# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA


**INTEGRACION DE REDES TCP/IP CON ATM**

**INFORME DE SUFICIENCIA**

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO ELECTRÓNICO**

**PRESENTADO POR:**

**LIDIA MAGALY MONTES LLANOS**

**PROMOCIÓN**
**2001 – I**

**LIMA – PERÚ**
**2006**

# INTEGRACION DE REDES TCP/IP CON ATM

*Dedico este trabajo a:*

*Mis padres y mis hermanos por el apoyo*

*incondicional en mi carrera,*

*Mi hija y mi esposo que son el mejor estímulo*

*para seguir avanzando.*

## SUMARIO

El trabajo que aquí se presenta, exhibe a dos de las tecnologías más importantes en el mundo de las redes de computadoras: TCP/IP y ATM. Se señalan las características más importantes de ambos tipos de redes y como parte principal de revisan los mecanismos que existen, o en otros casos, se plantean para la integración de ambos tipos de redes. ATM aporta elevadas prestaciones como son la escalabilidad de su ancho de banda, su rendimiento y su habilidad para integrar y soportar datos, audio y video. Por otro lado, IP ofrece también atractivas características como su simplicidad, su filosofía abierta y el soporte sobre entornos LAN, MAN y WAN. Como podrá verse ambos tipos de redes tienen sus propias características que han hecho de ellas las más destacadas, sin embargo la integración, para poder obtener lo mejor de ambas, resulta algo complicado por lo diferente del funcionamiento en cada uno de los casos.

# ÍNDICE

**CAPÍTULO II**

**SERVICIOS TCP/IP Y SERVICIOS ATM**



**CAPÍTULO III**

**TCP/IP SOBRE ATM**

# PROLOGO

El concepto de trabajo en redes es probablemente tan antiguo como lo es el de las telecomunicaciones. Lo podemos notar cuando nuestros antepasados, en la edad de piedra querían comunicarse recurriendo a "protocolos" rudimentarios o al apoyo de otros (trabajo en red). Por supuesto, la humanidad ha avanzado un poco desde la antigüedad; ya no se usan primitivos artefactos ni tenemos los mismos inconvenientes que nuestros antepasados. En la actualidad, contamos con computadoras que hablan con otras sobre una colección de cables, fibra óptica, microondas, etc.

Sin embargo, no es precisamente el desarrollo acelerado de las redes la causa del asombro principal, sino su poder de penetración en la vida humana, su capacidad de revolucionar desde el puesto de trabajo hasta las relaciones sociales: su capacidad de mediar en casi todos los actos de la vida moderna.

Acercándonos más al tema aquí tratado consideremos que así como Internet revolucionó las comunicaciones a nivel mundial, el Asynchronous Transfer Mode (ATM) aporta actualmente un nuevo sentido a las redes de alta velocidad. El ATM representa a una nueva generación de redes. Promete ser un medio clave en las redes para el empleo tanto de las aplicaciones existentes como emergentes en los campos de la ciencia, la medicina y la educación.

El debate actual sobre ATM difiere de las primeras batallas entre el X.25 y TCP/IP en que no lucha por la supervivencia. Sin embargo, se puede concebir un despliegue inicial en que ATM utilice TCP/IP y, en forma gradual, introducir aplicaciones propias de esta nueva tecnología. Finalmente, ATM podría dominar la transferencia de información en Internet y el TCP/IP constituirse en un sector del ATM.

Se ha entrado a una nueva era cultural, la era del acceso instantáneo a cualquier lugar del mundo, la era en la que existe, por primera vez en la historia, una total libertad para la comunicación y el flujo sin limitaciones de información, la era en que todas las culturas podrán enlazarse por medio de las computadoras para conformar una inteligencia

colectiva que llevará a cambios fundamentales en las respuestas culturales, políticas y sociales de los pueblos.

# CAPÍTULO I
# FUNDAMENTOS

## 1.1 Pila de protocolos TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) ha llegado a ser común en el mundo de las redes y es el suit de protocolos más empleado. Es también un elemento importante para Internet (red de redes). Muchos sistemas operativos de red (NOS), por ejemplo Windows NT 4.0 Server, Windows 2000 Server, y Novell Netware 5.0, abrazan TCP/IP como su suit de protocolos de red por defecto.

TCP/IP fue desarrollado originalmente como un sistema de los protocolos WAN que se podrían utilizar para mantener enlaces de comunicaciones entre diferentes puntos incluso si ciertos puntos llegaran a ser inoperables durante una guerra nuclear mundial. La verdad de las cosas es que su uso tiene un sesgo diferente considerando que fue desarrollado originalmente como clase de sistema de seguridad para la red en tiempo de guerra por el departamento de la defensa.

Otro punto a saber sobre TCP/IP es que se ha convertido en una pieza integral en la operación y soporte de ruteadores en una interconexión. Los administradores de ruteadores Cisco usan Telnet (parte de la pila TCP/IP) para comunicarse con los ruteadores alejados y utilizan TFTP (otro protocolo de TCP/IP) como un mecanismo para copiar y guardar archivos y cargar nuevo software IOS en el ruteador. La mayoría de las redes grandes utilizan TCP/IP como su protocolo de red, de tal modo que una carencia en la comprensión del apilado TCP/IP hará difícil el trabajo con los ruteos y las interconexiones.

## 1.2 TCP/IP y el modelo OSI

TCP/IP fue desarrollado en los años 70 y precedió a la culminación del modelo de OSI (en los años 80). Esto significa que los diferentes grupos de protocolos (en 4 capas) en la pila TCP/IP no corresponden directamente a cada capa en el modelo de OSI (aunque los protocolos de la capa de red y de enlace en las capas inferiores, tales como IP y ARP, se acercan al equivalente conceptual en el modelo de OSI). Cuando TCP/IP fue

desarrollado, el departamento de la defensa (DOD) desarrolló su propio modelo conceptual – el modelo DOD – (también conocido como el modelo de DARPA) por como varios protocolos en el apilado TCP/IP funcionan. Este modelo de la referencia divide el movimiento de datos de un nodo que envía a un nodo que recibe en cuatro capas (comparadas a las siete capas del modelo de OSI). La figura 1.1 compara el modelo DOD con el modelo OSI.

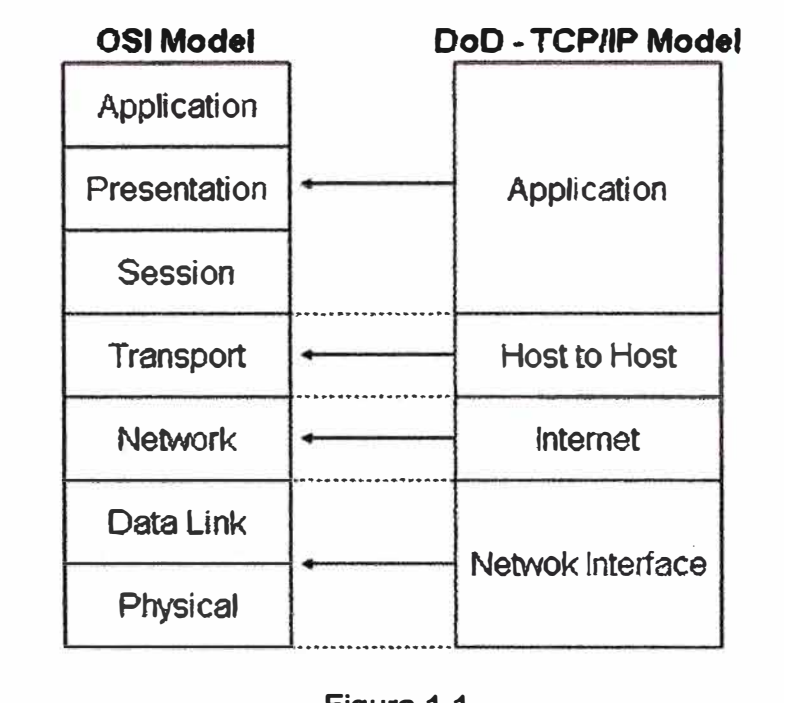


Figura 1.1

Cada capa en el apilado conceptual de DOD-TCP/IP define el trabajo que los protocolos de TCP/IP hacen que funcionen en ese nivel particular (solo como lo hace el modelo de OSI). Posteriormente se verá que sucede en cada capa del apilado conceptual de DOD-TCP/IP y de los protocolos reales del apilado de TCP/IP que funciona en estos niveles. En la figura 1.2 muestra la correspondencia entre la pila de protocolos TCP/IP y el modelo de DOD.

### 1.3 Capa Aplicación

Los protocolos de la capa de aplicación proporcionan la interfaz de usuario para los varios protocolos y aplicaciones que tienen acceso a la red. Los protocolos de la capa de aplicación en la pila TCP/IP manejan transferencia de archivo, login remoto a otros nodos, la funcionalidad del e-mail, y la supervisión de la red. Un número de diversos protocolos residen a este nivel:

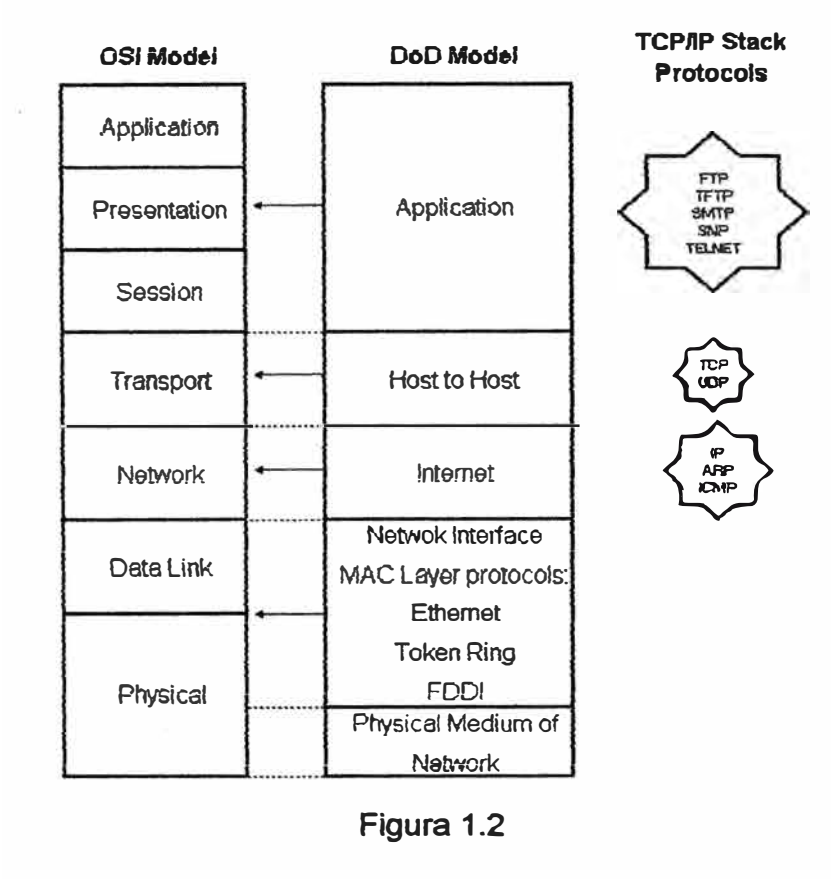


Figura 1.2

### 1.3.1 FTP (File Transfer Protocol)

Es un protocolo que presenta la capacidad de transferir archivos entre dos computadoras. El ftp es realmente una potente aplicación (clientes ftp pueden descargados de Internet y ser utilizados para mover archivos entre las computadoras) y un protocolo que es apoyado por otras aplicaciones tales como browsers de la Web.

### 1.3.2 TFTP (Trivial File Transfer Protocol)

Es una versión del ftp que proporciona una manera de mover archivos sin ningún tipo de autenticación (significando sin usuario ni contraseña). TFTP se utiliza en el mundo del direccionamiento como una manera de salvar archivos de configuración del ruteador o de poner al día el IOS del ruteador.

### 1.3.3 SMTP (Simple Mail Transport Protocol)

Es un protocolo que proporciona la entrega de correo entre dos computadoras. Es un protocolo apoyado por los clientes e-mail y usado para enviar y recibir e-mails en Internet.

### 1.3.4 SNMP (Simple Network Management Protocol)

Es un protocolo que proporciona la capacidad para recoger la información de la red. El SNP utiliza a agentes (vigilantes de software que observan los procesos de la red) que

recogen datos sobre el funcionamiento de la red. Los datos recogidos pueden ser comparados con información en línea. Los paquetes de software como CiscoWorks utilizan el SNMP para ayudar a administradores de redes a supervisar el buen funcionamiento de una red.

**Telnet**

Es un protocolo de emulación de terminal que permite que usted conecte una computadora local con la computadora remota (u otro dispositivo tal como un ruteador). La computadora local se convierte en un terminal virtual que tiene acceso a las aplicaciones y a otros recursos de la computadora remota.

**a. Capa Transporte**

Los protocolos de la capa de transporte proporcionan control de flujo y confiabilidad a la conexión mientras los datos se envían y reciben entre computadoras. Esta capa toma la información de los protocolos de la capa de aplicación y comienza el proceso de alistar los datos para el transporte en la red. Dos protocolos del suit de protocolos TCP/IP constituyen la capa de transporte: TCP y UDP.

**TCP (Transport Control Protocol)**

Es un protocolo orientado a la conexión que proporciona un circuito virtual (semejante al establecimiento de una llamada telefónica entre los nodos que envían y reciben) entre las aplicaciones de los usuarios en las máquinas que envían y reciben información. TCP toma los datos de los protocolos de la capa de aplicación y los divide en segmentos y luego se cerciora de unirlos en el extremo de recepción. TCP requiere que las computadoras: la que transmite y la que recibe, establezcan una conexión sincronizada, que es hecha en el intercambio de paquetes que llevan una secuencia de números y un bit de control de sincronismo.

**UDP (User Datagram Protocol)**

Es un protocolo de transporte no orientado a la conexión que proporciona una conexión entre los protocolos de la capa de aplicación que no requieren los reconocimientos y la sincronización proporcionados por TCP. El UDP es como enviar una postal a través del sistema del correo. El paquete se direcciona para el nodo de recepción y se envía así. El UDP es mucho más pasivo que el TCP. Entre los protocolos de la capa de aplicación que utilizan el UDP están el TFTP y el SNMP.

## 1.5 Capa Internet

La capa Internet (que corresponde a la capa de red del modelo OSI) es responsable del encaminamiento de datos a través de las trayectorias lógicas de la red y proporciona un sistema de dirección a las capas superiores del modelo conceptual. Esta capa también define el formato del paquete usado para los datos mientras que se mueve sobre la red interna. La capa Internet realmente gira alrededor de un protocolo - IP. Otros protocolos en esta capa proporcionan básicamente soporte para el sistema de direccionamiento de IP y el formato del paquete. Un trabajo importante de la capa de Internet es resolver direcciones lógicas (tales como direcciones IP) para las direcciones reales del hardware (MAC) de los nodos en la red.

### 1.5.1 IP (Internet Protocol)

IP toma los datos de la capa de transporte y fragmenta la información en paquetes o los datagramas. Etiqueta cada paquete con la dirección IP del dispositivo que envía y la dirección IP del dispositivo de recepción. El IP también reensambla los datagramas en la máquina de recepción en segmentos para los protocolos de la capa superior. El IP es un protocolo no orientado a la conexión por lo que no tiene interés en el contenido de los datagramas. Su único trabajo es direccionar y enviar los datagramas hacia su destinación.

### 1.5.2 ARP (Address Resolution Protocol)

Cuando el protocolo IP prepara un datagrama, sabe la dirección IP de las computadoras origen y destino (recibe esta información de los protocolos de las capas superiores tales como Telnet o SMTP). El IP también necesita la dirección física MAC de la computadora destino porque debe proporcionar esta información al protocolo de la capa de acceso a red usado en la red (tal como Ethernet). El ARP proporciona el mecanismo para resolver el direccionamiento IP para una dirección física. El ARP envía broadcasts con el IP address de la computadora destino y pide a dicha computadora contestar con su dirección física.

