, sin que perjudique a alguna de las dos. Por lo tanto, para servicios multipunto se debe adoptar un modelo de sincronización externa donde cada nodo de la red esté sincronizado con un reloj externo. En la práctica, esto es fácil de lograr por la gran disponibilidad de estándares globales de tiempo.

## **Aplicaciones**

Existen muchas aplicaciones para el transporte de voz sobre ATM. Estas abarcan tanto al constructor de la red corporativa, como al proveedor público de servicios.

Se pueden distinguir tres clases de operadores de red:

- Operadores Nacionales o Internacionales
- Operadores Alternos o Proveedores de Redes de Valor Agregado
- Redes Corporativas (Privadas)

## **Operadores Nacionales o Internacionales**

Estas organizaciones comúnmente tienen un servicio PSTN bastante grande ya instalado, operando sobre infraestructura PDH o SDH/SONET. Además, tienen servicios de redes de datos que soportan a usuarios domésticos y de negocios. En donde el ancho de banda es limitado, existe un fuerte requerimiento de integrar tráfico de voz y datos en una sola red ATM por razones de eficiencia. Esto es particularmente cierto dentro del segmento internacional de una red de un portador de servicios, donde el costo de renta de ancho de banda internacional demanda una máxima eficiencia. Dentro del backbone central, ATM puede ser una valiosa solución para transportar voz y datos hasta los negocios contratantes, ya sea con arquitectura de fibra óptica o de cobre mejorado.

## **Operadores Alternos o Proveedores de Redes de Valor Agregado**

Estas compañías normalmente obtienen licencias para proveer servicios de comunicación en competencia con los operadores a nivel nacional. No son dueños de su infraestructura de transmisión. Por lo tanto, compran ancho de banda del operador primario o forman alianzas con empresas que sí tienen la infraestructura. En estos casos, el costo y la limitación del ancho de banda demandan la eficiencia de ATM, y la integración de servicios de voz y datos. También se debe resaltar que muchos operadores de telefonía celular se encuentran en esta situación, ya que deben construir una red de voz fija para interconectar sus células y enviar mensajes a sus centros de conmutación, y ATM les puede ayudar a mejorar la relación costo-beneficio de la red.

### **Redes Corporativas (Privadas)**

La mayoría de las empresas privadas compran ancho de banda a tarifas comerciales, y deben lograr lo máximo posible con los recursos que se tienen a mano. En cualquier corporación, una parte significativa del tráfico en la red es voz, por lo que la integración de voz y datos en ATM es una meta evidente. En muchos casos, tales organizaciones ya tienen una estructura de red TDM con enlaces E1 o T1. Se pueden integrar estas soluciones en una nueva red ATM, y obtener mejoras en el desempeño de la red y en eficiencia cambiando de TDM a multiplexaje estadístico.

### **Dos Modelos Básicos**

Desde esta perspectiva, surgen dos modelos fundamentales para el transporte de voz: Estos se conocen como 'Voice Trunking' y Conmutación de Voz.

#### ***Voice Trunking***

Normalmente, involucra el tunneling del tráfico de voz a través de una red entre dos extremos finales fijos. Este es un mecanismo apropiados para unir centros de conmutación de voz, PBX, o centros de conmutación de mensajes. No se requiere que la red que la red sea capaz de procesar o terminar señalización, excepto la de utilizar la señalización para detectar canales desocupados. Sin embargo, el gran tamaño de estas redes frecuentemente permiten que se obtengan configuraciones muy eficientes

únicamente utilizando el análisis y uso de mecanismos tradicionales de ingeniería de tráfico de PSTN.

### **Conmutación de Voz**

En este modelo, se necesita que la red ATM interprete la información de señalización de voz y el ruteo de una llamada a través de la red. El switch ATM, quien recibe la llamada, la debe rutear hasta el destino adecuado. Este tipo de funcionalidad es más adecuado para una red VPN.

Esto representaba un gran reto anteriormente, puesto que existían muchos métodos de señalización, la mayoría de ellos propietarios. Hoy, este problema está en vías de superarse. Muchos proveedores venden soluciones basadas en ATM que pueden interpretar la señalización de sus propios conmutadores de voz. Y, lo que es más significativo, la amplia adopción de la señalización de ISDN y QSIG permite que los proveedores ofrezcan una interfaz estándar.

### **Soluciones**

El Foro ATM ha definido tres aproximaciones principales para transportar voz a través de una red ATM. Estos son:

- Servicio de Emulación de Circuitos (CES) - Para transportar tasas de bits de circuitos E1 o T1 entre dos puntos finales.
- Servicio de Emulación Dinámica de Circuitos (DBCES)
- Servicios de Banda Angosta o ATM Trunking, usando AAL2 (aún en desarrollo).

Una cuarta aproximación es el transporte de tráfico de voz que ha sido encapsulado previamente en otro protocolo, por ejemplo, voz sobre IP o Voz sobre Frame Relay.

### **Emulación de Circuitos (CES)**

Se definió por el Foro ATM en enero de 1997. Hoy, representa un estándar estable y confiable, que ha sido ampliamente implementado por proveedores de equipo ATM. Cuando se utiliza CES, la red ATM simplemente provee un mecanismo de transporte

transparente para enlaces estructurados según la especificación G.703/4. La voz se codifica en estos enlaces como si fuera una red TDM normal, utilizando PCM, ADPCM u otros mecanismos de codificación y compresión. La red debe asegurarse que el circuito entregado sea reconstruido exactamente como se recibió. CES es un mecanismo full-duplex, y hace pensar al equipo de voz que tiene un circuito rentado. Esta aproximación es muy valiosa ya que no se tienen que hacer cambios a la red TDM o PBX existente. Un enlace con emulación de circuito puede, de hecho, transportar cualquier tipo o mezcla de tráfico. CES utiliza el mecanismo de adaptación AAL1 para segmentar el tráfico entrante en celdas ATM con la información de sincronía necesaria para asegurar que el circuito pueda ser reensamblado correctamente en el destino. Las ventajas de esto.

## Capítulo VI

### MIGRACIÓN DE X.25 A ATM

#### VI.1 Proyecto de migración

El caso de estudio sobre el que se trabajará para realizar la migración de una red con tecnología X.25 a una red de alta velocidad ATM, es la red de datos de la empresa de telefonía celular Telcel, S.A. de C.V.

Los orígenes de la empresa Telcel se remontan al año 1978 cuando inició la instalación y operación de un sistema de radiotelefonía móvil en el Distrito Federal. En 1984 obtuvo la concesión para explotar la red de servicio radiotelefónico móvil en el área metropolitana de la ciudad de México, bajo la denominación de "Radiomovil DIPSA, S.A. de C.V.". En 1989 surge la marca Telcel cuando comienza a ofrecer los servicios de telefonía celular en la ciudad de Tijuana B.C., al autorizar la Secretaría de Comunicaciones y Transportes la introducción de la telefonía celular en nuestro país. A partir de 1990 expandió los servicios de telefonía celular en el Distrito Federal y su zona metropolitana y paulatinamente ofreció el servicio a nivel nacional. A través de una asociación empresarial estratégica con las compañías Southwestern Bell y France Telecom, dentro de Carso Global Telecom, han construido una empresa sólida en la industria de las telecomunicaciones en México.

El sistema de comunicaciones de la empresa consiste de una red de área amplia para transmitir datos a nivel nacional con presencia en 30 ciudades del país; el protocolo que se utiliza para la red WAN es X.25 y las subredes LAN utilizan tecnología Ethernet.