### 1.5.3 ICMP (Internet Control Message Protocol)

Este protocolo es un protocolo de administración y proveedor de servicio de mensajes que es utilizado por los ruteadores para enviar mensajes a los ordenadores host que están enviando los datos que deben ser ruteados. Los ruteadores pueden enviar información al host para darle a conocer cuando un destino es inalcanzable o cuándo la memoria de almacenamiento de los ruteadores está llena de información. Una vez más,

el ICMP se utiliza básicamente como protocolo de soporte para el direccionamiento IP tal como el protocolo ARP.

## 1.5 Capa Acceso a Red

La capa de acceso a red consiste de protocolos que toman los datagramas de la capa de Internet y los convierten en un tipo específico de trama (marco) que luego es puesta en el medio físico de la red como una corriente del bits. Los protocolos que se incluyen de esta capa relacionan a las arquitecturas de red tales como Ethernet, Token Ring, y FDDI. La IEEE proporciona las especificaciones para los diversos tipos de tramas usadas por estas arquitecturas de red.

Debido a que estos protocolos residen en la capa MAC (una parte de la capa de acceso a red del modelo DOD y de la capa de enlace de datos del modelo OSI), están implicados integralmente en el direccionamiento físico de los paquetes de los datos. La dirección física para una computadora se quema realmente en la tarjeta de interfaz de red que se coloca en la computadora. Los ruteadores Ethernet, Token Ring, y las interfaces FDDI también tienen direcciones del MAC quemadas en la ROM de control de interfaz (las interfaces seriales en los ruteadores no tienen direcciones MAC).

## 1.6 ATM

ATM o cell relay, fue destinado a sustituir, eventualmente, a la mayoría de las tecnologías WAN. Como Frame Relay, ATM proporciona un servicio no fiable, orientado a la conexión. ATM permite establecer una conexión entre sitios, pero la fiabilidad es responsabilidad de un protocolo de nivel superior como TCP.

ATM mejora el rendimiento de Frame Relay. En lugar de utilizar tramas de longitud variable, ATM recoge una unidad de datos del protocolo, PDU (Protocol Data Unit), del trafico LAN, como un datagrama de IP, y los segmenta en trozos de 48 bytes, a cada segmento se le añade una cabecera de 5 bytes. Las tramas de 53 bytes de ATM con los segmentos de los datagramas IP se envían por la red ATM, llamado celda ATM, permite optimizar el rendimiento de la red de conmutación ATM.

ATM ha funcionado a velocidades de hasta 9.6 Gbps con la red óptica síncrona (SONET), una especificación internacional para la comunicación de fibra óptica. ATM es una solución escalable para datos, voz, audio, fax y video y puede acomodar todos estos tipos de información simultáneamente. ATM combina las ventajas de la conmutación de

circuitos, retrazo fijo de tránsito y ancho de banda garantizado, con las ventajas de la conmutación de paquetes, eficiencia en las ráfagas de tráfico.

Está claro que la tecnología del Asynchronous Transfer Mode (ATM) desempeña un papel central en la evolución de las actuales redes de empresas, grupos de trabajo y centros de estudios. ATM entrega importantes ventajas sobre las tecnologías LAN y WAN existentes, incluyendo la promesa de anchos de banda escalable a precios sin precedentes y garantías en los puntos del funcionamiento y calidad de servicio (QoS ), que facilitan nuevas clases de usos tales como multimedia.

Estas ventajas, sin embargo, tienen un precio. Contrario a las ideas falsas comunes, ATM es una tecnología muy compleja, quizás la más compleja desarrollada por la industria de las redes. Mientras que la estructura de las celdas ATM y la celda de conmutación facilitan el desarrollo del hardware intensivo y conmutadores ATM de alto rendimiento, el despliegue de redes ATM presenta requerimientos altamente complejos de, software intensivo, infraestructura de protocolo. Esta infraestructura requerida permite a los conmutadores individuales ATM enlazarse en una red, y para que tales redes se enlacen en la WAN.

Asincrónica significa que el ancho de banda de red disponible no está dividido en canales fijos o ranuras sincronizadas por un mecanismo temporizador o un reloj. El diseño de los dispositivos que se comunican de forma asincrónica no está relacionado con su capacidad para enviar y recibir información a una determinada velocidad de transmisión. En su lugar, el emisor y el receptor negocian la velocidad a la que se comunicarán, de acuerdo con las limitaciones físicas del hardware y la capacidad de mantener un flujo fiable de información a través de la red.

Modo de transferencia hace referencia a la forma en que la información se transfiere entre el emisor y el receptor. En ATM, se utiliza el concepto de celdas pequeñas de longitud fija para estructurar y empaquetar los datos para las transferencias. Al utilizar celdas, en contraste directo con el mecanismo de paquetes de longitud variable utilizado por la mayoría de las tecnologías de red actuales, ATM asegura que las conexiones pueden negociarse y administrarse sin que ninguno de los tipos de datos o conexiones puedan apropiarse en exclusiva de la trayectoria de transferencia.

## 1.7 La celda ATM

La celda ATM consta de cabecera de 5 bytes y 48 bytes de datos. Existen 2 tipos de cabeceras de ATM:

Cabecera de interfaz de red de usuario, UNI (User Network Interface). Cabecera de ATM que existe dentro de una red privada o entre el sitio de un cliente y el proveedor de servicios ATM público.

Cabecera de interfaz de red a red, NNI (Network - to - Network Interface). Cabecera de ATM que existe entre redes de proveedores de servicios públicos ATM.

En la figura 1.3 se muestra el formato de la cabecera de las celdas de ATM UNI tanto en entornos públicos como privados.

Los campos de la cabecera de ATM se definen de la siguiente forma:

Control de Flujo Genérico, CFG (Generic Flow Control). Campo de 4 bits que se añadió inicialmente para permitir la conexión de redes ATM a redes de acceso compartido como un anillo de Bus dual con cola distribuida, DQDB (Distributed Queue Dual Bus). El campo GFC se diseñó para dar a la UNI 4 bits con los que negociar la multiplexación y el control de flujo entre las celdas de un único circuito virtual de ATM. Sin embargo el uso de valores exactos del campo GFC no se han normalizado por lo que siempre su valor es 0x0.

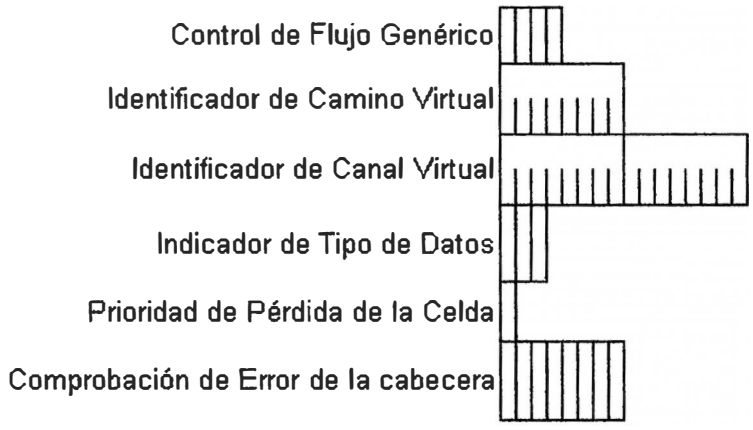


Figura 1.3

Identificador de Camino Virtual, VPI (Virtual Path Identifier). El identificador de camino virtual para esta celda. El VPI para un circuito virtual de ATM se descubre durante el proceso de establecimiento del circuito virtual para los SVC, y se configura manualmente para los PVC. En el UNI, el VPI es de 8 bits, lo que permite hasta 256 caminos virtuales

diferentes. VPI 0 existe predeterminado en todos los equipo de ATM y se usa para tareas administrativas como la señalización para crear y eliminar conexiones ATM dinámicas.

Identificador de Canal Virtual, VCI (Virtual Channel Identifier). El identificador de un canal virtual dentro del camino virtual especificado. Los VCI se asignan dinámicamente para las conexiones SVC y manualmente para las conexiones PVC. El VCI es de 16 bits, lo que permite hasta 65536 canales virtuales distintos. Existen VCI reservados y estos se usan para señalización, operación y mantenimiento y administración de recursos.

La combinación VPI y VCI identifica el circuito virtual de una celda ATM dada, es la información de enrutamiento.

Identificador del Tipo de Datos, PTI (Payload Type Indicator). Campo de 3 bits que consta de los siguientes campos:

Tipo de Celda ATM
Indicación explicita de congestión hacia delante, EFCI.
Indicación de segmentación AAL5.

Prioridad de Pérdida de Celda, CLP (Cell Loss Priority). Campo de 1 bit que se usa como indicador de prioridad de celda. Si está en 0, la celda es de alta prioridad y los conmutadores internos deben realizar todo lo que puedan para reenviar la celda correctamente. Si el bit CLP está a 1, los conmutadores pueden decidir si descartan la celda en caso de congestión.

Comprobación de Error de Cabecera, HEC (Header Error Check). Campo de 1 byte que permite a un conmutador de ATM o a un extremo de ATM corregir un único bit de error, o detectar múltiples bits de error en los primeros cuatro bytes de la cabecera de ATM.
En la Figura 1.4 se muestra la cabecera de una celda ATM NNI pública o privada. Las únicas diferencias entre las cabeceras UNI y NNI son las siguientes:
*No existe campo GFC.* Los conmutadores ATM de un proveedor de servicios ATM no necesitan un mecanismo para negociar el multiplexado de distintos tipos de conexiones de usuario de acceso compartido.

VPI ahora tiene 12 bits. De esta manera se pueden establecer hasta 4096 caminos virtuales por caminos de transmisión. Con una VPI extendida, los proveedores de servicios ATM disponen de mayor flexibilidad para realizar conmutación entre caminos

virtuales y crear una arquitectura troncal que admita líneas troncales en los sistemas de telefonía vocal.

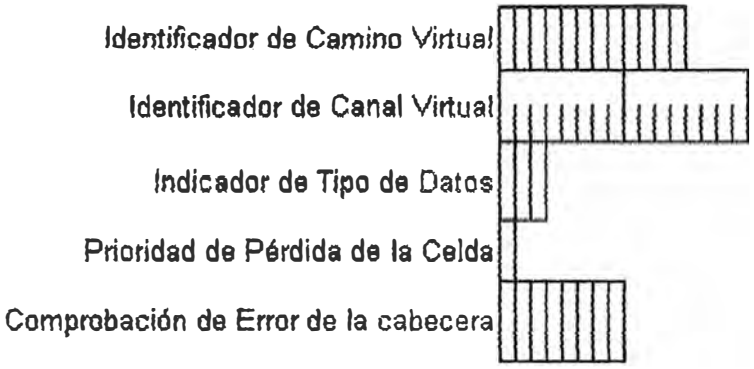


Figura 1.4

## 1.9 Arquitectura de ATM

El modelo arquitectónico de ATM, conocido como modelo B-ISDN/ATM, tiene tres niveles principales.

### 1.9.1 Nivel Físico

El nivel físico proporciona la transmisión y recepción de celdas ATM a través de un medio físico entre dos dispositivos ATM y se subdivide en sub-nivel PMD (Phisical Médium Dependent), que es el responsable de la transmisión y recepción de los bits individuales en un medio físico; y sub-nivel TC (Transmission Convergence) actúa como conversor entre el flujo de bits del sub-nivel PMD y las celdas ATM; también se encarga del control de error HEC y del sincronismo de celdas.

### 1.9.2 Nivel ATM

El nivel ATM proporciona las funciones de multiplexado de celdas, demultiplexado y enrutamiento VPI/VCI. Además el nivel ATM es responsable de la supervisión del flujo de celdas para asegurar que todas las conexiones se mantienen dentro de los límites de rendimiento negociados. El nivel ATM puede tomar acciones correctivas de forma que aquellas operaciones fuera de los parámetros negociados no afecten a otras conexiones que siguen los parámetros negociados. Además, el nivel ATM asegura que se mantenga la secuencia de las celdas de cualquier emisor.

### 1.9.3 Nivel de Adaptación de ATM

El nivel de adaptación de ATM (AAL) es responsable de la creación y recepción de los datos de 48 bytes vía el Nivel ATM a través de distintos tipos de aplicaciones. El nivel AAL se subdivide en sub-nivel de convergencia y sub-nivel de segmentación y reensamblado. CS (capa o sub-nivel de convergencia), determina el tamaño de buffer. SAR (sub-nivel de segmentación y reensamblado) trabaja en la segmentación y reensamble, control de errores y pérdidas de segmentos.

Se conoce también al nivel Físico y al nivel ATM como capa 1a y capa 1b respectivamente, mientras que al nivel de Adaptación de ATM se le indica como capa 2.

### 1.10 Operación de la Red ATM

Las redes ATM están formadas por tres elementos diferentes: usuarios (dispositivos de extremo), conmutadores e interfaces. Consiste en un sistema de conmutadores ATM interconectados en enlaces ATM punto a punto y señalar acoplamientos o interfaces ATM. Los conmutadores ATM soportan 2 clases de interfaces: interfaz de red de usuario (UNI) e interfaz de nodo a red[1] (NNI). UNI conecta extremo de sistemas ATM (hosts, ruteadores, etcétera) mediante un conmutador ATM, mientras que una NNI se puede definir como una interfaz que conecta dos conmutadores ATM juntos. Los formatos de las celdas para cada uno de los casos son levemente diferentes. Para ser más precisos NNI es cualquier enlace físico o lógico a través del cual dos conmutadores ATM se comunican con el protocolo NNI.

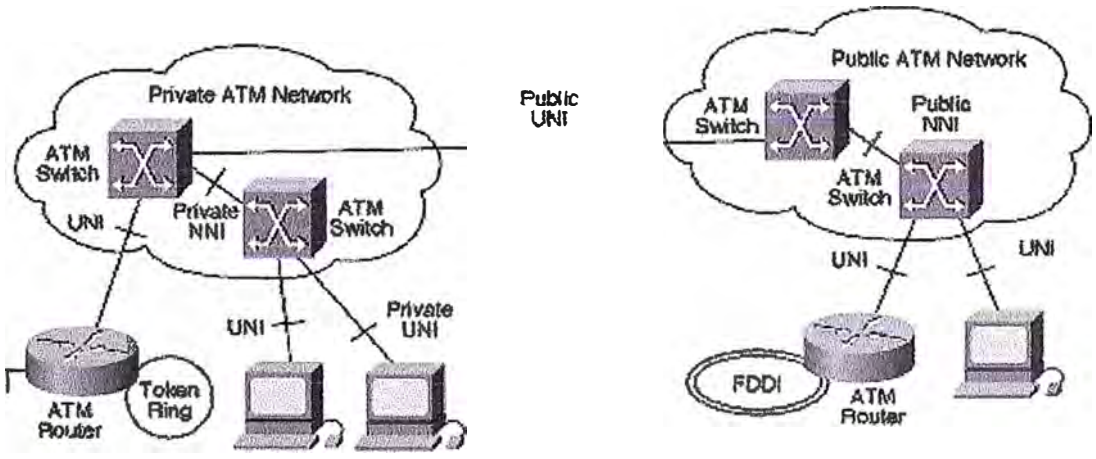


Figura 1.5 Interfaces de la Red ATM

[1] Algunas veces se conoce también interfaz de red a red, la diferencia es sutil y poco trascendente.

Según lo observado, las redes ATM son fundamentalmente orientadas a la conexión. Esto significa que un circuito virtual necesita ser configurado a través de la red ATM antes de cualquier transferencia de datos. Los circuitos ATM son de dos tipos: caminos virtuales, identificados por los identificadores de camino virtual (VPI); y canales virtuales, identificados por la combinación de un VPI y de un identificador de canal virtual (VCI). Un camino virtual es un paquete de canales virtuales, que son cambiados transparentemente a través de la red ATM en base a un VPI común. Los VCI y VPI, sin embargo, tienen solo significación local a través de un enlace particular, y son remapeados apropiadamente en cada conmutador. En operación normal, los conmutadores asignan todas las conexiones de UNI dentro de VPI=0.

La operación básica de un conmutador ATM es muy simple: recibir una celda a través de un enlace en un valor conocido de VCI o VPI; observar el valor de la conexión en una tabla local de traducción para determinar el puerto de salida (o puertos) de la conexión y el nuevo valor de VPI/VCI de la conexión en ese enlace; y entonces retransmitir la celda en ese enlace de salida con los identificadores apropiados para la conexión.

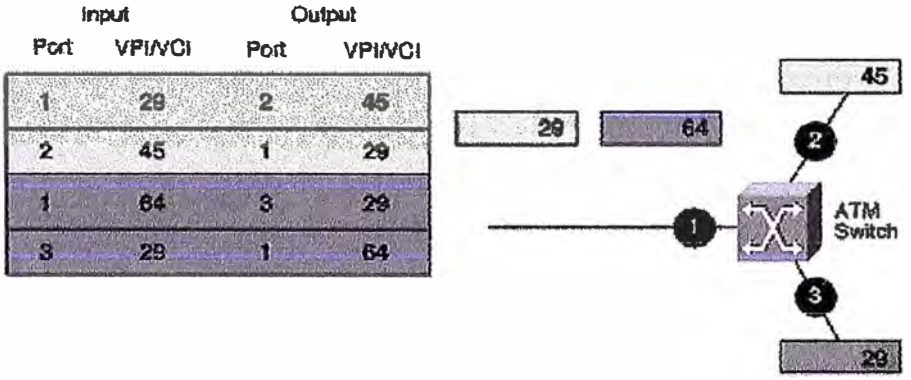


Figura 1.6: Operaciones del Conmutador ATM

La operación del conmutador es tan simple porque los mecanismos externos instalan las tablas locales de traducción antes de la transmisión de cualquier dato. La manera en que estas tablas son configuradas determina los dos tipos fundamentales de conexiones ATM.

### 1.10.1 Conexiones Virtuales Permanentes (PVC)

PVC es una conexión configurada por un mecanismo externo, típicamente el administrador de la red, en la cual un conjunto de conmutadores entre un origen y un destino ATM en un sistema ATM son programados con valores apropiados para VPI/VCI.

Las PVCs requieren siempre una configuración manual. Como tal, su uso puede a menudo ser incómodo.

### 1.10.2 Conexiones Virtuales Conmutadas (SVC)

SVC es una conexión que se instala automáticamente con un protocolo de señalización. Una SVCs no requiere la interacción manual necesitada para configurar PVCs y, como tal, es más usada. Todos los protocolos de capas superiores que operan sobre ATM usan principalmente SVCs.

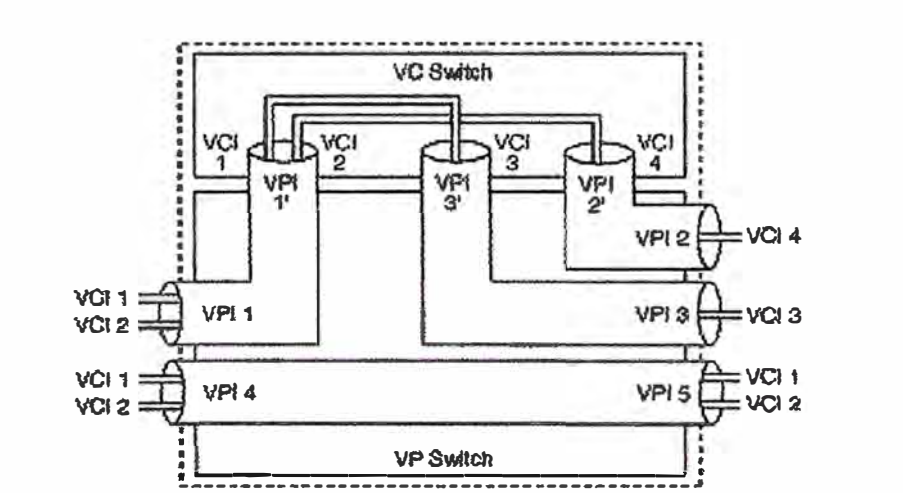


Figura 1.7: Conmutación de Canal virtual y Camino Virtual.

# CAPÍTULO II
# SERVICIOS TCP/IP Y SERVICIOS ATM

## 2.1 Características de los Servicios en TCP/IP

En TCP/IP todos los protocolos de alto nivel tienen algunas características en común:

Pueden ser aplicaciones escritas por el usuario o aplicaciones estandarizadas y distribuidas con un producto TCP/IP. De hecho, la pila TCP/IP incluye protocolos de aplicación tales como: TELNET para el acceso interactivo de una terminal a un host remoto; FTP (File Transfer Protocol) para transferencias de alta velocidad de un disco a otro; SMTP (Simple Mail Transfer Protocol) como sistema de correo de Internet. Estas son las aplicaciones implementadas más ampliamente, pero existen muchas otras.

Usan UDP o TCP como mecanismo de transporte. Recordar que UDP no es fiable ni ofrece control de flujo, por lo que en este caso la aplicación ha de proporcionar sus propias rutinas de recuperación de errores y de control de flujo. Suele ser más fácil desarrollar aplicaciones sobre TCP, un protocolo fiable, orientado a conexión. La mayoría de los protocolos de aplicación utilizan TCP, pero algunas aplicaciones se construyen sobre UDP para proporcionar un mejor rendimiento reduciendo la carga del sistema que genera el protocolo.

La mayoría de ellas usa el modelo de interacción cliente/servidor.

## 2.2 Modelo cliente/servidor

TCP es un protocolo orientado a conexión. No hay relaciones maestro/esclavo. Las aplicaciones, sin embargo, utilizan un modelo cliente/servidor en las comunicaciones.

Un servidor es una aplicación que ofrece un servicio a usuarios, de Internet por ejemplo; un cliente es el que pide ese servicio. Una aplicación consta de una parte de servidor y una de cliente, que se pueden ejecutar en el mismo o en diferentes sistemas.

Los usuarios invocan la parte cliente de la aplicación, que construye una solicitud para ese servicio y se la envía al servidor de la aplicación que usa TCP/IP como transporte.

El servidor es un programa que recibe una solicitud, realiza el servicio requerido y devuelve los resultados en forma de una respuesta. Generalmente un servidor puede tratar múltiples peticiones (múltiples clientes) al mismo tiempo.

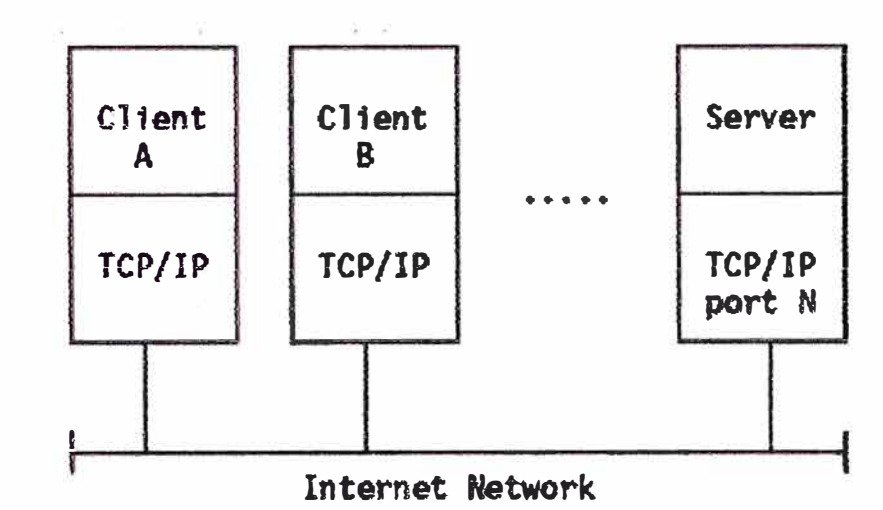


Figura 2.1 El modelo de aplicación cliente/servidor.

Algunos servidores esperan las solicitudes en puertos bien conocidos de modo que sus clientes saben a que zócalo IP deben dirigir sus peticiones. El cliente emplea un puerto arbitrario para comunicarse. Los clientes que se quieren comunicar con un servidor que no usa un puerto bien conocido tienen otro mecanismo para saber a qué puerto dirigirse. Este mecanismo podría usar un servicio de registro como Portmap, que utiliza un puerto bien conocido.

## 2.3 Utilidades y servicios de TCP/IP

Las utilidades y servicios TCP/IP permiten la conexión en red a otros equipos, como las estaciones de trabajo UNIX. Es preciso que tenga instalado el protocolo de red TCP/IP para poder utilizar dichas utilidades. Veremos a continuación algunas de las más importantes.

## 2.4 Telnet

TELNET es un protocolo estándar siendo su número STD de 8. Su status es recomendado. Se describe en el RFC 854 - Especificaciones del protocolo TELNET y RFC 855 - "TELNET Option Specifications".

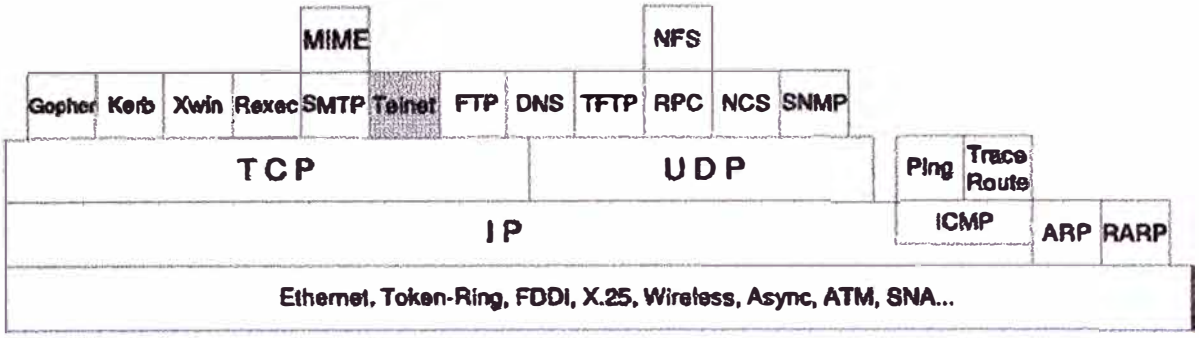


Figura2.2 TELNET- Protocolo de conexión remota.

El protocolo TELNET proporciona una interfaz estandarizada, a través de la cual un programa de un host (el cliente de TELNET) puede acceder a los recursos de otro host (el servidor de TELNET) como si el cliente fuera una terminal local conectada al servidor.

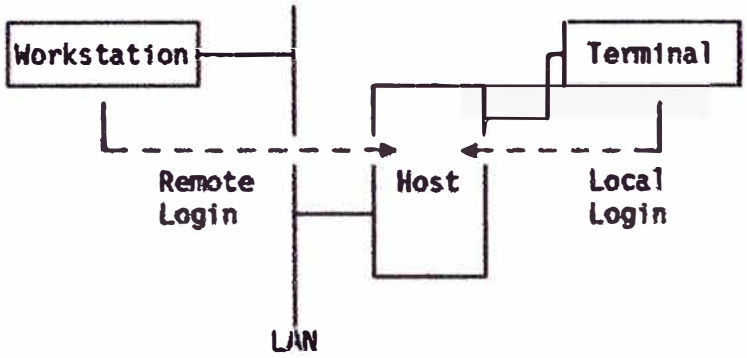


Figura 2.3 Conexión remota usando TELNET.

Por ejemplo, un usuario de una estación de trabajo situada en una LAN se puede conectar al host. Por supuesto, TELNET se puede usar tanto en LANs como en WANs.

TELNET permite la entrada del usuario conectado a la LAN del mismo modo que lo haría el usuario de una terminal local.

La mayoría de las implementaciones de TELNET no soportan entornos gráficos.

## 2.5 Funcionamiento de TELNET

TELNET es un protocolo basado en tres ideas:

El concepto de NVT (Network Virtual Terminal) (NVT). Una NVT es un dispositivo imaginario que posee una estructura básica común a una amplia gama de terminales reales. Cada host mapea las características de su propia terminal sobre las de su correspondiente NVT, y asume todos los demás hosts harán lo mismo.

Una perspectiva simétrica de las terminales y los procesos.

Negociación de las opciones de la terminal. El protocolo TELNET usa el principio de opciones negociadas, ya que muchos host pueden desear suministrar servicios adicionales, más allá de los disponibles en la NVT. Se pueden negociar diversas opciones. El cliente y el servidor utilizan una serie de convenciones para establecer las características operacionales de su conexión TELNET a través de los mecanismos "DO, DON'T, WILL, WON'T" ("hazlo, no lo hagas, lo harás, no lo harás").

Los dos hosts comienzan verificando que existe una comprensión mutua entre ellos. Una vez que se ha completado esta negociación inicial, son capaces de trabajar en el nivel mínimo implementado por la NVT. Después de haber logrado este entendimiento mutuo, pueden negociar opciones adicionales para ampliar las capacidades de la NVT y así reflejar con precisión la capacidad del hardware real que se está usando. Debido al modelo simétrico usado por TELNET, tanto el cliente como el servidor pueden proponer el uso de opciones adicionales.

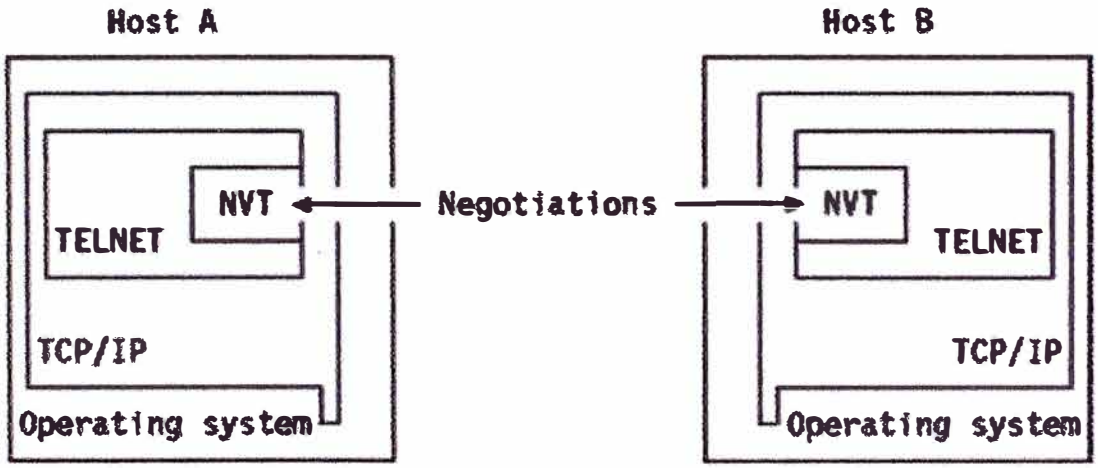


Figura 2.4 El modelo simétrico de TELNET.

## 2.6 TFTP (Trivial File Transfer Protocol)

El protocolo TFTP es un protocolo estándar siendo su número STD el 33.Su status es electivo y se describe en el RFC 1350 - El protocolo TFTP (Revisión 2).

La transferencia de ficheros en TCP/IP es una transferencia de datos de disco a disco, en oposición, por ejemplo, al comando SENDFILE de VM, una función que en el mundo de

TCP/IP se considera de correo, en la que envías a los datos al buzón de alguien (el lector en el caso de VM).

TFTP es un protocolo extremadamente trivial para la transferencia de ficheros. Se implementa sobre la capa UDP(User Datagram Protocol) y carece de la mayoría de las características de FTP (ver FTP(File Transfer Protocol)). La única cosa que es capaz de hacer es leer/escribir un fichero de/en un servidor. No dispone de medios para la autentificación de usuarios: es un protocolo inseguro.

## 2.7 Usos del TFTP

El comando:

*TFTP <nombre del host>*

Conduce al prompt interactivo en el que se pueden introducir sub-comandos:

*Connect <host>*

Especifica el identificador del host de destino

*Mode <ascii/binary>*

Especifica el tipo del modo de transferencia

*Get <remote filename> [<nombre del fichero local>]*

Recupera un fichero

*Put <remote filename> [<nombre del fichero local>]*

Almacena un fichero

*Verbose*

Activa o desactiva el modo "verbose", en el que muestra información adicional durante la transferencia del fichero.

*Quit*

Salir TFTP

## 2.8 Descripción del protocolo

Cualquier transferencia comienza con una solicitud para leer o escribir un fichero. Si el servidor concede la solicitud, se abre la conexión y el fichero se envía en bloques consecutivos de 512 bytes (longitud fija). Los bloques del fichero se numeran correlativamente, comenzando en 1. Cada paquete de datos debe ser reconocido mediante un paquete de reconocimiento antes de que se envíe el siguiente paquete. Se asume la terminación de la transferencia al recibir un paquete de menos de 512 bytes.