Se considera como *backbone* de la red nacional a los nodos que componen la región nueve (Distrito Federal); esto se debe a que administrativamente es la más importante y concentra el mayor tráfico de información de toda la red. Actualmente opera en un rango de ocupación de un 80% de su capacidad y picos de hasta el 95%, utilizando aplicaciones y servicios que satisfacen únicamente los requerimientos básicos de la empresa, sin la posibilidad de mejorarlos o añadir nuevos servicios debido a las limitaciones de la tecnología utilizada en la red desde su implementación.

El principal objetivo que se pretende cumplir con la migración de la red Telcel, es brindar un servicio de comunicaciones digitales confiable y eficiente, creando la infraestructura necesaria para que todas las instalaciones de telecomunicaciones que conforman el corporativo, tengan la misma posibilidad de escalabilidad ante las necesidades futuras. De aquí se desprenden varias metas entre las que destacan las siguientes:

- Proveer las capacidades necesarias de transporte en tiempo real para aplicaciones multimedia.
- Facilitar la interconectividad entre LAN's y WAN's. Actualmente ruteadores y puentes necesitan de una mayor conversión protocolaria con el objeto de proporcionar acceso a servicios de área amplia.
- Usar en la medida de lo posible, estándares recientes de ATM. Esto tiene la ventaja de hacer uso de un desarrollo en pleno crecimiento.





**Fig. 6.2** Regiones de la Red Nacional de Datos Telcel

## REGION 9

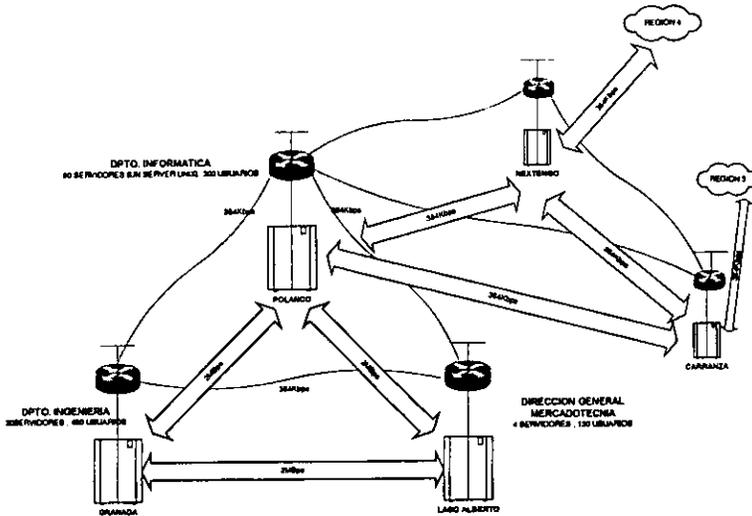


Fig. 6.3 Región 9

### Breve descripción de la región 9

**Nodo Polanco.-** Cuenta con 80 servidores y 300 usuarios. Las aplicaciones que utilizan son administrativas, publicitarias, correo electrónico y algunas aplicaciones de ingeniería. Por otro lado esta área se encarga de monitorear y controlar tráfico en la red de TELCEL, asegurar el óptimo desempeño así como soporte para las diferentes aplicaciones que corren sobre la red. Debido al tráfico que se genera en este nodo resulta imposible aumentar el número de usuarios o servidores, a pesar de las necesidades de la empresa.

La red de información local tiene una velocidad de 10Mbps y este nodo se conecta en forma directa con el Nodo Lago Alberto y el Nodo Polanco a una velocidad de 2Mbps. Los equipos de comunicaciones con los que cuenta son los siguientes:

EQUIPO	FUNCION
SWITCH CISCO X.25 4 puertos seriales	Conexión WAN con las oficinas de los nodos 92 y 95
Router CISCO 2500 4 puertos ethernet y 4 puertos seriales	Ruteo LAN dentro del mismo nodo y hacia la WAN
Switch CISCO Base10TX 24 puertos ethernet	Switcheo entre 45 servidores, 14 switches con conexiones de 5 hubs cada uno y sólo uno tendrá 4 hubs conectados.
Hub CISCO 24 puertos LAN	Conexión a la red LAN de los equipos terminales (workstations) 14 hubs con 24 conexiones cada uno y sólo uno de trece.

Se utiliza un switch x.25 para la conexión WAN, hacia abajo se conecta con un router 2500 que se va a encargar de efectuar el ruteo hacia las diferentes direcciones dentro de los segmentos Ethernet. La red tiene protocolos de comunicación ipx/spx y tcp/ip, predominando este último y tratando de erradicar el primero, así mismo aún se cuenta con algunas aplicaciones que corren sobre x.25. Continuando con el esquema tenemos un switch ethernet 10Mbps el que se encarga de proporcionarle a cada puerto que tiene esta velocidad de manera que se optimiza este ancho de banda sobre todo para equipos que requieran correr a la mayor velocidad por los procesos que realizan (servidores o workstations), hacia este se encuentran conectados hubs para conexiones locales, normalmente se encuentran en un sólo hub, existe alto riesgo de colisiones que originan bajo desempeño de la red e incluso podrían llegar a colapsarla.

**NOTA:** *Este esquema de conectividad se encuentra presente en todos y cada uno de los nodos de TELCEL dentro y fuera de la Cd. de México, únicamente cambia la velocidad de los enlaces.*

**Nodo Granada.-** Es de gran importancia por las actividades de ingeniería de la empresa por lo que requiere sistemas que demandan mayores recursos de cómputo y de red. Se compone de 20 servidores y 400 usuarios, en este nodo se desarrollan diversas actividades como el diseño de planos de equipos para comunicación celular, diseño y desarrollo de radiocelulas y equipo para el control de tráfico celular nacional de todos los subscriptores de la empresa. En este nodo realizan auditorías de control de calidad en los equipos, el análisis, diseño e implementación de nuevos servicios digitales hacia los clientes de la empresa entre otras actividades.

**Nodo Lago Alberto.-** Tiene 4 servidores y 150 usuarios, en esta área se efectúa el desarrollo de negocios, la publicidad de los diferentes servicios y equipos con los que cuenta TELCEL, así mismo aquí se lleva a cabo la dirección de operaciones del negocio, análisis financieros y de mercado, las contrataciones y colocaciones de personal, sistemas de control jurídico, entre otras cosas.

**Nodo Nextengo y Carranza.-** Estos nodos principalmente son un enlace de comunicaciones para la red Telcel, esta ubicado en una central telefónica de Telmex y controla todo el tráfico que entra y sale de la región 9, es de suma importancia que este nodo tenga alta disponibilidad, es decir, sistemas de redundancia y niveles de servicio óptimos.

Tienen 3 servidor y 40 usuarios entre ambos nodos.