La mayoría de los errores provocarán la terminación de la conexión (falta de fiabilidad). Si un paquete se pierde en la red, se producirá un "timeout", tras el que se efectuará la retransmisión del último paquete (de datos o de reconocimiento).
En el RFC 783 se describió un bug bastante grave, conocido como el Síndrome del Aprendiz de Brujo. Puede causar una retransmisión excesiva en ambas partes de la conexión en algunas circunstancias en las que se producen retardos de red. Se documentó en el RFC 1123 y se corrigió en el 1350. Para más detalles, remitirse a estos RFCs.

### 2.9 Modos de transferencia

Actualmente se definen tres modos de transferencia en el RFC 1350:
NetASCII. US-ASCII tal como se define en el Código Estadounidense Estándar para el Intercambio de Información ("USA Standard Code for Information Interchange") con modificaciones especificadas en el RFC 854 - Especificaciones del protocolo Telnet y extendido para usar el bit de mayor orden. Es decir, se trata de un juego de caracteres de 8 bits, a diferencia del US-ASCII, que es de 7-bits.

Octeto. También llamado binario, consiste simplemente en bytes de 8 bits.

Correo. Este modo se definió originalmente en el RFC 783 y el RFC 1350 lo declaró obsoleto. Permitía efectuar la transferencia enviando correo a un usuario en vez de un fichero.

### 2.10 FTP ("File Transfer Protocol")

FTP es un protocolo estándar con el STD 9. Su status es recomendado. Se describe en el RFC 959 – FTP ("File Transfer Protocol").
La copia de ficheros de una máquina a otra es una de las operaciones más frecuentes. La transferencia de datos entre cliente y servidor puede producirse en cualquier dirección. El cliente puede enviar o pedir un fichero al servidor.

Para acceder a ficheros remotos, el usuario debe identificarse al servidor. En este punto el servidor es responsable de autentificar al cliente antes de permitir la transferencia de ficheros.

Desde el punto de vista de un usuario de FTP, el enlace está orientado a conexión. En otras palabras, es necesario que ambos hosts estén activos y ejecutando TCP/IP para establecer una transferencia de ficheros.

## 2.11 Descripción de FTP

FTP usa TCP como protocolo de transporte para proporcionar conexiones fiables entre los extremos. Se emplean dos conexiones: la primera es para el login y sigue el protocolo TELNET y la segunda es para gestionar la transferencia de datos. Como es necesario hacer un login en el host remoto, el usuario debe tener un nombre de usuario y un password para acceder a ficheros y a directorios. El usuario que inicia la conexión asume la función de cliente, mientras que el host remoto adopta la función de servidor.

En ambos extremos del enlace, la aplicación FTP se construye con intérprete de protocolo (PI), un proceso de transferencia de datos, y una interfaz de usuario (ver Figura - Principios de FTP).

La interfaz de usuario se comunica con el PI, que está a cargo del control de la conexión. Este intérprete de protocolo ha de comunicar la información necesaria a su propio sistema de archivos.

En el otro extremo de la conexión, el PI, además de su función de responder al protocolo TELNET, ha de iniciar la conexión de datos. Durante la transferencia de ficheros, los DTPs se ocupan de gestionar la transferencia de datos. Una vez que la operación del usuario se ha completado, el PI ha de cerrar la conexión de control.

## 2.12 Operaciones de FTP

Al usar FTP, el usuario realizará alguna de las siguientes operaciones:

- Conexión a un host remoto
- Selección de un directorio
- Listado de ficheros disponibles para una transferencia
- Especificación del modo de transferencia
- Copiar ficheros de o al host remoto
- Desconectar del host remoto

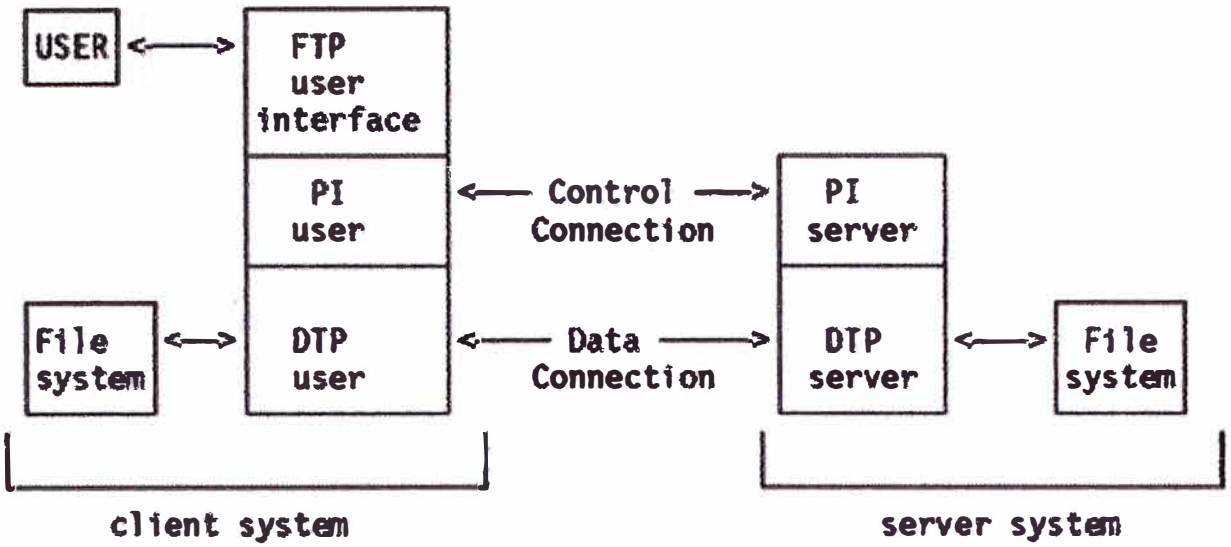


Figura 2.5 Principios de FTP

Conexión a un host remoto. Para ejecutar una transferencia de ficheros, el usuario comienza haciendo un login en el host remoto. Este es el método primario para manejar la seguridad. El usuario debe tener un identificador y un password para el host remoto, a menos que use un FTP anónimo.

Se usan tres comandos:

*Open* Selecciona el host remoto de inicia la sesión con el login

*User* Identifica al ID del usuario remoto

*Pass* Autentifica al usuario

*Site* Envía información al host remoto utilizado para proporcionar servicios específicos para ese host

Selección de un directorio. Cuando se establece el enlace de control, el usuario puede emplear el sub-comando cd ("change directory") para seleccionar un directorio remoto de trabajo. Obviamente, el usuario sólo podrá acceder a directorios a los que su ID le da acceso. El usuario puede seleccionar un directorio local con el comando lcd ("local change directory"). La sintaxis de estos comandos depende del sistema operativo.

Listado de ficheros disponibles para una transferencia. Se hace con los sub-comandos dir o ls.

Especificación del modo de transferencia. La transferencia de datos entre sistemas diferentes suele requerir transformaciones de los datos como parte del proceso de transferencia. El usuario ha de decidir dos aspectos de la manipulación de los datos:
La forma en qué se transferirán los bits. Las distintas representaciones de los datos en la arquitectura del sistema. Esto se controla por medio de dos sub-comandos:

Mode: Especifica si el fichero se ha de tratar como si tuviera estructura de registros o como un flujo de bytes.

Block: Se respetan las separaciones lógicas entre registros.

Stream: El fichero se trata como un flujo de bytes. Esta es la opción por defecto, y proporciona una transferencia más eficiente, pero puede que no produzca los resultados deseados cuando se trabaja con ficheros estructurados por registros.

Type: Especifica el conjunto de caracteres usado para los datos.

ASCII: Indica que ambos host están basados en ASCII, o que si uno está basado en ASCII y el otro en EBCDIC, se debería realizar una traducción ASCII-EBCDIC.

EBCDIC: Indica que ambos host se basan en EBCDIC.

Image: Indica que los datos deben tratarse como bits contiguos empaquetados en bytes de 8 bits.

Debido a que estos sub-comandos no cubren todas las posibles diferencias entre sistemas, el sub-comando SITE está disponible para lanzar comandos dependientes del sistema.

Copia de ficheros

Get: Copia un fichero del host remoto al host local.

Put: Copia un fichero del host local al host remoto.

Finalización de la sesión de transferencia

Quit: Desconecta del host remoto y cierra el FTP. Algunas implementaciones usan el sub-comando BYE.

Close: Desconecta del host remoto pero deja al cliente FTP ejecutándose. Se puede lanzar un comando open para trabajar con otro host remoto.

## 2.13 SMTP ("Simple Mail Transfer Protocol")

El correo electrónico (E-mail) es probablemente la aplicación TCP/IP más usada. Los protocolos de correo básicos proporcionan intercambio de correo y mensajes entre hosts TCP/IP; se han añadido servicios para la transmisión de datos que no se pueden representar con texto ASCII de 7 bits.

Hay tres protocolos estándares que se aplican a este tipo de correo. Todos son recomendados. El término SMTP se emplea con frecuencia para referirse a la combinación de los tres protocolos, por su estrecha interrelación, pero estrictamente hablando, SMTP es sólo uno de los tres. Normalmente, el contexto hace evidente de cuál de los tres se está hablando. Cuando haya ambigüedad, se emplearán los números STD o RFC. Los tres estándares son:

Un estándar para el intercambio de correo entre dos ordenadores (STD 10/RFC 821), que especifica el protocolo usado para enviar correo entre hosts TCP/IP. Este estándar es SMTP.

Un estándar (STD 11) para el formato de los mensajes de correo, contenido en dos RFCs. El RFC 822 describe la sintaxis de las cabeceras y su interpretación. El RFC 1049 describe como un conjunto de documentos de tipos diferentes del texto ASCII plano se pueden usar en el cuerpo del correo (los mismos documentos están en ASCII de 7 bits con información de formato embebida: Postscript, Scribe, SGML, TEX, TROFF y DVI aparecen en el estándar). El nombre oficial del protocolo para este estándar es MAIL.

Un estándar para el encaminamiento de correo usando el DNS, descrito en el RFC 974. El nombre oficial del protocolo para este estándar es DNS-MX.

El STD 10/RFC 821 establece que los datos enviados por SMTP son ASCII de 7-bits, con el bit de orden superior a cero. Esto es adecuado para mensajes en inglés, pero no para otros lenguajes o datos que no sean texto. Hay dos estrategias para superar estas limitaciones:

MIME ("Multipurpose Internet Mail Extensions"), que especifica un mecanismo para codificar texto y datos binarios en ASCII de 7 bits en el mensaje.

SMTPSE ("SMTP Service Extensions"), que define un mecanismo para extender las posibilidades de SMTP más allá de las limitaciones.

Un protocolo para la declaración del tamaño del mensaje que permite a un servidor informar al cliente del tamaño máximo de mensaje que puede aceptar. Sin esta extensión, un cliente sólo puede ser informado de que un mensaje ha excedido el tamaño máximo (sea fijo o temporal, por falta de espacio en el servidor) tras transmitir todo el mensaje. Cuando esto sucede, el servidor desecha el mensaje. Con ella, el cliente puede declarar el tamaño estimado del mensaje y el servidor devolverá un error si es demasiado grande.

Todas estas extensiones son borradores y tienen status efectivo.

### 2.14 Cómo funciona SMTP

SMTP está basado en la entrega punto-a-punto; un cliente SMTP contactará con el servidor SMTP del host de destino directamente para entregar el correo. Guardará el correo hasta que se haya copiado con éxito en el receptor. Esto difiere del principio de retransmisión común a muchos sistemas de correo en las que el correo atraviesa un número de host intermedios de la misma red y donde una transmisión con éxito implica sólo que el correo ha alcanzado el host correspondiente al siguiente salto.

En varias implementaciones, existe la posibilidad de intercambiar correo entre los sistemas de correo locales y SMTP. Estas aplicaciones se denominan pasarelas o puentes de correo. Enviar correo a través de una pasarela puede alterar la entrega punto-a-punto, ya que SMTP sólo garantiza la entrega fiable a la pasarela, no al host de destino, más allá de la red local. La transmisión punto SMTP en estos casos es host-pasarela, pasarela-host o pasarela-pasarela; SMTP no define lo que ocurre más allá de la pasarela. CSNET proporciona un interesante ejemplo de servicio de pasarela de correo. Diseñada en principio como un servicio barato para interconectar centros científicos y de investigación, CSNET opera una pasarela que permite a sus suscriptores enviar y recibir correo en Internet con sólo un módem con dial. La pasarela sondea a los suscriptores a intervalos regulares, les entrega su correo y recoge el correo de salida. A pesar de no ser una entrega punto-a-punto, ha demostrado ser un sistema muy útil.

Cada mensaje tiene:

Una cabecera. La cabecera termina con una línea nula (una línea con sólo la secuencia).

Contenido. Todo lo que hay tras la línea nula es el cuerpo del mensaje, una secuencia de líneas con caracteres ASCII(aquellos con valor menor del 128 decimal).

Como siempre, el cliente SMTP es el que inicia la sesión (el emisor) y el servidor el que responde a la solicitud de sesión(el receptor). Sin embargo, como el cliente suele actuar como servidor para un programa de correo del usuario, es más sencillo referirse a él como emisor SMTP, y al servidor como receptor SMTP.

## 2.15 Adaptación De Celdas AAL

En contraste con otras técnicas de transmisión por paquetes no está previsto en la capa 2 una comunicación del tipo HDLC.

Sub-Capas AAL. En la capa AAL (ATM Adaptation Layer) se configura el payload de la celda. Se trata de dos sub-capas:

SAR (Segmentation and Reassembly Sublayer): Procesa y segmenta las unidades de datos en celdas.

CS (Common Part Convergence Sublayer): Para funciones de multiplexación y detección de pérdida de celdas.

Las funciones de adaptación son distintas para un tren de datos continuo o para servicios en paquetes. En la capa 2, para servicios de datos continuos, se realiza el ensamblado de celdas, la compensación de retardo variable y el tratamiento en el caso de pérdidas de celdas. Cuando se trata de servicios en paquetes se efectúa la segmentación, y el relleno de celdas parcialmente ocupadas, la adaptación de velocidad y el tratamiento en caso de pérdida de celdas.

## 2.16 Tipos de Servicios AAL

Se disponen de dos tipos de servicios de acuerdo con la tasa de generación de datos: La tasa de bits constante CBR (Constant Bit Rate) sensible al retardo y a la latencia y la tasa variable VBR (Variable Bit Rate) insensible a pequeños retardos.

Servicio Tipo AAL1. En Tabla 3.1 se muestra información de cada clase. Son ejemplos de este tipo de servicio la telefonía y la TV convencional. Se trata de servicios sensibles al retardo y la pérdida de celdas. Se debe emular un circuito de velocidad constante (Circuit Emulation) para una conexión convencional (línea dedicada). La tasa de datos es constante y la conexión es permanente; requiere sincronismo de bit y detección de celdas perdidas para un eventual relleno o la interpolación de datos perdidos.

| | |
|---|---|
| | **Tipo AAL1.** |
| -SN | 4 bits. (Sequence Number) Para numeración de la secuencia transmitida. |
| .CSI | 1 bit. Indicador de sub-capa de convergencia. |
| .SCF | 3 bits. Campo de conteo secuencial de celdas (módulo 8). Para detección de celdas perdidas y permitir la interpolación de muestras. |
| -SNP | 4 bits. (SN Protection) Para protección de SN. Contiene: |
| .CRC | 3 bits. Campo de chequeo de errores para corregir un error en SN (polinomio $X^3+X+1$). |
| .P | 1 bit. Bit de paridad para detectar 2 errores. |
| | **Tipo AAL2.** |
| -Head | 1 byte. Para secuenciamiento e identificación de celda |
| .SN | 4 bits. Para numeración de la secuencia transmitida. Similar a AAL1. |
| .CT | 4 bits. (Celd Type) Identifica el tipo de celda (única, inicio, medio, final) en una segmentación. |
| -Trailer | 2 bytes. Para corrección de errores en la carga útil de la celda. |
| .LI | 6 bits. Indicador de longitud de la información en la carga útil en celdas parcialmente ocupadas. |
| .FEC | 10 bits. Permite corrección de 2 errores mediante CRC. |
| | **Tipo AAL3/4.** |
| -ST | 2 bits. (Segment Type) Identifica al segmento único, al inicio, continuación y al final del mensaje. |
| -SN | 4 bits. Para numeración de la secuencia módulo 16. |
| -MID | 10 bits. (Multiplexing Identifier) Reservados en el tipo 3 y usados en el tipo 4 como: |
| .P | 1 bit. Permite 2 niveles de prioridad. |
| .MID | 9 bits. Identificador de multiplexación para distintos usuarios. |
| -LI | 6 bits. (Length Indicator) Indicador de longitud en Bytes de celdas parcialmente ocupadas (máximo 44). |
| -CRC | 10 bits. Para corrección de 1 error en los 48 bytes. Polinomio generador: $X^{10}+X^3+1$. |
| | **Tipo AAL5. (No posee bytes reservados para sub-capa SAR)** |

Tabla 3.2 Carga útil para servicios AAL en la sub-capa SAR.