## REGION 4

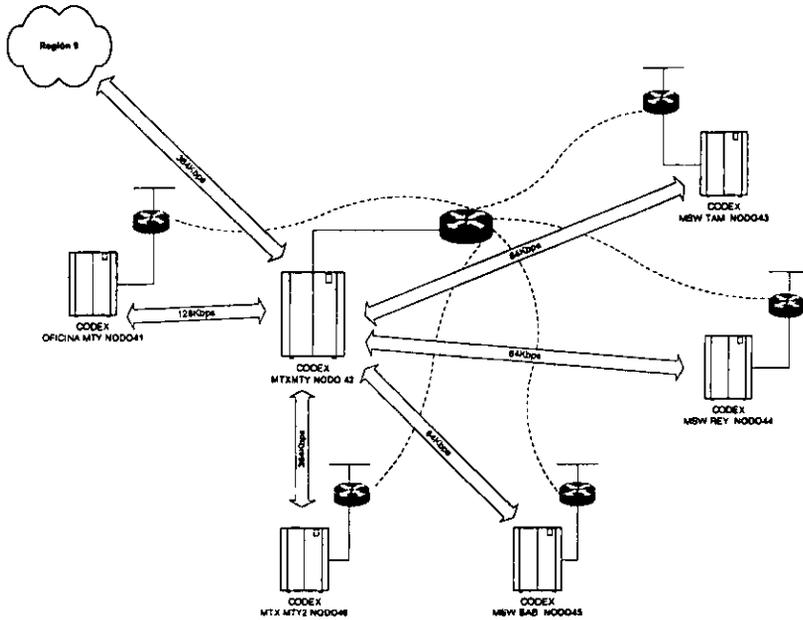


Fig. 6.4 Esquema de la región 4

**Nodo Monterrey 1.-** Este nodo está conectado a la Cd. de México. Permite la conectividad del Distrito Federal con el resto de las sucursales en Monterrey. Este nodo cuenta con servidores y 45 usuarios. Los equipos de comunicaciones y cómputo son iguales en cada uno de los sitios de Monterrey y las aplicaciones de software. En este nodo se centraliza la mayor cantidad de actividades contables, administrativas, gerenciales y publicitarias. El equipo que tienen es el siguiente:

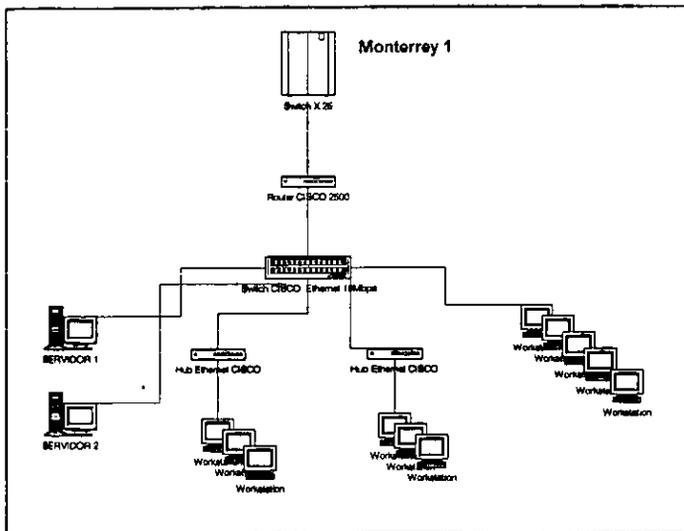


Fig. 6.5 Esquema del nodo de Monterrey (42)

Cada servidor se conecta a uno de los 12 puertos del switch de manera que cada equipo contara con 10MBps para sus procesos, por otro lado hay 5 workstations conectadas directamente al switch ya que procesan aplicaciones administrativas y gráficas que requieren una mayor velocidad. Por último se conectan tres hubs para 60 usuarios compartiendo cada hub 10Mbps.

El switch en uno de sus puertos Ethernet conecta con el router 2500 efectuando el ruteo de las diferentes redes a lo largo de TELCEL, el router 2500 se conecta con un puerto Ethernet al switch x.25 y este a su vez por uno de sus puertos seriales configurados para comunicación x.25 se enlaza con la Cd. de México así como con el Nodo Monterrey 2 y 41 a una velocidad de 384Kbps y con los nodos 45,44 y 48 a una velocidad de 128Kbps.

**Nodo Monterrey 3.-** Cuenta con un servidor y 35 usuarios que acceden en ocasiones información del Nodo Monterrey 1, tienen software administrativo y aquí trabajan con ingeniería. Debido a estos requerimientos el esquema es igual al del Nodo Monterrey 1, solo que cuentan con menos equipo de cómputo, es decir, cuentan con el siguiente equipo:

Al switch Ethernet se conectan los dos servidores, dos hubs y 7 usuarios de ingeniería, así mismo a cada uno de los hubs se conectan 17 y 18 usuarios respectivamente, los cuales comparten 10Mbps por cada hub y esta velocidad a su vez se divide entre el número de conexiones en cada hub.

**Nodo Tampico, 44 y 45.-** Cuentan con la misma configuración e incluso el mismo número de usuarios, cada uno de estos sitios tiene un servidor y 20 usuarios. Estos nodos se conectan punto a punto con el Nodo Monterrey 1 con un enlace de 128Kbps, teniendo software administrativo y algo de ingeniería. El equipo es el siguiente:

**Nodo Monterrey 2.-** Cuenta con 40 usuarios, 1 servidor y un enlace de 128Kbps. Al igual que los anteriores, el esquema de comunicaciones de red LAN y WAN es el mismo y las características del equipo son las siguientes:

Los cinco nodos comparten recursos de la red, pero principalmente esto ocurre entre los nodos Monterrey 1 y Monterrey 2, e incluso en algunas ocasiones entre el Nodo Monterrey 1 y las oficinas de la Cd. De México, tendiendo a incrementarse este tipo de conexiones a corto plazo

**REGION 5**

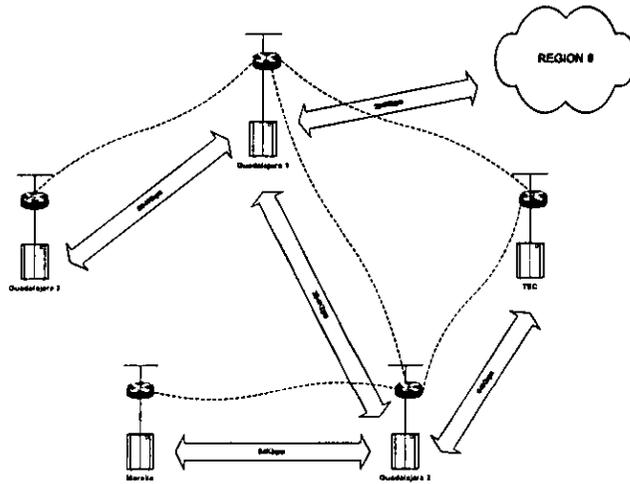


Fig. 6.6 Esquema de la región 5

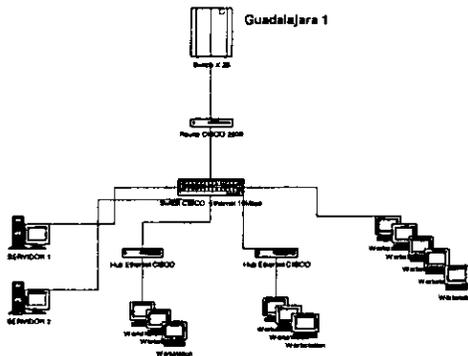


Fig. 6.7 Esquema del nodo Guadalajara

## Breve Descripción de la región 5

**Nodo Guadalajara 1.-** Este nodo cuenta con 2 servidores y 47 usuarios, aquí se realizan enlaces hacia Oficinas en la Cd. de México, por otro lado se corren aplicaciones administrativas, ingenieriles y publicitarias, lo cual origina que se busque contar con la mejor tecnología de comunicaciones. El canal de comunicación hacia la Cd. de México es de 384Kbps y la red interna corre a 10Mbps en configuración Ethernet.

Al switch se conectan dos servidores, dos hubs y 15 usuarios por requerimientos de procesamiento, por otro lado a los dos hubs se conectan 16 usuarios en cada uno, así mismo el switch en uno de sus puertos ethernet conecta con el router 2500 efectuando el ruteo de las diferentes redes a lo largo de TELCEL, el router 2500 se conecta con un puerto ethernet al switch x.25 y este a su vez por uno de sus puertos seriales configurados para comunicación x.25 se enlaza con la Cd. de México como acceso WAN y con otros dos nodos (51 y 55) a una velocidad de 384Kbps hacia cada uno de ellos.