Se procede a segmentar la información para una carga útil de 44 Bytes. El campo ST identifica el inicio BOM (Beginning Of Message), la continuación COM (Continuation OM) y final de la segmentación EOM (End OM); así como un segmento individual SSM (Single SegMent). El campo SN determina la numeración secuencial de las celdas producidas por la misma segmentación. Si falta una celda la segmentación completa es descartada. Este tipo de numeración no detecta la pérdida de un múltiplo entero de 16 celdas; para ello se dispone del campo CS y Btag/Etag (son valores idénticos y avanza en forma secuencial a cada mensaje que se transmite). El campo MID identifica a todas las celdas de la misma segmentación. El campo de longitud PL para EOM y SSM es múltiplo de 4 Bytes; el campo PAD se ocupa de asegurar esta variable mediante relleno de tipo 00...0.

Servicio Tipo AAL5. En AAL5 se admiten celdas dedicadas sin encabezamiento adicional a los 5 Bytes de ATM. La trama formada en la sub-capa CS contiene un campo de compensación PAD e indicadores similares a ALL3/4. No soporta la función de multiplexación y por ello se la aplica para datos de señalización y Operación sobre ATM. AAL5 es útil para aplicaciones de Internet sobre ATM. Se define también la interfaz ILMI (Interim Local Management Interface) para operar el protocolo SNMP sobre AAL5. Ver la Tabla 3.2.

La sub-capa SAR utiliza un Byte de la carga útil de la celda para numeración secuencial, permitiendo actuar al buffer que absorbe las variaciones del retardo e ingresar una celda sustituta cuando una celda se ha perdido (la capa 1b descarta las celdas que contienen error en el encabezado). El campo posee una verificación de error para comprobar errores en la numeración secuencial. En AAL1 el formato puede ser con-puntero o sin-puntero. Al usar puntero, un Byte de la carga útil (restan 46) se utiliza para indicar el corrimiento entre el puntero y el inicio de los datos. Esto es útil en el caso de ingresar datos en tramas estructuradas por bytes.

| Calificación del Servicio | A | B | C | D |
|---|---|---|---|---|
| Tipo / Atributos AAL | 1 | 2 | 3/4-5 | 3/4 |
| Tasa de bits constante CBR | X | | | |
| Tasa de bits variable VBR | | X | X | X |
| Orientado con conexión | X | X | X | |
| Orientado sin conexión | | | | X |
| Ritmo end-end temporizado | X | X | | |
| Ritmo end-end no-mantenido | | | X | X |
| Video y voz a velocidad constante | X | | | |
| Video y voz a velocidad variable | | X | | |
| Datos X.25, Frme Relay y SMDS | | | X | |
| Red de área local LAN e Internet | | | | X |

Tabla 3.1 Clase de servicios ATM y trama AAL.

Servicio Tipo AAL2. La información de telefonía o vídeo codificada a velocidad variable es tipo AAL2 y tratándose de un servicio orientado a la conexión la tasa de celdas no es constante. Este servicio aún no está disponible pero su aplicación en el futuro será de importancia cuando la tarifa de estos servicios involucre el número de celdas transportadas.

Servicio Tipo AAL3/4. La transmisión de datos dispone de dos tipos de alternativas: AAL3/4 y AAL5. Se trata de servicios que admiten el retardo producido por la red. En el tipo AAL3/4 se tiene previsto aceptar celdas desde SMDS (IEEE 802.6) y Frame Relay. En AAL3/4 la sub-capa SAR ocupa 4 Bytes (2 de cabecera y 2 de trailer) en la carga útil de la celda.

# CAPÍTULO III
# TCP/IP sobre ATM

## 3.1 Consideraciones para una red ATM

Un Administrador de llamadas UNI ATM que cumple las especificaciones del Foro ATM para la señalización en ATM y admite la creación de circuitos virtuales conmutados (SVC) y circuitos virtuales permanentes (PVC).

Un módulo de cliente de emulación de LAN que cumple la especificación LANE 1.0 del Foro ATM, que permite a programas y protocolos existentes diseñados para redes Ethernet y Token Ring ejecutarse en una red ATM sin modificarlos.

Un servicio ARP/MARS que permite a la pila TCP/IP de Microsoft resolver las direcciones ATM en direcciones de hardware para utilizar de un modo más directo y eficaz los medios ATM. El módulo IP sobre ATM cumple las especificaciones RFC del protocolo de resolución de direcciones (ARP) sobre medios ATM, así como la compatibilidad con un servicio de resolución de direcciones de multidifusión (MARS).

Compatibilidad mejorada con programas y servicios TAPI.

Compatibilidad con filtrado de acceso a canales sin procesar para su uso en entornos de programas que incluyan DirectStreaming.

Compatibilidad ampliada con acceso telefónico PPP sobre medios ATM, que permite crear y usar una conexión de acceso telefónico PPP en cualquier adaptador ATM compatible instalado en un equipo con un sistema operativo Windows Server 2003. Esta característica proporciona compatibilidad con ATM sobre DSL, ATM sobre módem por cable y otras opciones de conectividad ATM a petición.

Acceso a servicios nativos ATM con Winsock 2.0 sobre ATM. Disponible a través del Windows Sockets ATM Service Provider, Winsock 2.0 permite el acceso directo a los servicios ATM de programas en modo de usuario. También permite a los programas que emplean TCP/IP como protocolo de transporte ejecutarse en redes ATM e interoperar con clientes IP estándar basados en LAN.

Ethernet encapsulado sobre una conexión virtual permanente (PVC), que permite la transmisión de paquetes de Ethernet a través de PVC en un adaptador de red

ATM. Para efectuar esto, actúa como un adaptador de Ethernet para el protocolo TCP/IP y utiliza PVC en el adaptador ATM para transferir paquetes de Ethernet.

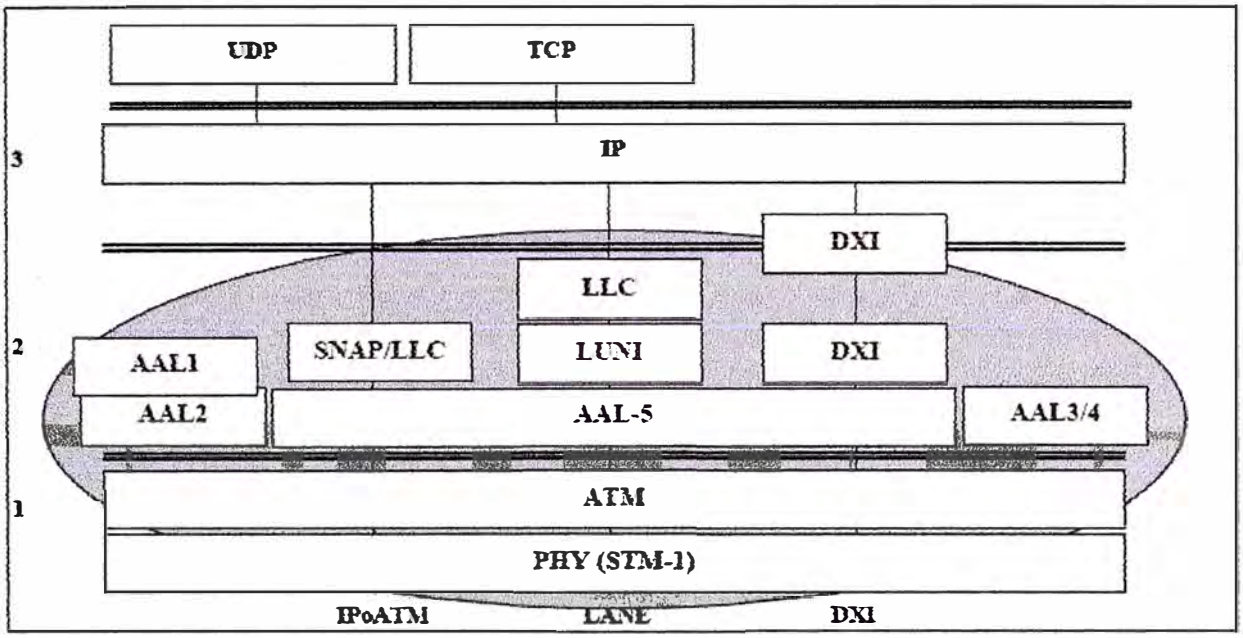


Figura 3.1 Modelo de capas para TCP/IP sobre ATM.

## 3.2 Protocolos para Redes ATM

La tecnología ATM continúa evolucionando y siendo fuente de interesantes y novedosas propuestas. El desarrollo de avanzados protocolos de comunicaciones es uno de los campos de investigación más activo, con la aspiración de ofrecer el adecuado soporte a las nuevas aplicaciones adaptadas a las clases de servicio nativas ATM. Los protocolos son los responsables, entre otras funciones, de garantizar la QoS demandada por los usuarios de avanzados servicios multimedia. En este contexto son aspectos clave los relativos a los protocolos nativos ATM, así como las características multicast, la escalabilidad y la fiabilidad.

La actual demanda de aplicaciones relacionadas con información multimedia, como son la videoconferencia, audio-conferencia, video bajo demanda (VoD) o sistemas colaborativos (pizarras compartidas, teletrabajo, telemedicina, etc.) y su coexistencia con aplicaciones más clásicas (bases de datos, transferencias de ficheros, WWW, etc.), requiere de tecnologías de comunicaciones capaces de ofrecer elevadas prestaciones. Estas prestaciones están directamente relacionadas con la QoS y, más concretamente, con conceptos parametrizables como el ancho de banda y la velocidad de transmisión (throughput), el retardo de las transferencias (delay); la variabilidad en los retardos (jitter); la fiabilidad (reliability) de las transmisiones; las características de multidifusión a grupos

dispersos de usuarios (multicast) y la posibilidad de gestionar múltiples clases de servicio o flujos de información en redes multiclass.

Para que las nuevas tecnologías en comunicaciones puedan ofrecer estas características es necesario revisar, potenciar y ampliar las actuales arquitecturas, servicios y protocolos de comunicaciones. En los últimos años, las investigaciones en el campo de ATM están dando lugar a importantes propuestas cuyo principal objetivo es ofrecer a las aplicaciones más demandadas algunas, todas o superiores características a las citadas anteriormente.

Por este motivo, se revisan algunos de los más importantes conceptos, técnicas, ideas y mecanismos en materia de protocolos de altas prestaciones para redes de tecnología ATM.

### 3.3 Conceptos Clave

La tecnología ATM ofrece importantes características como la integración de servicios, el elevado rendimiento y la escalabilidad. Las aplicaciones multimedia son el objetivo de las redes ATM ya que éstas requieren de características como la garantía de QoS y el soporte multicast. Las redes ATM se caracterizan también por congestiones indeterministas en los conmutadores causadas por ráfagas esporádicas provenientes de varias fuentes, y por frecuentes, inesperados y repentinos cambios en el ancho de banda disponible debidos a llegadas y salidas de conexiones ABR, CBR, VBR o UBR. ATM es, por tanto, una tecnología de comunicaciones mucho más sofisticada y compleja que otras como X.25, IP, Frame Relay, etc.

### 3.4 Modo Nativo

Las aplicaciones nativas ATM están específicamente pensadas para usar la tecnología ATM y para explotar al máximo sus especiales características. Los protocolos nativos se encargan, por tanto, de ofrecer esas características intrínsecas de las redes de tecnología ATM (soporte de QoS, señalización, direccionamiento, etc.) a las aplicaciones nativas ATM (VoD, pizarras compartidas, video-conferencia, etc.). No obstante, existen también activas investigaciones para conseguir soportar sobre redes ATM aplicaciones no nativas ATM desarrolladas para otras tecnologías (IP, Frame Relay, SMDS...).

El termino native ATM services define servicios ATM específicos disponibles para el software y hardware residentes en dispositivos de usuario UNI ATM. Por tanto, el

programador de aplicaciones dispone de nuevos servicios entre los que se pueden destacar los siguientes:

Transferencias de datos (fiables o no) usando la capa ATM y varias capas de adaptación (AAL).

Disponibilidad para usar y ofrecer circuitos virtuales conmutados (SVC) y circuitos virtuales permanentes (PVC).

Consideraciones relativas a la gestión de tráfico (clases de servicio, garantías de QoS, etc.).

Posibilidad de distribución de conexiones.

Posibilidad para participar localmente en la administración de la red (protocolos ILMI y OAM).

El propósito de los servicios nativos ATM es ofrecer el acceso a las CoS o a las características de QoS.

Estos servicios nativos también ofrecen soporte a un amplio y heterogéneo rango de flujos con diversas propiedades y requerimientos.

Los protocolos de transferencia nativos ATM gestionan la señalización UNI para establecer los SVC, configurar PVC y mapear los perfiles de QoS en la correspondiente CoS. Los protocolos nativos también realizan funciones clásicas como las de transporte, mecanismos de control de errores, transferencia de datos, y controles de flujo y de congestión.

Es útil contrastar la semántica de los servicios con las redes ATM actuales que usan TCP como capa de transporte, e IP-over- ATM como capa de red. Planteamiento éste que puede considerarse poco adecuado por estas razones:

Las redes IP no garantizan la QoS extremo-extremo ofrecida por las redes ATM a circuitos individuales. IP multiplexa múltiples conexiones de transporte con distintos requerimientos de QoS en VC simples.

TCP no soporta células RM (Resource Management) ABR y, como consecuencia, no puede usar directamente las garantías de QoS ofrecidas por la red.

ATM Adaptation Layer 5 (AAL-5) realiza labores de checksum para detectar corrupción de datos. TCP también realiza estas labores (redundantes con AAL-5) costosas en overhead (cada byte de un paquete debe ser chequeado).

TCP e IP son la representación de un grupo de protocolos anteriores a ATM y que ya han experimentado determinados arreglos y evoluciones, lo mismo que las aplicaciones que los emplean, lo que acaba dando, en algunos casos, inadecuados comportamientos por la evolución independiente de ambas tecnologías.

Estos y otros problemas son eliminados usando pilas de protocolos en modo nativo. La Figura 3.2 muestra el modelo de referencia para servicios nativos ATM.

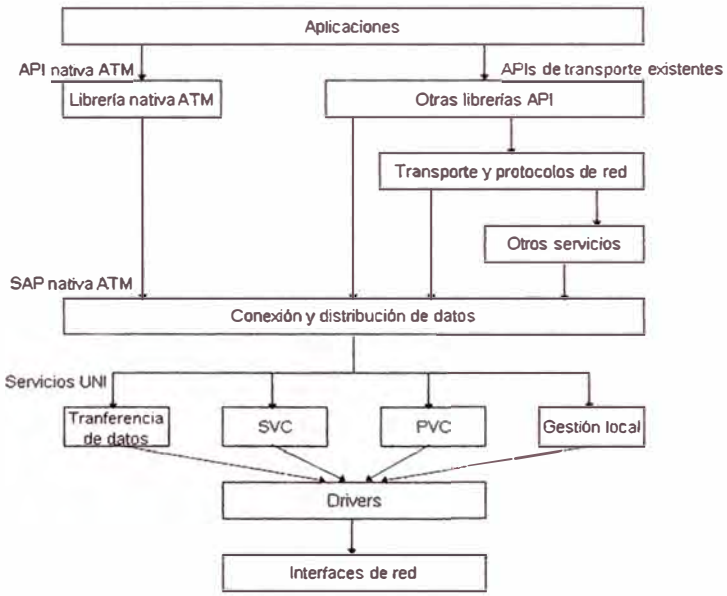


Figura 3.2 Modelo de Referencia para servicios nativos ATM.