**Nodo Guadalajara 3.-** Cuenta con 1 servidor y 38 usuarios, trabajando con aplicaciones administrativas, ingeniería y publicidad de manera muy similar al Nodo Guadalajara 1, teniendo en ocasiones que acceder datos de este otro nodo, el equipo con el que cuenta es el siguiente:

La forma como se conectan los diferentes equipo es igual que en el nodo anterior, todos siguen el mismo esquema y configuraciones.

Cuenta con una conexión LAN a 10Mbps y una conexión WAN con el Nodo Guadalajara 1 de 384Kbps.

**Nodo Morelia.-** Cuenta con 1 servidor y 18 usuarios, trabajando con aplicaciones administrativas y publicitarias, el equipo con el que cuenta es el siguiente:

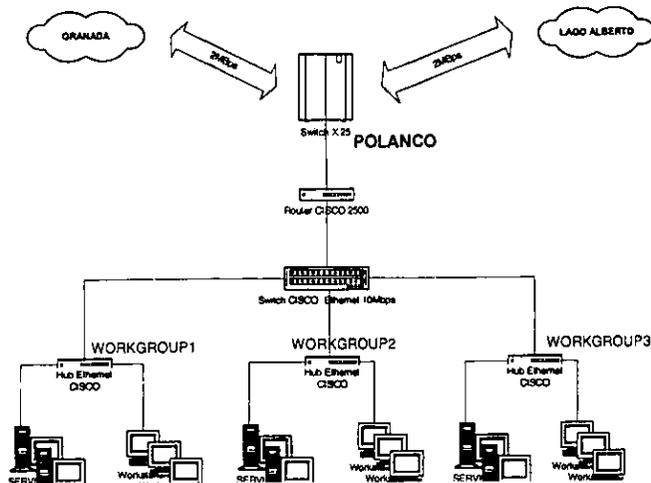
La forma como se conectan los diferentes equipos es igual que en el nodo anterior, todos siguen el mismo esquema y configuraciones.

**Nodo Guadalajara 2.-** Cuenta con 1 servidor y 28 usuarios, trabajando con aplicaciones administrativas e ingenieriles de manera muy similar al Nodo Guadalajara 1, teniendo en ocasiones que acceder datos a los demás nodos de la región. El equipo con el que cuenta es el siguiente:

Cuenta con una conexión LAN de 10Mbps y una conexión WAN hacia el Nodo Guadalajara 1 de 384Kbps y hacia los otros dos nodos a 128Kbps.

**Nodo Tecoman.-** Cuenta con 1 servidor y 17 usuarios, trabajando con aplicaciones administrativas, el equipo con el que cuenta es el siguiente:

Cuenta con una conexión LAN de 10Mbps y una conexión WAN de 128Kbps.



### VI.3 Propuesta de solución

Actualmente, el 90 por ciento de la utilización de poder de cómputo reside en computadoras de escritorio y esta utilización está creciendo aún más. Las aplicaciones distribuidas cada vez consumen un mayor ancho de banda, y la popularización de Internet y aplicaciones basadas en WEB están llevando a las arquitecturas LAN tradicionales al límite. Las comunicaciones de voz se han incrementado significativamente y cada vez tienen mayor dependencia en sistemas centralizados de correo de voz. Las redes internas son una herramienta crítica para el flujo de información.

Tradicionalmente, las comunicaciones de área local y de área amplia permanecen separadas desde el punto de vista lógico. En una LAN, el ancho de banda es sumamente económico y la conectividad se limita únicamente por el costo del hardware y la implementación. En una WAN, el ancho de banda es el costo principal y el tráfico sensible al retraso, como la voz, se mantiene separado de los datos. Sin embargo, el desarrollo de nuevas aplicaciones y la nueva economía, están forzando que estas convenciones converjan.

Las aplicaciones de hoy día que manejan voz y video, requieren un desempeño mejor y más predecible de LANs y WANs. Además, necesitan que la WAN reconozca (y otorgue tratamiento diferente) al distinto tráfico que va dirigido hacia las LANs, por lo que se necesita forzosamente la integración de ambas redes.

ATM es una de las tecnologías más efectivas para esta integración LAN/WAN. ATM puede soportar cualquier tipo de tráfico en *streams* separados o mezclados, tráfico sensible a los retrasos y tráfico de datos normal.

Adicionalmente, ATM puede escalar de bajas a altas velocidades. Ha sido adoptado por una gran cantidad de proveedores de equipo para la industria, desde el mercado de LANs hasta los PBX. Con ATM, es posible integrar LANs con WANs, soportar las aplicaciones emergentes, y soportar los protocolos ya existentes dándoles una eficiencia adicional.

Como se pudo apreciar en el estudio de la situación actual, la región 9 (D.F.) es la que mayores problemas presenta de tráfico y tiempos de respuesta, por lo que la propuesta es migrar en una primera fase, los switches principales de dicha región (Lago Alberto, Polanco, Granada) así como Nextengo, para evitar un cuello de botella al establecer conexiones desde la región 4 (la segunda más importante de la red nacional) hacia el DF. Posteriormente, sería necesario cambiar los nodos de Carranza, Guadalajara y Monterrey en una segunda fase.

Como parte de la solución, se contempla la posibilidad de incorporar la transmisión de voz sobre ATM, ya que es posible utilizar la misma infraestructura ya existente (se tienen más de 20 enlaces E1). También es posible unificar y mejorar las LANs de la empresa por medio de LAN Emulation y switches Ethernet-ATM.

A continuación se presenta el esquema de la solución:

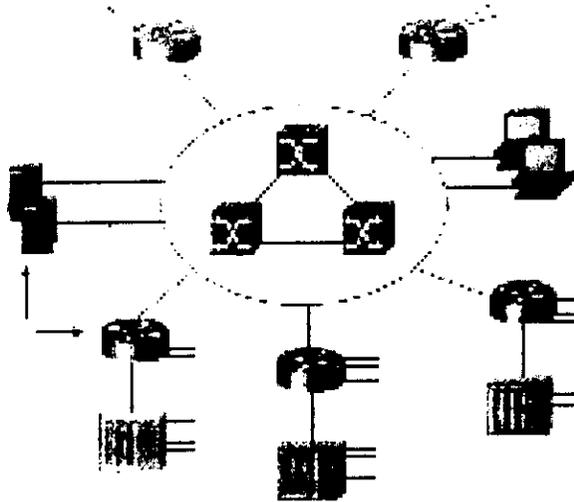


Figura 6.9. Solución ATM

En la figura, se muestra como el Backbone está formado por los Switches ATM. Estos switches se pueden conectar tanto a tarjetas ATM en la máquina del usuario final, como a ruteadores con capacidad ATM, para poder utilizar LAN emuladas. Para completar la solución, se propone la instalación de switches ATM-Ethernet (EAS). Las principales funciones de cada EAS, son:

- Conmutación de tramas entre puertos Ethernet
- Conmutación de celdas hacia los switches ATM
- Soporte a clientes de emulación de redes LAN

La diferencia entre la anterior y la nueva configuración es que mientras las estaciones de trabajo siguen conectadas a un concentrador Ethernet, cada concentrador está dividido en diferentes subredes, las cuales están conectadas individualmente a un puerto conmutado del EAS. Esto mejora el ancho de banda disponible para cada grupo de trabajo, mientras que reduce el número de computadoras por cada segmento Ethernet.