Para concluir pueden argumentarse las siguientes razones para justificar el desarrollo de pilas de protocolos nativos ATM:

En la actualidad existen aplicaciones pensadas para explotar avanzados servicios usando tecnología ATM y también existen otras aplicaciones más antiguas y no nativas. Este escenario implica cambiar las aplicaciones o proponer nuevas pilas de protocolos nativos ATM.

La encapsulación consecutiva de paquetes genera problemas de overhead y funciones redundantes como se ha argumentado anteriormente.

La limitación de recursos en los sistemas finales es otra importante motivación para usar pilas de protocolos nativos y ligeros.

La QoS ofrecida por el modo nativo es aprovechada por los usuarios para demandar recursos a los proveedores de servicios en redes privadas. Los proveedores de servicios públicos disfrutan también de estas ventajas.

ATM, RDSI y la telefonía ofrecen un esquema de direccionamiento universal basado en NSAP/E.164 el cual es capaz de enrutar tráfico de forma nativa. Por tanto, aunque ATM dispone de protocolos nativos con direccionamiento intrínseco, estructurado y jerárquico, éste no es aprovechado por las aplicaciones que están basadas en IP. El esquema de direccionamiento ATM es una de las principales dificultades en los protocolos propuestos como nativos.

### 3.5 Escalabilidad

ATM Forum ha normalizado protocolos de routing y señalización para PNNI (Private Network-Network Interface) para conseguir la escalabilidad de las redes ATM. Los actuales estándares proponen esquemas de señalización y routing punto-a-punto.

Los componentes diseñados para ofrecer QoS deben ser escalables, es decir, deben poder ser usados aunque sean aplicados a muy larga escala. Con respecto a las aplicaciones multimedia, la escalabilidad tiene, como poco, dos aspectos clave:

Escalabilidad con respecto al número de participantes en una aplicación: debe ser posible transmitir un flujo multicast a un, potencialmente, muy largo número de participantes. Los protocolos Internet IP-multicast y ST-2+ soportan este requerimiento. RSVP también soporta un cierto nivel de escalabilidad, que puede verse comprometida o ser discutible y matizable en el caso de que existan varios miles de participantes.

Escalabilidad con respecto al número de aplicaciones concurrentes: debería ser posible soportar muchas aplicaciones independientes y, por consiguiente, cientos de flujos simultáneos.

En la actualidad, parece que es más importante la escalabilidad referida a una sola aplicación, pero en el futuro todo dependerá de los requerimientos de cada situación particular.

### 3.6 Transferencia Multicast

Los dos modos clásicos de transferencia de paquetes entre nodos son los conocidos unicast y multicast. En las transferencias unicast un nodo envía paquetes a un único nodo

receptor. Las comunicaciones multicast las constituyen un nodo fuente que realiza una sola operación atómica (sólo se envía una copia de cada paquete sobre un enlace) a un grupo multicast de más de un participante (receptores) no necesariamente en la misma red. Una forma eficiente de hacer esto es construir un árbol de distribución multicast optimizado en coste. El multicasting se usa en aplicaciones multimedia para proveer de datos, audio y video a grupos dispersos de usuarios. El conjunto de participantes puede ser fijo o cambiar dinámicamente durante el curso de la sesión. El broadcast es un caso especial de multicast en el cual los paquetes son transferidos a todos los nodos conectados a una red.

ATM es considerada aún como una tecnología emergente diseñada para ser usada por aplicaciones de datos, audio y video, lo que requiere un buen comportamiento de las transferencias unicast y multicast. User Network Interface (UNI 3.0) para ATM define conexiones punto-a-multipunto, y las conexiones multipunto-a-multipunto sólo pueden ser obtenidas de las dos siguientes formas:

El primer esquema consiste en configurar N conexiones punto-a-multipunto para conseguir conectar todos los nodos en una topología completamente mallada todos-con-todos. Aunque esta topología ofrece conexiones multipunto-a-multipunto, hay que destacar que no escala bien cuando el número de participantes es elevado.

Una alternativa al anterior esquema es el uso de un servidor que actúa a modo de raíz en el árbol multipunto. Este método sólo requiere un nodo raíz para almacenar información, pero la desventaja de este método son las potenciales congestiones en el servidor cuando debe encargarse de envíos y retransmisiones de las conexiones multipunto-a-multipunto.

Para solventar las limitaciones de UNI 3.0 y UNI 3.1 que soportan conexiones uno-a-muchos, pero no directamente (nativamente) conexiones muchos-a-muchos, y ofrecer a ATM verdadero servicio multicast, ATM Forum, ITU-T e IETF han realizado varias propuestas al actual mecanismo de señalización ATM (UNI 3.1, UNI 4.0).

### 3.7 Protocolos Nativos ATM

ATM Forum ha definido las especificaciones y también existen importantes investigaciones en torno a los protocolos nativos ATM. Aquí se mostraran las propuestas más importantes en materia de protocolos nativos ATM.

Conociendo el diseño, implementación y comportamiento de una pila en modo nativo ATM, se contrasta la semántica de su capa de transporte con TCP. Este trabajo es diferente a IP-over-ATM, y justifica el uso de la pila nativa ATM para solventar automáticamente los siguientes problemas:

IP-over-ATM no ofrece garantía de QoS pues sus aplicaciones sólo "ven" la interfaz IP.

El núcleo de los sistemas operativos y los sistemas finales son sobrecargados con considerable complejidad pues el subsistema IP-over-ATM debe encargarse de las peticiones de la señalización.

IP-over-ATM debe emular el routing IP sobre conexiones punto-a-punto de la red ATM, lo que supone pagar un elevado precio en prestaciones.

N3 (Native Non-broadcasting medium access Networking) es un protocolo de transporte ligero y nativo ATM. La pila N3 se ha diseñado para ofrecer servicios multimedia a comunidades residenciales. El documento describe una arquitectura capaz de ofrecer aplicaciones nativas ATM. La pila de protocolo de transporte N3 se basa en implementaciones previas y, además, aporta otras importantes novedades. Los principales componentes de N3 incluyen una API sockets ATM nativa, un protocolo de transporte ATM y un servicio de nombres ATM (ver Figura 3.3).

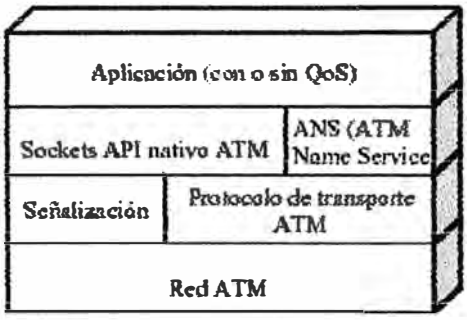


Figura 3.3 Visión de alto nivel de la pila de protocolos.

La arquitectura de servicio ATM en modo nativo ATM es capaz de ofrecer a las aplicaciones nativas ATM acceso completo a las CoS ATM. Los elementos de esta arquitectura se responsabilizan de las transferencias eficientes de datos sobre ATM, del control de errores extremo-extremo, del control de flujo y congestión de la transferencia de datagramas y de la multiplexación de VC.

La Figura 3.4 presenta los elementos de Native Mode Service Architecture donde el Flow Management es el componente más importante. El Flow Management se responsabiliza de manipular los flujos de datos desde y hasta la red vía la interfaz AAL. La segmentación, el reensamblado y el control de errores es también realizada por esta entidad. Para las CoS CBR, VBR y ABR se emplea un sencillo esquema de control llamado Back-Pressure Flow. Para servicios UBR se emplea un control de congestión y de flujo extremo-extremo más complejo.

Investigadores han presentado una nueva arquitectura de protocolo adaptada a la tecnología ATM y a las aplicaciones multimedia. El diseño está basado en tres principios básicos: separación de flujos de control y de datos; minimización del overhead y de la duplicidad de funciones; y acceso de las aplicaciones al nivel ATM con garantías de QoS.

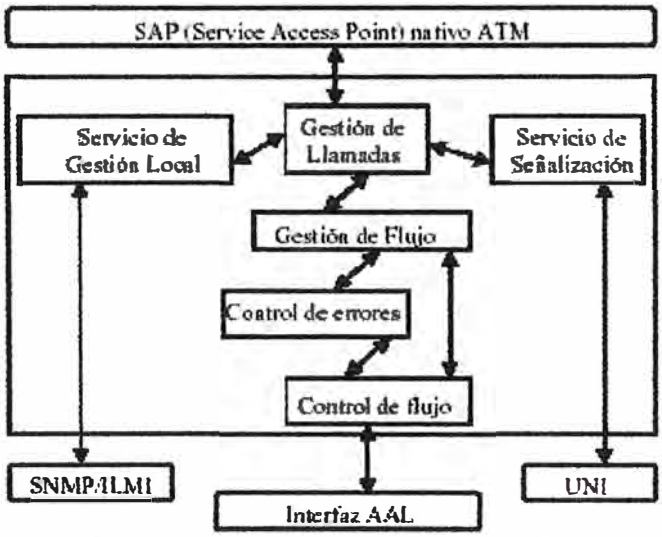


Figura 3.4. Arquitectura de servicio nativo ATM

La idea es mezclar el soporte nativo ATM en la estructura existente del protocolo (Figura 3.5) que muestra dos caminos separados en el protocolo: la familia nativa ATM y la familia del protocolo IP. Las aplicaciones que tienen acceso transparente a la red ATM usan la familia del protocolo PF_INET. El mapeo de IP en ATM es gestionado por la interfaz de red ATM (IF_ATM) usando el protocolo IP-over-ATM.

La interfaz Native ATM está constituida por la familia de protocolos PF_ATM que es directamente soportada encima del dispositivo de red ATM sobrepasando la capa interfaz de red. El módulo CNTL abre una conexión de señalización con el dispositivo ATM y establece una gestión de las llamadas de mensajes de configuración.

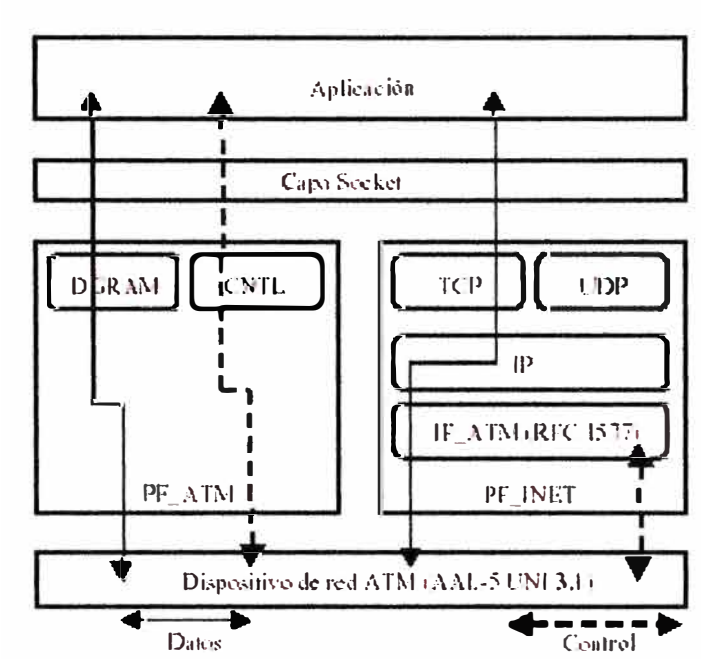


Figura 3.5. Descripción de alto nivel de la arquitectura de protocolo

PF_ATM separa flujos de datos y de control para aliviar el límite de rendimiento en las comunicaciones.

Esto permite a los mecanismos de control de tráfico ser rápidos y sencillos, mientras los mecanismos de control pueden ser tan complicados como sea necesario. Esta separación permite también que los dispositivos puedan estar en los puntos finales de una conexión.

La interfaz PF_ATM aporta a las aplicaciones acceso directo a la capa de enlace ATM y extiende las garantías de QoS a los puntos extremos de la comunicación.

Un segundo prototipo es diseñado e implementado con dos objetivos principales para la mejora de la pila nativa ATM:

Optimizar los caminos de datos entre los adaptadores ATM aprovechando la separación de flujos de control y de datos y la capacidad de gestión de datos específicos de las conexiones de la pila ATM.

Optimizar el procesamiento de overheads usando una pila de protocolos nativo ATM en lugar de UDP/IP.

CONGRESS (CONnection oriented Group-address RESolution Service),

otro eficiente protocolo nativo ATM para la resolución y gestión de direcciones de grupos multicast en una red ATM. El servicio CONGRESS resuelve direcciones de grupo multicast y mantiene los miembros pertenecientes a esos grupos para uso de las aplicaciones. CONGRESS sirve de soporte al servicio IMSS, y ofrece escalabilidad con su diseño basado en los dos siguientes principios:

Diseño jerárquico: los servicios del protocolo son ofrecidos a las aplicaciones por múltiples servidores organizados jerárquicamente.

No inundación: se evita la inundación de la WAN en cada cambio de grupos multicast.

Otra propuesta de arquitectura presenta kStack, una nueva capa de transporte nativa ATM en el espacio de usuario con soporte de QoS. Esta implementación sobre Unix y Windows NT está basada y es compatible con los trabajos originales de Ahuja, Keshav y Saran Native-Mode ATM Stack. El protocolo kStack es similar al original, pero se ha modificado sustancialmente en los siguientes aspectos:

Ha sido implementado en el espacio de usuario.

Se ha ampliado, implementando una capa de transporte con QoS.

Se ha añadido un módulo que monitoriza la QoS extremo-a-extremo.

Kstack es por tanto una implementación en el espacio de usuario de una pila de protocolos en modo nativo ATM sobre la capa de transporte. Soporta QoS para monitorización y adaptación del nivel de aplicación. La QoS es monitorizada para cada conexión extremo-a-extremo e independientemente del resto de conexiones.

### 3.8 Integración IP-ATM

Como ya se ha comentado, ATM aporta elevadas prestaciones como son la escalabilidad de su ancho de banda (desde pocos Mbps hasta varios Gbps), su rendimiento (alta capacidad o velocidad) y su habilidad para integrar y soportar datos, audio y video (tráfico multiservicio). Por otro lado, IP ofrece también atractivas características como su simplicidad, su filosofía abierta y el soporte sobre entornos LAN, MAN y WAN.

Estas y otras causas como la creciente expansión de las aplicaciones IP y la actual implantación y uso de redes ATM han impulsado el rápido crecimiento de ambas tecnologías y en la actualidad existen diversos intentos por combinar las ventajas de ATM e IP para ejecutar aplicaciones Internet sobre redes de tecnología ATM. Esta migración permite a los protocolos y aplicaciones IP disfrutar de las elevadas prestaciones de ATM.

Pero la emulación de IP sobre ATM genera comportamientos no óptimos debidos a las diferencias fundamentales entre ambas tecnologías como, por ejemplo, que mientras ATM es una tecnología orientada a la conexión, IP es un protocolo sin conexión. Además, IP tiene problemas para soportar aplicaciones multimedia y/o en tiempo real, mientras éstas son la principal característica para ATM. Por otro lado, ATM tiene problemas para soportar servicios multipunto, mientras IP tiene resueltas sus posibilidades multicast.

Existen diversas investigaciones para implementar el protocolo IP sobre redes ATM como: IP over ATM (classical), LANEmulation, IP switching, Tag switching, Address resolution NARP, next hop resolution NHRP, MPOA y MPLS.

El principal problema para integrar IP y ATM es aprovechar la velocidad y rendimiento de la tecnología de conmutación y también la escalabilidad y flexibilidad de IP por no ser orientado a conexión. Además, las diferencias comentadas entre ambas tecnologías causan duplicaciones de funcionalidad (IP y ATM requieren sus propios protocolos de routing y funciones de mantenimiento y gestión).

La encapsulación de datagramas para su transmisión a través de una red ATM se deduce de manera directa. En contraste, la asignación de direcciones IP puede ser difícil. Como en otras tecnologías de red, ATM asigna a cada computadora conectada una dirección física que puede emplearse cuando se establece un circuito virtual. Por un lado, como las direcciones físicas de ATM son más grandes que las direcciones IP, una dirección física ATM no puede codificarse dentro de una dirección IP. Así, el IP no puede utilizar la asignación de direcciones estáticas para redes ATM. Por otro lado, el hardware ATM no soporta la difusión. Por lo tanto, IP no puede utilizar ARP convencional para asignar direcciones en redes ATM.