Se evaluó la opción de utilizar ruteadores en lugar de switches haciendo un análisis del tipo de tráfico de la red con la ayuda de un analizador de protocolos

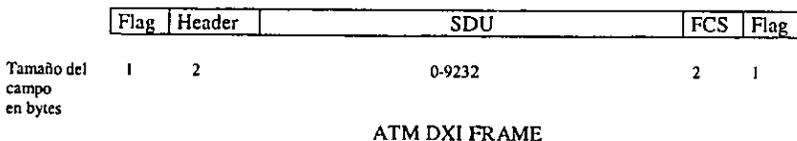
(Internet Adviser – Hewlett Packard). El resultado fue que el tráfico originado por IP entre estaciones de trabajo en grupos de trabajo homogéneos fue el mayor con cerca del 70%. El tráfico originado por broadcast es muy pequeño y el de otros protocolos (LAN-manager y DECnet) representó el 15 %.

Como se necesita mantener el tráfico broadcast entre diferentes áreas, la mejor solución para manejar esta situación es el uso de switches. Con esta solución se incrementa notablemente el desempeño de la red. Por otro lado, se han configurado dos tipos de servidores: el primer tipo es de uso local para dos o tres grupos de trabajo (servidores de aplicación), los cuales están conectados a los switches Ethernet-ATM por medio de enlaces dedicados a 10 Mbps. El segundo tipo de servidores es de uso global, cada servidor es conectado directamente al switch ATM mediante un enlace de 10 Mbps. Esto permite una mejor logística y facilita la administración para aplicaciones de cliente-servidor. La nueva posición de los servidores de uso global en combinación con la alta velocidad de operación de ATM, ayudará a aprovechar al máximo el hardware de los servidores.

### Interconexión entre ATM y X.25

Para poder utilizar la funcionalidad de ATM lo más pronto posible, sin necesidad de migrar completamente toda la red, el Foro ATM desarrolló un estándar conocido como *Interfase de Intercambio de Datos ATM* (DXI, Data Exchange Interface). Este estándar se utiliza para proveer interfaces UNI entre ruteadores y la red ATM. La Unidad de Servicio de Datos de ATM (ADSU) recibe los datos del ruteador en formato ATM DXI, a través de una Interface Serial de Alta Velocidad (HSSI). El DSU convierte los datos en celdas ATM y los transfiere a la red.

En el ruteador, los datos de los protocolos de mayor nivel (tal como X.25) se encapsulan en el formato de trama ATM DXI.



El ruteador, configurado como un dispositivo DTE, se conecta al ADSU. El ADSU se configura como un dispositivo DCE. El ruteador envía las tramas ATM DXI al ADSU, que convierte las tramas a celdas ATM, procesándolas a través de las

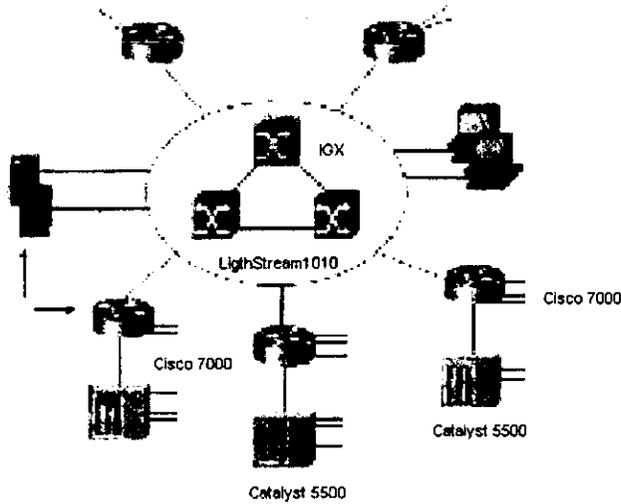
capas AAL5 CS y SAR. La capa ATM le agrega el encabezado y las celdas se envían a la interface ATM UNI.

### **Solución Particular**

Se eligió CISCO como el proveedor de tecnología ATM a utilizar, tanto por su precio como por su adhesión a los estándares, así como por que proporciona una variedad de productos que permiten ofrecer una solución total. El equipo requerido es el siguiente:

- Switches ATM de datos: LigthStream 1010
- Switches ATM para conexión con PBX: StrataCom IGX
- Ruteadores: Catalyst 4700
- EAS: Catalyst 5500

La solución quedaría como se ve en la figura 6.10.



**Fig. 6.10** Solución con CISCO

### **Catalyst 5500**

El switch Catalyst 5500 provee conmutación de alto rendimiento entre estaciones de trabajo, servidores, switches y ruteadores. Su módulo de LAN es un switch con 13 ranuras. La Ranura 1 está reservada para el módulo supervisor de ingeniería, que provee conmutación, administración local y remota, y enlaces duales Fast Ethernet. La ranura 2 está disponible para un segundo módulo de supervisión, redundante, o cualquier otro módulo soportado. Las Ranuras 3 a 12 están disponibles. Soporta Ethernet, FastEthernet, FDDI/CDDI, ATM Lan Emulation, y se puede conectar a un switch LighStream 1010.

Las ventajas que ofrece utilizar este switch para LAN, son las siguientes:

- Gran ancho de banda
- Calidad de Servicio (QoS)
- Bajo Costo
- Facilidad de configuración.

## **Cisco 7000**

Para ofrecer servicios avanzados de interconexión, se debe de utilizar, adicionalmente, un ruteador, tal como se muestra en la figura 6.10. Los servicios adicionales son los siguientes:

- Broadcast Firewalling
- Direccionamiento Jerárquico
- Comunicación entre LANs de topología diferente
- Rápida Convergencia
- Políticas de Ruteo
- Ruteo de QoS
- Seguridad
- Redundancia y balance
- Administración del flujo de tráfico
- Membresía para grupos multimedia.

La principal característica de este ruteador es el poseer la primera interfase de ruteo nativa de ATM, el Procesador de Interfase ATM (AIP), la cual es clave para habilitar la integración de redes LAN y WAN ya existentes, con redes basadas en ATM.

El AIP cuenta con capacidades sofisticadas de señalización ATM y administración de tráfico, lo cual también permite el desarrollo de servicios como las VLANs, ya que les permite interconectarse unas con otras o con redes externas.

## **LigthStream 1010**

Esta familia de switches está especialmente diseñada para backbones. Incorpora soporte para las especificaciones más recientes del foro ATM. Soporta una gran cantidad de interfaces modulares y de WAN ATM.

Para poder soportar las ráfagas de tráfico generadas por los switches LAN y los ruteadores, este switch posee mecanismos avanzados de administración de tráfico. Tiene un mecanismo inteligente que le permite descartar paquetes completos de datos, en lugar de descartar celdas individuales, cuando es necesario, lo cual mejora el rendimiento para protocolos tales como TCP/IP e IPX. También soporta las

especificaciones mas recientes de control de congestión, como la Tasa de Bits Disponible ABR del Foro ATM. Esta especificación le permite al LigthStream 1010 hacer mas lentas las fuentes de tráfico, antes de que la congestión se vuelva excesiva.

### **StrataCom IGX**

Para interconexión de redes de área amplia, los datos que fluyen de las LANs entre diferentes sitios de la empresa, se agregan en el ruteador y después se mezclan con voz. Tradicionalmente, los backbones de una empresa utilizan tecnología TDM. Sin embargo, conforme el uso de LANs ha explotado y equipo TDM antiguo se ha depreciado completamente, se pueden justificar por costo nuevas soluciones. La familia de switches Cisco/StrataCom IGX provee el enlace necesario entre los datos de LAN de altas velocidades y las velocidades de voz, mas bajas.