### 3.8.1 Classical IP over ATM

El RFC 1577 del IETF Classical IP over ATM es un intento por ejecutar TCP/IP sobre ATM usando el entorno conmutado ATM como enlace de datos para IP. Se plantea el problema de que mientras IP over ATM ofrece una plataforma para comunicación de datos sobre redes heterogéneas, las aplicaciones IP no se pueden beneficiar de las características de QoS de ATM porque la naturaleza de IP over ATM "esconde" las capas por debajo de ATM para poder conseguir el acceso transparente para IP. Algunos de los principales problemas para integrar IP sobre ATM residen en la implementación de IP multicast sobre ATM.

### 3.8.2 IMSS (IP Multicast Shortcut Service)

Presenta una solución novedosa para IP multicast sobre redes ATM de área extensa. El gran problema es escalar adecuadamente en un entorno ATM amplio, e IMSS supera los problemas de escalabilidad con una mezcla dinámica de servidores multicast y de conexiones directa y completamente malladas. IMSS es un servicio best-effort de IP-multicast sobre ATM.

### 3.8.3 NHRP (Next Hop Resolution Protocol)

Ha sido desarrollado con la intención de facilitar inter-LIS (Logical IP Subnets) VC con el objetivo de aprovechar los beneficios potenciales de ATM que no son empleados en los métodos clásicos como IP over ATM. NHRP es un mecanismo de resolución de direcciones que mapea una dirección IP de destino en una dirección ATM de destino. Aunque NHRP supera algunas de las debilidades de IP over ATM, cuenta también con sus propias limitaciones como la imposibilidad para soportar multicast.

### 3.8.4 IP switching y Tag switching

Son dos técnicas actuales de conmutación propuestas para ofrecer a las redes ATM mecanismos de routing IP. Ambas están basadas en un mecanismo de intercambio de etiquetas, pero sus implementaciones son diferentes. Ambas técnicas mejoran el routing IP clásico, aunque entre ellas no se encuentran diferencias espectaculares en cuanto al rendimiento se refiere. A continuación se comentan brevemente estos dos mecanismos de conmutación.

IP switching (ATM bajo IP) es una alternativa para obviar la conexión extremo-extremo de ATM e integrar su hardware directamente con IP preservando su característica nativa de no orientación a conexión.

Para ello implementa IP directamente sobre el hardware ATM mientras mantiene el modelo no orientado a la conexión característico de IP. IP switching soporta también IP multicast y, como la conexión extremo-extremo es desechada, no se necesitan la señalización ni el direccionamiento, siendo únicamente necesarios los protocolos estándares de routing IP. Un conmutador IP es idéntico a un conmutador ATM, sin modificación de hardware alguno, pero al que se ha eliminado completamente el software residente en el procesador de control bajo AAL-5 (señalización, protocolo de routing, resolución de direcciones, etc).

Constan de GSMP (General Switch Management Protocol) que es un protocolo de bajo nivel para controlar y permitir el acceso del conmutador hardware al controlador de acceso del conmutador IP. El controlador del conmutador IP ejecuta software estándar de routing IP con extensiones como IFMP (Ipsilon Flow Management Protocol) que se encarga de asociar los flujos IP con circuitos virtuales ATM. IFMP puede ser visto como un protocolo de señalización, aunque se ejecuta independiente en cada link y simplemente asocia una etiqueta local con un flujo IP.

Mientras otros métodos (IP over ATM y LANE) proponen un modelo de red como medio lógico compartido encima de la red ATM, IP switching propone un modelo de red más natural para ATM basado en técnicas punto-a-punto en lugar de usar el modelo clásico de nube.

IP switching separa cuidadosamente los actos de etiquetar y conmutar un flujo lo que le permite asegurar la escalabilidad en redes extensas. El etiquetado o la conmutación para un link particular no afecta al resto de las redes.

CSR (Cell Switch Router), como IP Switch, usa un protocolo para ligar un flujo a un VCI y, por tanto, sólo se necesita un único VCI en el controlador del conmutador. La propuesta CSR permite el uso de PVC o SVC en una red ATM. El mecanismo CSR híbrido conmutador/router dispone de todas las funciones habituales en los routers IP y es capaz de ofrecer un servicio de reenvío IP no orientado a la conexión.

Por otro lado, la técnica de Tag switching emplea una componente de control y otra de reenvío. El control se encarga de crear y mantener un Tag Information Base (TIB) sobre un grupo de routers tag-switching interconectados. La componente de reenvío usa las entradas existentes en la TIB y la etiqueta de cada paquete para realizar el reenvío de los paquetes a sus correspondientes routers. La información es distribuida entre routers Tag-switched mediante el protocolo TDP (Tag Distribution Protocol).

Para la asignación de una etiqueta a una ruta existen tres esquemas en Tag switching:

Downstream allocation: esquema llamado así porque las etiquetas salientes son asignadas por los nodos ya atravesados por el flujo de paquetes. El ruteador Tag-switched crea en su TIB una entrada para cada ruta existente en su tabla de rutas. El ruteador asigna una etiqueta a esa ruta y la almacena como etiqueta entrante

en su TIB, avisando del hecho a sus ruteadores Tag-switched adyacentes. Cuando las entradas de una ruta han concluido pueden ser usadas por la fase de reenvío.

El esquema Downstream-on-demand allocation es similar al anterior, salvo en que un ruteador Tag-switched aún no atravesado por el flujo, se encarga de solicitar a los ya pasados una etiqueta para una ruta específica.

En el esquema Upstream allocation las etiquetas son asignadas por los nodos aún no alcanzados por el flujo, mientras los nodos alcanzados son notificados.

### 3.8.5 ARIS (Aggregated Route-Based IP Switching)

Es, como Tag-switching, una aproximación a IP over ATM que proponen asignación de etiquetas en función de la topología de la red. Las etiquetas son asignadas en función de la información obtenida por los protocolos de routing, y las conexiones virtuales son establecidas antes de que el tráfico sea recibido. ARIS introduce el concepto de egress identifier para definir granularidad. Para cada valor de identificador de salida el protocolo ARIS establece un árbol multipunto-a-punto. ARIS, como Tag-Switching, soporta multicast.

### 3.8.6 MPOA (MultiProtocol Over ATM)

Aparte de las técnicas de conmutación IP que acaban de comentarse existe también la propuesta oficial del ATM Forum que es MPOA (MultiProtocol Over ATM) basada en otras tecnologías existentes como LANE (que ofrece puenteo de nivel 2) y NHRP (que ofrece encaminamiento de nivel 3). Al combinar puenteo y encaminamiento, MPOA es capaz de soportar protocolos encaminables y no encaminables (IP, IPX, DECnet, AppleTalk, etc.) lo que aporta el calificativo multiprotocolo a MPOA. Aunque no ofrece QoS directamente, ésta es proporcionada por LANE, lo mismo que el soporte multicast. Es importante destacar también que existen investigaciones en marcha para permitir la interoperación entre MPOA y RSVP. MPOA simplifica las comunicaciones entre redes virtuales y, como reduce el protagonismo de los routers en el envío de tráfico, permite obtener mejoras de rendimiento. Los otros métodos de conmutación más importantes (IP Switching y Tag-Switching) quizás aporten mejores prestaciones en cuanto a soporte multicast, QoS y a gestión de tráfico. MPOA ofrece emulación transparente de protocolos enrutados sobre red ATM, lo mismo que LANE ofrece emulación transparente de protocolo LAN sobre red ATM. MPOA opera a niveles 2 y 3 y algunos de sus principales aspiraciones son: permitir a los dispositivos MPOA establecer conexiones ATM directas;

integración con LANE; soporte de multicast y broadcast; y separación de conmutación y routing.

Sobre todo cabe destacar que, mientras las propuestas de IETF se preocupan por soportar IP sobre todas las tecnologías estructuradas en capas (ATM es una de ellas), ATM Forum intenta solventar que todos los protocolos de nivel 3 (IP es uno de ellos) se ejecuten sobre ATM.

Existe otra gran familia de soluciones para el soporte de tráfico de datos TCP sobre la clase de servicio ATM-UBR que se encargan de ofrecer rendimiento, justicia y de mantener controlado el retardo. PPD (Partial Packet Discard), EPD (Early Packet Discard), RED (Random Early Detection) y FBA (Fair Buffer Allocation) son algunos de los esquemas de gestión de buffers ATM pensados para ofrecer elevado rendimiento y justicia.

EPD es una técnica para mantener la integridad de los paquetes mientras se producen sobrecargas en los conmutadores ATM. Esta técnica de gestión de buffers ATM asegura elevado rendimiento extremo-extremo para aplicaciones que generan datos a ráfagas durante periodos de sobrecarga. En realidad, EPD es uno o varios de los mecanismos propuestos para la gestión de congestiones en redes ATM.

Por otro lado, PPD es otro conocido esquema de control de congestión para ATM-UBR. PPD descarta las células después de rebasar el tamaño del buffer. La diferencia con EPD es que PPD descarta partes de paquetes. PPD alivia el efecto de fragmentación de paquetes, a la vez que presenta una variante de EPD consiguiendo mejorar los parámetros de rendimiento y justicia ofrecidos por este esquema.
RED es otra técnica para mantener elevado rendimiento mientras se minimiza el retardo en la clase de servicio UBR. RED controla el tamaño medio de la cola y se deshace de los paquetes cuando cambia la carga de la red. RED también identifica las conexiones que comparten elevados anchos de banda.

El protocolo AREQUIPA (Application REQuested IP over ATM) es un mecanismo que permite a las aplicaciones IP solicitar SVC con QoS garantizada. El RFC 2170 describe este protocolo como un mecanismo para establecer conexiones ATM extremo-a-extremo.

Hay que destacar otro planteamiento general en cuanto a la integración de IP con ATM. En este caso se trata del protocolo RSVP (Resource ReSerVation Protocol) pensado para ofrecer QoS a los flujos IP o IPQoS. IP ofrece entrega best-effort de datagramas que es suficiente para servicios clásicos como correo electrónico, WWW o transferencias de correo. Sin embargo, las aplicaciones multimedia requieren las garantías de servicio que IP no ofrece, por lo que IETF ha creado el grupo de trabajo Integrated Services cuyo principal objetivo es el soporte eficiente en Internet de aplicaciones que requieran garantías de servicio.

En este contexto se ha desarrollado RSVP como un protocolo de señalización para Internet encargado de potenciar las redes IP para ofrecer QoS extremo-extremo y no relacionado con ATM, aunque sus objetivos sean los mismos. No obstante, existen trabajos en desarrollo pensados para la interrelación de RSVP con ATM.

Otra novedosa propuesta donde la integración de IP y ATM es una aspiración importante, es MPLS (Multi Protocol Label Switching). MPLS propone el reenvío de paquetes basado en etiquetas que son asignadas cuando los paquetes entran en la red. Los nodos MPLS reenvían los paquetes y/o células ATM basándose en las etiquetas, en lugar de fijarse en la información IP. Esto permite el reenvío del tráfico de la misma forma, tanto en los conmutadores ATM como en los routers. Sin embargo, el encolado ATM viene dado por los valores de las etiquetas (VCI), y el encolado en los routers está determinado por los valores de determinados bits de la cabecera. Es importante destacar que los conmutadores ATM no pueden analizar las cabeceras de la capa 3, y que las etiquetas pueden ser distribuidas por diferentes protocolos como LDP, RSVP, PIM, BGP, etc.

### 3.9 TCP sobre ATM

En lo relativo a las investigaciones sobre la evaluación del rendimiento de TCP sobre ATM éstas se pueden dividir en tres grandes grupos:

Las que se fijan en el dinamismo de TCP.

Las que atienden al comportamiento de ATM.

Las que prestan atención a la interacción entre las ventanas de TCP y los mecanismos de control de congestión de la capa ATM.

Aunque la evaluación del rendimiento de TCP sobre ATM ha sido fuente de diversas investigaciones, las propuestas resuelven sólo problemas particulares como es la

fragmentación de TCP, los requerimientos de buffers, la interacción entre los esquemas de congestión de TCP y ATM, y la degradación de TCP.

La mayor parte de aplicaciones de datos no son capaces de predecir sus propias necesidades de ancho de banda, por lo que se necesita de algún servicio que permita a todos los usuarios activos de la red compartir dinámicamente el ancho de banda disponible. Sabemos que en el caso de ATM las CoS ABR y UBR son la propuesta estándar para soportar el tráfico de datos. En redes TCP sobre ATM se comprueba cómo el throughput de TCP cae también cuando se comienzan a descartar células en los conmutadores ATM. El bajo throughput conseguido se debe al desaprovechamiento del ancho de banda en los enlaces congestionados que transmiten células de paquetes corrompidos, es decir, paquetes en los cuales se ha tirado alguna de sus células. Otras investigaciones han demostrado que TCP sobre UBR con EPD experimenta una apreciable degradación en el funcionamiento, requiriendo además de un tamaño de buffer relativamente grande, incluso con pocas conexiones. Sin embargo, cuando se emplea la CoS ABR con esquemas de realimentación de velocidad explícita ofrecen a TCP mejor comportamiento y aprovechamiento de los enlaces y, todo ello, con tamaños de buffer menores que con UBR.

Existen otras formas de evitar la degradación del throughput de fuentes TCP sobre UBR. Para ello lo que se hace es desactivar los descartes de células ATM durante un periodo de tiempo en el que se están produciendo congestiones. De este modo se evitan los timeouts de TCP que son la principal causa de descenso del throughput de TCP, y se acortan los periodos de congestión evitando el gran retardo experimentado con el algoritmo de retransmisión rápida de TCP antes de que el emisor reciba los ACK duplicados.

Uno de los principales problemas que experimentan las fuentes de tráfico TCP cuyos segmentos son transferidos sobre ATM es que, al usarse como indicación de congestión la propia pérdida de paquetes, esto provoca que la gestión de las congestiones se realice cuando ya es demasiado tarde. Es decir, cuando el buffer se llena, el conmutador descarta los paquetes, el receptor detecta la pérdida y éste avisa al emisor que acaba reaccionando con la retransmisión de los paquetes perdidos. Se impone por tanto la necesidad de aportar mecanismos más ágiles para la solución de las congestiones del tráfico TCP que es transferido sobre tecnología ATM.

Nos encontramos con la característica que TCP es un protocolo orientado a conexión y fiable (confirmación de segmentos entregados), mientras que ATM es también orientado a conexión pero no ofrece de forma estándar ningún mecanismo de confirmación de células entregadas. Puede hablarse así de comportamientos independientes entre ambas tecnologías. Además, cuando TCP funciona sobre ATM, el control de la red es más complejo por requerirse un mecanismo de control de congestión diferente en cada una de las capas. Existen dos diferencias básicas entre los esquemas de control de congestión de TCP y la CoS ABR de ATM:

El mecanismo de realimentación de ABR con células RM controla la velocidad de transmisión de las células desde el emisor (control de velocidad), mientras el mecanismo de realimentación de TCP controla el tamaño de una ventana (control de créditos)

El mecanismo de realimentación de ABR puede ser realizado por conmutadores intermedios de la red, o por el extremo receptor del tráfico, mientras en TCP el mecanismo de realimentación es realizado sólo por el nodo destino mediante ACK extremo-a-extremo que es lo que aporta la fiabilidad a TCP.

En las fuentes TCP el tráfico máximo es controlado por la ventana CWND. Sin embargo, en el caso de la CoS ABR de ATM el tráfico es controlado por diversos parámetros como MCR, PCR y ACR. Son también aspectos clave para TCP sobre ATM los mecanismos de gestión de tráfico usados en los nodos extremos de TCP, en los nodos extremos de ATM y en los conmutadores de la red para, entre todos ellos, aportar el adecuado goodput para reducir el retardo causado por las retransmisiones. El retardo de procesamiento de los paquetes TCP es un periodo de tiempo aleatorio que modela la media del retardo de procesamiento de paquetes con una cierta variación de retardo. Esto se aplica, tanto a paquetes de datos, como a los de confirmación entre emisores y receptores.

A la vista de todas estas características diferenciadoras y, dado que ATM es siempre un protocolo situado por debajo del protocolo de la capa de transporte TCP, se requieren soluciones para resolver los problemas de rendimiento provocados por la integración de ambas tecnologías. Estas soluciones parece lógico que estén en la línea de realizar cambios en los conmutadores ATM dentro de la red, o bien en la nueva implementación de extensiones para TCP, o también en la propuesta de protocolos especializados para los nodos que están en los límites de la red ATM con la red TCP.