Con el switch IGX, se puede aprovechar ATM para bajar costos, de la siguiente manera:

- Aplicar tarifas de utilización en el diseño de la red para los PVC's origen
- Combinar múltiples redes en una sola red multiservicios.
- Optimizar la red de transmisión con herramientas de diseño.

### **Costos de los equipos enlaces**

#### **CISCO SYSTEMS**

<b>Stratacom IGX 8400</b> (Conectividad LAN-WAN)	<b>\$58,675</b>
Chasis IGX8400 incluyendo fuente de poder, enlace de línea privada, interfaz para voz.	<b>\$25,490</b>
4 puertos ATM OC3/STM-1 (SMF, MMF, electrical)	<b>\$3,125</b>
8 Puertos T1/E1	<b>\$8,550</b>
8 Puertos T1/E1 o J1	<b>\$3,150</b>

(channel associated signaling [CAS]  
and common channel signaling [CCS])

4 Jumpers para conexión multimodo  
con fibra óptica

**\$560**

Multiplexor inverso para enlaces E1  
Redundant Network  
(Processor Module ? 32MB DRAM)

**\$1,150**

Módulo de Administración y monitoreo  
Alarm Relay Module  
Fuente de poder redundante

**\$16,650**

**ROUTER 7140 - 2MM3 VPN**  
(Ruteo LAN)

**\$52,462**

Chasis Router 7140  
Fuente de poder, incluyendo ATM Data  
Terminal Exchange, Frame Relay, HDLC,  
PPP, SMDS

**\$29,550**

2 Puertos Multimodo ATM OC-3

**\$2,456**

Módulo de administración y monitoreo  
Fuente de Poder redundante

**\$20,456**

**LIGHTSTREAM 1010**  
(Conmutación Ethernet ATM)

**\$ 21,550**

LightStream 1010 Chasis  
AC Power Cord North  
America

**\$2,750**

Light Stream 1010 AC Power  
Supply

**\$1,250**

IISP&PNN1 Feature Set-Installed	<b>\$2,500</b>
ATM Switch Processor with FC-Per-Class Queuing	<b>\$5,600</b>
LightStream 1010/C5500 Carrier Module (Installed)	<b>\$1,200</b>
4 Port STS-3c/STM-1 Multimode Fiber PAM	<b>\$8,250</b>
<b>CATALYST 5500 Equipo ATM-ETHERNET Segment</b>	<b>\$21,730</b>
Catalyst 5500 Chasis	<b>\$995</b>
Catalyst 5000/5505 AC Power Supply	<b>\$1,250</b>
Catalyst 5002/5500 Supervisor 1 (100BaseTX, 2 port)	<b>\$4,495</b>
Catalyst 5000 Ethernet Switching Module (10BaseT, 24 Port)	<b>\$4,995</b>
Catalyst 5000 ATM OC-3 LANE MODULE DUAL PHY (MMF,SC)	<b>\$9,995</b>
<b>TOTAL CON EQUIPO CISCO Incluye un año de mantenimiento</b>	<b>\$ 154,417</b>

## **COSTOS ENLACES SERVICIO TELMEX PARA CADA NODO**

Enlace a 64KB en el área metropolitana costo inicial **\$2,400** y renta mensual **\$640**, el contrato se da por un periodo mínimo de un año, en caso de cancelación antes del vencimiento, el cliente se compromete a pagar las mensualidades no cubiertas, el tiempo de entrega en los servicios nacionales, es de ocho a doce semanas a partir de la fecha que sean contratados, a los precios antes descritos se deberá agregar el 15%

Enlace E1 2MB en el área metropolitana costo inicial **\$11,800** y renta mensual **\$1,350** el contrato se da por un periodo mínimo de un año, en caso de cancelación antes del vencimiento, el cliente se compromete a pagar las mensualidades no cubiertas, el tiempo de entrega en los servicios nacionales, es de ocho a doce semanas a partir de la fecha que sean contratados, a los precios antes descritos se deberá agregar el 15%

### **VI.4 PROPUESTA DE IMPLEMENTACION**

Debido a la inversión que debe realizarse y buscando minimizar los tiempos muertos en transferencias de información dentro de la red Telcel, la implementación de la nueva tecnología ATM se divide en tres etapas:

1. Migración de los tres principales nodos dentro de la Cd. De México incluyendo un nodo más en el sitio Nextengo.
2. Migración de los nodos Carranza, Monterrey y Guadalajara
3. Migración de los nodos restantes de la red Telcel que justifiquen el aprovechamiento de la nueva tecnología.

Se decide migrar cuatro nodos durante la primera etapa, comenzando por los tres nodos de la Cd. De México debido a su importancia dentro del esquema de red Telcel, integrándose dentro del plan la migración del nodo Nextengo por ser el siguiente en importancia en la transferencia de información así como debido a la conectividad requerida del backbone (nombre asignado a los tres nodos importantes en la Cd. De México, por la complejidad que representan) hacia los nodos externos de Nextengo y Carranza.

La migración de los nodos Carranza, Monterrey (Región 4) y Guadalajara (Región 5) complementarán la solución de interconectividad requerida, mientras que para el resto de la red Telcel continuará utilizándose el esquema de X.25. Esta secuencia sugerida se basa en que los nodos involucrados en la etapa 3 no presentan problemas críticos en aplicaciones, transferencias de información y ancho de banda como sucede en los nodos de la etapa 1 y 2. Por lo que, si algún nodo lo requiriese podría cambiarse durante la tercera etapa.

#### **VI.4.1 Etapa 1**

Todo el tráfico de producción continuará viajando por la red X.25 mientras que por la red ATM existirá solamente tráfico de prueba.

La solución considera tener 5 enlaces E1 a 2MB cada uno de ellos. Inicialmente se utilizarán 4 de estos enlaces para el trabajo paralelo de la nueva red ATM dejando el actual enlace E1 de 2MB para trabajar con la red X.25. En cuanto toda la red ATM se encuentre en producción, se asignará ese quinto enlace a la nueva red.

El orden para los reemplazos en el equipo es el siguiente:

1. Reemplazo del equipo en el nodo de Ingeniería
2. Nodo Informática
3. Nodo Dirección General de Mercadotecnia
4. Nodo Nextengo

Este orden debido a las necesidades de comunicación, y previniendo posibles contingencias, sobre todo con el nodo principal Dirección General de Mercadotecnia que requiere de comunicación confiable, constante y no es posible arriesgarlo con posibles problemas de conexión y se queda como tercer nodo a migrar en esta primera etapa sobre todo para tomar experiencia con los dos anteriores.

Pasos a seguir para realizar la etapa 1 de migración:

- Instalación y configuración del anillo de switches WAN ATM Stratacom 8500 con sus 4 enlaces E1
- Instalación y configuración de los switches Ethernet ATM (EAS) así como la adaptación a los switches LAN ATM Lighstream 1010

- Pruebas exhaustivas en desempeño

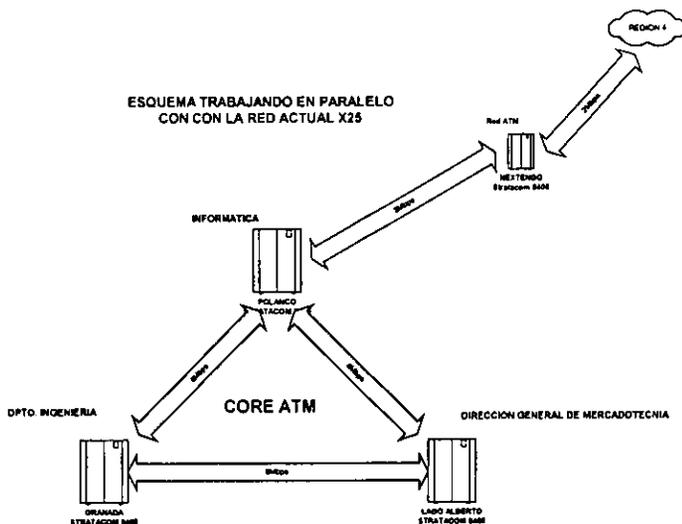


Fig. 6.11 Migración

Una vez comprobado el correcto funcionamiento de la infraestructura armada y habiendo concluido el periodo de pruebas comienza la desconexión del concentrador

Ethernet conectado hacia el ruteador LAN CODEX 2500 en el ambiente anterior X.25 y conectarlo ahora hacia el EAS para el nuevo trabajo sobre ambiente WAN ATM. Será necesario desconectar cada concentrador Ethernet que se enlaza con ruteadores X.25, re-configurarlos y conectarlos con su respectivo switch EAS, como se mencionó en un principio para cada una de las regiones migradas. Realizando el proceso de forma simultánea dentro del backbone así como para el nodo Nextengo, de tal forma que el sistema nuevo completo arranque para los 4 sitios en la misma fecha.





## CONCLUSIONES

La obtención oportuna de información en las empresas se ha vuelto un factor tan importante para su éxito como la producción misma de bienes y servicios. En la actualidad las empresas tienen una necesidad cada vez más grande de contar con información actualizada, a la vez que la automatización de los procesos en la misma se hacen vitales para su adecuada operación.

El nuevo siglo trae consigo nuevas necesidades así como exigencias en el intercambio de información, así mismo repercute esto en las tecnologías de cómputo, sistemas operativos con interfaces gráficas, procesadores de documentos y manejadores de bases de datos, comunicaciones remotas desde los sitios donde se encuentren mediante sistemas notebook, transferencias de mensajería electrónica llevando voz, datos y video dentro de estos paquetes, en fin paquetes de software muchísimo más poderosos que sus antecesores los cuales requieren de la existencia de una plataforma de red robusta, rápida y confiable, con tecnología de procesadores de terahertz para procesamientos rápidos, memorias principales de varios gigabytes y capacidades en discos duros de decenas y cientos de gigabytes así como el manejo de lectoras ópticas, unidades de respaldo hacia CD ROMs por la velocidad de acceso y sin fin de necesidades que surgen gracias a esta ola de nuevos sistemas de información.

Durante la evolución de las redes de datos, cada fabricante decide basar sus esquemas en sistemas propietarios e intercomunicar sus equipos, esto porque estos sistemas les brindaban seguridad y garantizaban su servicio así como su mantenimiento por contar con expertos dedicados únicamente a estos sistemas, la principal característica que encontramos hoy en día es la necesidad de interconectar diferentes equipos, así como diversos sistemas de procesamiento de información que no siempre utilizan los mismos esquemas de comunicación, esto nos lleva a la búsqueda de tecnologías abiertas que se manejen por estándares mundiales y nos permita interactuar con ellos utilizando estos parámetros estándares haciéndonos menos especialistas en los sistemas y más enfocados al manejo de estándares.

Como resultado de los puntos antes mencionados consideramos que hoy por hoy la tecnología de redes que cumple con los requerimientos del siglo XXI es ATM, por

lo que nuestra propuesta-estudio de solución en el esquema actual de la red TELCEL se enfoca en esos puntos, así como en la capacidad de ofrecer posibilidades de superar las limitantes que se tienen con tecnologías anteriores, interconectar redes independientemente del protocolo que se maneje, y esto gracias a que ATM tiene la capacidad de interconectarse con diferentes sistemas sin problema utilizando alguna de las múltiples interfaces con las que cuentan los equipos ATM, esto permite la versatilidad de conectar diferentes tipos de redes LAN que se encuentran en cualquier otro sitio y compartir recursos como si se tratara de la misma red, siendo las conexiones transparentes para el usuario. ATM entre otras características cuenta con un mejor aprovechamiento en el ancho de banda pues cuenta con una asignación dinámica del ancho de banda esto es importante para aplicaciones que requieren una tasa de transmisión constante y grandes cantidades de información.

ATM es sin lugar a dudas una nueva tecnología que puede ser utilizada para aplicaciones que demanden gran ancho de banda, donde están implicadas las transmisiones de voz, datos y video. Permitiendo además a los proveedores de servicios de datos o de voz un medio eficaz de transporte que permita hacer un uso óptimo del ancho de banda disponible, teniendo mayor capacidad y mejorando la calidad del servicio. ATM permitirá en un futuro no muy lejano, la introducción de nuevos tipos de servicios de video y voz en redes de comunicaciones administradas en forma muy sencilla y con los mínimos costos.

En lo referente al diseño propuesto en esta tesis, la elección de la tecnología ATM se baso principalmente en que esta tecnología no solo cubre los requerimientos actuales en el diseño de la red sino que nos ofrece escalabilidad tanto en velocidad como en crecimiento de la misma, ya que permite el incremento paulatino en número de puertos y es compatible con las tecnologías que en un momento dado se requiera utilizar, independientemente de su velocidad.

ATM es la única tecnología actualmente probada y certificada que en la actualidad nos permite integrar en un todo universal, cualquier tipo de red LAN, enlaces de circuitos conmutados, comunicaciones seriales y transmisiones de datos a altas velocidades por Frame Relay, aplicaciones de video, etc.

Otro punto importante de la tecnología ATM es que nos permite contar con un sistema que cuente una plataforma adecuada que pueda configurarse de formas muy variadas y que tenga la capacidad para migrar hacia nuevas tecnologías sin quedar obsoleta conforme surjan nuevos estándares en redes de comunicaciones, así como la posibilidad de analizar el tráfico de datos en el canal de comunicación a una velocidad elevada (tiempo real) con el suficiente grado de exactitud para un diagnóstico rápido de problemas.

Para concluir mencionaremos que el esquema de nueva tecnología en redes para Grupo TELCEL que proponemos va dirigido a concientizar a la gente a cargo de las tecnologías de información en dicho Grupo, que observen detenidamente los esquemas con los que cuentan actualmente y en base a esto dar un siguiente paso tecnológico ubicados en la realidad que vivimos, así como el mundo tecnológico que nos espera.

## BIBLIOGRAFIA

### Libros:

Mc Dysan, David E. & Spohn, Darren L. "ATM: Theory and Application"  
Mc graw Hill. USA 1994

Minoli, Daniel & Vitella, Michael "ATM & Cell Relay Service for Corporate  
Enviroments. Mc Graw Hill. 1994

Stallings, William "ISDN and Broadband ISDN"  
Prentice Hall, USA 1994

Stallings, William "Local and Metropolitan Area Networks"  
Prentice Hall, USA 1994

Stallings, William "Networking Standards"  
Prentice Hall, USA 1994

McDysan, David E. & Spohn, Darren L. "ATM: THEORY AND  
APPLICATION"  
Mc Graw Hill, USA 1994

Stallings, William. " ISDN, FRAME RELAY & ATM"  
Prentice Hall, USA 1995

Miller, Mark A.P.E. "Analyzing Broadband Networks: Frame Relay ,  
SMDS, & ATM. M&T Books. USA 1995

Tanenbaum, Andrew S. "Computer Networks"  
Mc Graw Hill , México 1995

James Martin, et al "Asynchronous Transfer Mode : Atm Archctecture and  
Implementation"  
Mc Graw Hill USA 1995

Tesis Facultad de Ingeniería  
"Diseño de una red de comunicaciones asincrona de gran ancho de  
banda para transmisión simultánea de voz datos y video con tecnología  
ATM"  
Amador Allende, FI UNAM 1995

David Ginsburg "Atm : Solutions for Enterprise Internetworking "  
Prentice Hall ,  
USA 1996

LAN, ATM and LAN EMULATION TECHNOLOGIES  
Minoli Daniel  
Alles Anthony  
USA 1996

Clark, Martin P. "ATM NETWORKS Principles and Use"  
Wiley Teubner ,  
USA 1996

Sackett, George C. & Metz, Christopher Y. "ATM MULTIPROTOCOL  
NETWORKING"  
Mc Graw Hill,  
USA 1997

Minoli Daniel & Golway, Thomas with Parker, Smith " ATM NETWORKS"  
Manning,  
USA 1997

The ATM Forum " Anchorage Accord, The Official Interoperability  
Specification"  
The ATM Forum,  
USA 1997

Pattavina, Achille "Switching Theory: Architecture and Performance in  
Broadband ATM Networks"  
Wiley,  
USA 1998

Handel, Rainer-Huber, Manfred H-Schoder, Stefan "ATM Networks  
Concepts, Protocols and Applications"  
Addison-Wesley,  
USA 1998

#### **Revistas:**

Cabletron Systems " Atm LAN Emulation in Workgroup Networks 1997"  
" Atm and the New Network Infrastructure 1997"  
" LANE Book reference 1997"

Byte " Networks Infrastructure 1998"

Telecommunications "Ten Hottest Technologies 2000"

#### **Páginas de Internet:**

<http://www.cisco.com> .- Página de información técnica sobre  
soluciones de red, capacitación, eventos, seminarios, revistas, servicios,  
soporte, proveedores de equipos y tecnología de redes Cisco.

<http://www.telecoms-mag.com> .- Una de las principales páginas de información tecnológica actual para redes de comunicaciones, protocolos de vanguardia, equipos innovadores en telecomunicaciones, recomendaciones tecnológicas y estudios de mercado sobre empresas en el ramo de telecomunicaciones.

<http://www.foresystems.com>.- Ahora la página es: <http://www.marconi.com>, la página se refiere a tecnología de equipo FORE que ahora forma parte de la empresa Marconi también de telecomunicaciones. Es una página de información de redes ópticas, ruteo, equipo, servicios de consultoría en diseño y planeación de redes, sistemas para equipo móvil, soluciones de software para el manejo de microondas, soluciones de software para aplicaciones médicas (radiología, cuidados de la salud, consultas médicas).

<http://www.atmforum.com>.- Página de información sobre estándares, productos y servicios que la tecnología ATM ofrece. Este foro fue formado con el fin de incrementar el uso de ATM alrededor del mundo, informando de las ventajas de este sistema así como la interoperatividad con otras plataformas de red.

## APENDICE A. GLOSARIO DE TERMINOS

### A

AAL	ATM Adaptation Layer. Capa de adaptación de ATM.
ABR	Available Bit Rate. Tasa disponible de bits.
ACK	Acknowledgement -
ANSA	Advanced Networked Systems Architecture.
ARM	Advanced RISC Machine
ATM	Asynchronous Transfer Mode. Modo de transferencia asíncrono.

### B

Backbone	Red dorsal ó columna vertebral de una red.
B-ISDN	Broadband Integrated Services Digital Network.

### C

CBR	Constant Bit Rate. Tasa constante de bits.
CCITT	Comité Consultatif International Télégraphique et Téléphonique. Comité consultivo internacional telgráfico y telefónico. Ahora ITU.
CDV	Cell Delay Variation.
CLP	Cell Loss Priority (a bit in a B-ISDN cell header)
CRC	Cyclic Redundancy Check. Verificador de redundancia cíclica.
CPE	Customer Premises Equipment

### D

DAC	Digital to Analogue Convertor. Convertidor analógico digital.
DMA	Direct Memory Access. Acceso directo a memoria.
DRAM	Dynamic RAM. Memoria dinámica de acceso aleatorio.

### E

E1	2 Mbit/seg
E2	8 Mbit/seg
E3	34 Mbit/seg
EAS	Ethernet-ATM Switch
EATM	EISA ATM (an adaptor)
EISA	Enhanced Industry Standard Architecture (a bus)

### F

FDDI	Fiber Distributed Data Interface
FAS	Framing and Sequencing
FIFO	First In First Out
Forum ATM	Foro fundado por diversos proveedores de tecnología ATM
Frame Relay	Protocolo síncrono de red, basado en HDLC. Los datos son enviados en paquetes HDLC llamados frames.

### H

HEC	Header Error Check (an 8 bit CRC in a B-ISDN cell)
HDLC	High-level Data Link Control. Protocolo internacional definido por el ISO.

### I

IP	Internet Protocol
IRQ	Interrupt Request
ISDN	Integrated Services Digital Network. Red digital de servicios integrados.
ISO	International Standards Organization
ITU	International Telecommunication Union. Unión Internacional de Telecomunicaciones.

### J

### L

LAN	Local Area Network. Red de área local.
LANE	LAN Emulation. Emulación de una red de área local.
LAPB	Link Access Procedure Balanced. Procedimiento de enlace de acceso balanceado.
LCA	Logic Cell Array. Arreglo lógico de celdas.
LEC	LAN Emulation Client. Cliente de red de área local emulada..
LES	LAN Emulation Server. Servidor de red de área local.
<b>M</b>	
MAC	Media Access Control. Control de acceso al medio.
MAN	Metropolitan Area Network. Red de área metropolitana.
MDL	Media Data Link.
MSDL	MultiService Data Link. Enlace de datos de multiservicios.
<b>N</b>	
NAK	Negative acknowledgement -
NNI	Network Network Interface.
<b>O</b>	
OC3	155 Mbit/sec
OC12	622 Mbit/sec
OSI	Open Systems Interconnection. Interconexión de sistemas abiertos.
<b>P</b>	
PCR	Peak Cell Rate.
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit.
PTM	Packet Transfer Mode. Modo de transferencia de paquete.
PSTN	Public Switch Telephone Network
<b>Q</b>	
Q.93B	Protocolo estándar de señalización para ATM.
QoS	Quality of Service. Calidad de servicio.
<b>S</b>	
SAP	Service Access Point. Punto de acceso al servicio.
SDH	Synchronous Digital Hierarchy. Jerarquía síncrona digital.
SDL	Standard Data Link.
SDU	Service Data Units.
SONET	Synchronous Optical Network.
SSCOP	Signalling System Common Operations Protocol (the standard (i.e. awful) transport protocol for carrying Q.93B)
STM	Synchronous Transfer Mode. Modo de transferencia síncrono.
STS1	155 Mbit/seg
STS4	622 Mbit/seg
<b>T</b>	
T1	1.5 Mbit/seg
T3	45 Mbit/seg
TA	Terminal Adapter. Adaptador de terminal.
<b>U</b>	
UNI	User Network Interface. Interfase de red de usuario.
UBR	Unspecified Bit Rate. Tasa no especificada de bits.
UPC	Usage Parameter Control.
<b>V</b>	
VBR	Variable Bit Rate. Tasa variable de bits.
VC	Virtual Channel or Virtual Circuit.

VCI	Virtual Circuit Identifier.
VP	Virtual Path. Trayectoria virtual.
VPI	Virtual Path Identifier. Identificador de trayectoria virtual.
W	
WAN	Wide Area Network. Red de área amplia.
WAS	Wide Area Services. Servicios de área amplia.
X	
X.25	Protocolo de comunicaciones