# CAPÍTULO IV
# BENEFICIOS Y LIMITACIONES

## 4.1 Beneficios de ATM

ATM proporciona una solución flexible y escalable a la necesidad creciente de calidad de servicio en redes compatibles con varios tipos de información (como datos, voz, y vídeo y sonido en tiempo real). Con ATM, cada uno de estos tipos de información puede circular por una única conexión de red.

ATM ofrece las ventajas siguientes:

- Comunicación de alta velocidad
- Servicio orientado a la conexión, similar a la telefonía tradicional
- Conmutación rápida mediante hardware
- Un único transporte de redes universal e interoperable
- Una única conexión de red que puede mezclar de forma fiable voz, vídeo y datos
- Asignación flexible y eficaz del ancho de banda de la red

## 4.2 Limitaciones de ATM

En general, las soluciones a los problemas de congestiones se basan en equipar a los nodos intermedios de la red con mecanismos que permitan solventar estas situaciones de forma local sin implicar, ni al resto de la red, ni tampoco a las fuentes emisoras.

La tecnología ATM no emplea ningún mecanismo de confirmación de células entregadas para conseguir el mejor throughput posible que se vería afectado si se confirmasen las células de forma individual. Sin embargo, pueden usarse muy diversos mecanismos de solicitud de retransmisión de células perdidas, siempre agrupadas en PDU. Este mecanismo de feedback puede acabar provocando el también indeseable problema de la implosión sobre la fuente emisora de tráfico. La implosión es indeseable en todo tipo de aplicaciones pero, sobre todo, en aquellas en las que están implicados varios destinatarios en conexiones punto-multipunto ó multipunto- multipunto.

Por otro lado, aparecen otros fenómenos indeseables que provocan que las conexiones ATM no dispongan de servicio garantizado. Este tipo de problemas está también relacionado con las impredecibles congestiones que pueden producirse en los conmutadores. Uno de estos problemas es la fragmentación de las PDU que se ven afectadas por una congestión y que son descartadas parcialmente por no tener cabida en el buffer de los conmutadores. Éstos no son capaces de tratar las PDU como unidades de transferencia en la conmutación, por lo que las PDU pueden continuar su camino en dirección al destino fragmentadas cuando sabemos "a priori" que serán detectadas como corruptas por haber perdido parte de sus células.

La multiplexación en el mismo buffer de las células que provienen de varias fuentes provocan el segundo problema que es el de la mezcla (interleaving) en el mismo puerto de salida de células alternas de diferentes conexiones que tiene salida por el mismo enlace, aunque no vayan dirigidas a los mismos destinatarios.

Podemos decir que la tecnología ATM basa la mayor parte de su rendimiento en dos exigencias básicas como son la máxima velocidad de conmutación y la mínima complejidad en los conmutadores.

### 4.3 Transferencias ATM no fiables

Se han mencionado las dificultades de la tecnología ATM para aportar fiabilidad total en sus transferencias. Pero existen diversas propuestas para garantizar en la medida de lo posible el control de errores. De este modo sabemos que el campo HEC de las cabeceras de las células está pensado para detectar los posibles errores sólo en las cabeceras. El campo de datos de las células no tiene control de errores en células independientes pero, sin embargo, se dispone del campo CRC-32 en las PDU de AAL-5 para la detección de errores en una unidad de transferencia de tamaño mayor que las células.
FEC puede aportar la mayor seguridad posible en cuanto a la aparición de errores se refiere pagando un importante coste en overhead debido al código redundante que introduce.

Sin embargo, hemos partido también de la imposibilidad de disponer de fiabilidad total sin afectar al buen rendimiento de la red. Aunque es factible la detección de errores, tanto en cabeceras como en datos, lo que no podemos garantizar es que las células encargadas de las retransmisiones puedan perderse en la red por congestión en los conmutadores o

por fallos de conmutación provocados por errores en las cabeceras de esas células. De este modo, la red asume que pueden producirse pérdidas, de forma que la resolución de las mismas quedan delegadas en protocolos de capas superiores.

### 4.4 Números de secuencia inexistentes

La mayor parte de protocolos de comunicaciones de las capas de Enlace y de Transporte se enfrentan a los problemas de control de flujo y de errores contando con la posibilidad de identificar los paquetes que procesan mediante un identificador que es el que emplean para la detección de paquetes perdidos (cuando falla la secuencia) y para la solicitud de retransmisiones (generalmente extremo-extremo). Sin embargo, la tecnología ATM no dispone de números de secuencia ni en las células (para evitar el overhead), ni en unidades de transferencia mayores de la capa AAL (como pueden ser las PDU de AAL-5). Esta ausencia de números de secuencia en células y PDU impide la identificación de las unidades de transferencia que se pierden cuando la red experimenta congestiones. Esto obliga a que la detección de datos perdidos sea delegada a los protocolos de capas superiores que, como sabemos, repercute en la eficiencia de la red por la necesidad de realizar las retransmisiones extremo-extremo.

### 4.5 Retransmisiones extremo-extremo

Para implementar NACK usamos células estándares Resource Management (RM) propuestas para la clase de servicio ABR (Available Bit Rate), pero sin frecuencia fija[2] y generadas sólo cuando se congestiona un conmutador AcTMs. De este modo evitamos el efecto negativo de las sobrecargas de la red debidas a que un número fijo de células RM desaprovecharían el ancho de banda innecesariamente.

### 4.6 Implosión en las fuentes de tráfico

Los protocolos de transporte de alta velocidad para aplicaciones multimedia multipunto imponen nuevos cambios incluyendo el soporte para aplicaciones de medio continuo y soporte escalable para un gran número de participantes. El control de errores en los protocolos multicast actuales no escala bien debido a la sincronización de los mensajes de realimentación, ya sean debidos a ACK o a NACK desde los receptores del tráfico. Estos dos requerimientos tienen un importante impacto sobre los mecanismos de control de errores, los cuales no soportan actualmente recuperación de retardo-limitado y no

[2] ABR genera una célula RM cada 32 células de datos o cada 100 ms.

pueden controlar la implosión. La implosión[3] es causada en los receptores por la sincronización de los mensajes de realimentación desde los receptores en las conexiones multipunto.

El fenómeno de la implosión es un importante aspecto en comunicaciones escalables multicast. Este problema adquiere importancia en el control de congestión multipunto o en el transporte fiable. Debido a que los recursos son compartidos en el árbol multicast, las pérdidas experimentadas por diversos receptores tienden a estar fuertemente correlacionadas, dirigidas a una implosión de mensajes de solicitud de retransmisión hacia el emisor del tráfico. Este fenómeno puede ser evitado retardando los NACK hacia el emisor.

En las conexiones multipunto, el control de la implosión puede ser realizado por los receptores o por el emisor. En el primero de los casos los receptores colaboran para controlar la implosión y en la segunda es el emisor el responsable de controlar directamente la información de realimentación que proviene de los receptores. La implosión controlada por los emisores es apropiada para redes orientadas a la conexión donde los receptores son aislados unos de otros y no pueden colaborar (por ejemplo, como en una conexión bidireccional punto-multipunto).

### 4.7 Fragmentación de las PDU

Uno de los efectos colaterales provocados por la congestión de los conmutadores es la fragmentación de las PDU que han experimentado congestión. Por tanto, además de la pérdida de células pertenecientes a una misma PDU (que acabarán dando como resultado una PDU corrompida en el destinatario cuando sea aplicado el CRC de AAL-5), se produce la sobrecarga innecesaria de la red con los fragmentos de esas PDU que podrían haberse descartado completas en cuanto se detecte la congestión. Como sabemos, este es uno de los objetivos de varios algoritmos entre los que destaca EPD.

Los mecanismos de control de la fragmentación de paquetes se basan en aplicar una correcta política en los umbrales del buffer de los conmutadores. De este modo, ante la inminencia de una congestión lo que se hace es rechazar la entrada completa de una PDU ante el riesgo que ésta sea aceptada en parte y se envíen al siguiente conmutador algunas de sus células, pero otra parte de las mismas no tengan cabida en el buffer y

[3] Implosión: (De explosión, con cambio de prefijo) .f. Acción de romperse hacia dentro con estruendo de las paredes de una cavidad en cuyo interior existe una presión inferior a la que hay fuera.

sean descartadas generando así una PDU fragmentada. Podemos entender de forma clara que la fragmentación afecta muy negativamente al rendimiento de la red, que se ve obligada a transferir células innecesariamente cuando podrían ser descartadas, y por otro lado, se requerirá la retransmisión extremo-extremo de las PDU que han llegado fragmentadas. Se pierde por tanto ancho de banda de la red y también tiempo de proceso, ya que las pérdidas pueden ser solventadas antes de lo que se está haciendo actualmente.

### 4.8 Interleaving de células en los puertos de salida

Otro efecto pernicioso que se produce en las redes ATM actuales es el del interleaving. La mezcla de las células pertenecientes a diversas conexiones en los puertos de salida de los conmutadores afecta directamente al buen comportamiento de la red.

Existen diversas técnicas para evitar esta mezcla, y el VC Merge es una de las más adecuadas de las propuestas existentes. VC Merge se caracteriza por evitar el interleaving aplicando un mecanismo de asignación de valores de VCI iguales a los flujos que van a ser multiplexados por un enlace común.

# CAPÍTULO V
# FIABILIDAD Y GARANTÍA DE LOS SERVICIOS

## 5.1 Introducción

En los sistemas de comunicación se considera que un bit es erróneo cuando llega a su destino con un valor distinto del que tenía al ser transmitido. Según esto, se expresa el parámetro BER (Bit Error Rate) como el ratio entre los bits erróneos y los bits transmitidos en un espacio de tiempo representativo, y se considera como el parámetro más importante para caracterizar las imperfecciones en los sistemas de comunicación digitales. Como los bits son agrupados para su transmisión en paquetes (células en el caso ATM) pueden provocarse grupos de errores por pérdidas de paquetes o por un enrutamiento incorrecto de éstos. En los sistemas de transmisión suelen producirse errores de bits individuales, mientras en los sistemas de conmutación y multiplexación los errores pueden ser de bits y/o paquetes.

La tecnología ATM se caracteriza por su excelente comportamiento ante diversos tipos de tráfico y por ofrecer la posibilidad de negociar los parámetros generales de QoS como el throughput, delay, jitter y la reliability. Como hemos visto, la unidad básica de conmutación y multiplexación en las redes ATM es la célula de tamaño fijo de 53 bytes. Sabemos que la cabecera tiene, entre otros campos, el HEC (Header Error Control) de 8 bits, usado como CRC (Cyclic Redundancy Code) únicamente para el control de errores de cabeceras. La tecnología no dispone de ningún mecanismo de control de errores para el campo de datos de las células unitarias, aunque sí existen propuestas de aplicación de CRC para células agrupadas en paquetes o PDU (Protocol Data Unit) que son la unidad de procesamiento de la capa AAL. Es importante destacar que en ATM el control de errores se realiza extremo-extremo por los terminales de la comunicación, lo que afecta negativamente al rendimiento de la red de muy diversas formas como que, por ejemplo, la pérdida de una única célula provoca errores de reensamblado de CRC en la capa AAL-5, lo que requiere la retransmisión extremo-extremo de una PDU completa.

Las redes ATM pueden experimentar tres tipos de errores: bits erróneos que corrompen una porción de datos de una célula; errores de conmutación debidos a errores no

detectados en las cabeceras de las células y bits perdidos debidos a congestiones. Las investigaciones realizadas demuestran que en ATM las pérdidas por congestión son la forma predominante de errores dado que los elevados márgenes de fiabilidad aportados por la fibra óptica como medio de transmisión principal (probabilidades de error entre $10^{-8}$ y $10^{-12}$) evitan la aparición de los otros dos tipos de errores citados. Los errores debidos a bits erróneos son menos frecuentes y -en bastantes casos- menos importantes, ya que muchas aplicaciones de tiempo real prefieren perder células antes que soportar el retardo provocado por la retransmisión de células erróneas o congestionadas.

En el caso de los errores de conmutación y/o multiplexación los paquetes erróneos son causados por errores en las cabeceras que provocan errores de interpretación o de enrutamiento y acaban provocando la pérdida de los paquetes o su llegada a un destino equivocado. El propio dispositivo de conmutación o multiplexación también puede desechar células ATM por agotamiento de sus recursos cuando muchas células compiten por ellos, lo que acaba generando también errores. La unidad de pérdida es la célula ATM, y éstas pueden ocurrir a ráfagas afectando a varias células consecutivas en una misma conexión.

La teoría de codificación de información distingue entre dos tipos de corrupción de datos: un error se define como un bit con valor desconocido en una posición desconocida; y una borradura (erasure) es un bit con un valor desconocido en una posición conocida. Con este planteamiento, es destacable que los métodos de codificación aspiran a convertir o reemplazar los errores por erasure que son más fácilmente tratables, con lo que aumenta la eficiencia de los códigos correctores como FEC (Forward Error Correction).

En muchos casos suele recurrirse a protocolos de la capa de transporte extremo-extremo para incrementar la fiabilidad mediante retransmisiones o usando códigos generadores de información redundante. Tres técnicas básicas para ofrecer fiabilidad son: Automatic Repeat Request ARQ, Forward Error Correction FEC y también mecanismos híbridos de ARQ combinados con FEC.

Describiremos las diferencias entre el parámetro de QoS, fiabilidad y el de Garantía de Servicio.

## 5.2 Fiabilidad y Garantía de Servicio

En comunicaciones el concepto fiabilidad está claramente aceptado como la forma de aportar a las conexiones extremo-extremo garantía plena de que la información que transfieren llega sin ningún error o, si aparecen errores, todos pueden ser detectados y corregidos. Aplicar a una red, a un protocolo, o a una tecnología de comunicaciones el calificativo de fiable implica que ésta puede aportar la garantía de transferencias libres de errores. Para conseguir la fiabilidad total existen dos posibilidades: una consistente en aplicar un mecanismo de control en el que todos los tipos de datos transferidos son confirmados por el destino, con la intención de garantizar que no se pierde ni una sola unidad de transferencia; y la otra consistente en añadir información redundante a los paquetes de información que garantice a los receptores que esos paquetes no han sufrido ninguna variación en la red. En realidad, la fiabilidad se consigue uniendo estas dos técnicas, ya que la primera garantiza que no hay pérdidas de datos, y la segunda que los datos son correctos. Cuando se detectan pérdidas y/o errores se recurre a la retransmisión extremo-extremo entre el emisor y el receptor. Podemos ver cómo el concepto de fiabilidad no se enfrenta directamente a los problemas provocados por las congestiones, aunque veremos más adelante cómo existen pesadas técnicas de confirmación que pueden ser usadas para detectar las congestiones, aunque sea a costa de pérdida del goodput[4] en la red.

Aparece la idea de transmisiones garantizadas, lo que introduce el concepto de Garantía de Servicio (que identificamos en lo sucesivo como GoS) a las transferencias que se estime que así lo necesitan. GoS es en realidad un nuevo parámetro de QoS que se deriva directamente del parámetro de fiabilidad.

## 5.3 Códigos de redundancia cíclica (CRC)

Las redes ATM, como otras tecnologías, están sometidas a la aparición de errores, tanto aislados como a ráfagas. Son ya conocidos los diversos mecanismos que pueden usarse para enfrentarse a los errores producidos en los medios de transmisión, y todos ellos se basan en la estrategia de incluir más o menos código redundante en la información que se desea transferir. Cuanto mayor fiabilidad se desea aportar a las transmisiones, más información redundante habrá que añadir a los datos originales. Así, se pueden usar códigos redundantes para la detección de errores y códigos redundantes para la corrección de esos errores.

---

[4] El concepto goodput expresa el rendimiento de la red considerando no sólo la capacidad de transferencia (throughput), sino también el efecto generado por las retransmisiones.

Para los primeros se usan los conocidos códigos de Hamming, mientras para los segundos se emplean los, también conocidos, códigos polinómicos o Códigos de Redundancia Cíclica (CRC).

### 5.4 CRC aplicados a cabeceras de células ATM

En el caso de ATM se han realizado investigaciones en el campo de los CRC para garantizar la corrección, tanto de las cabeceras, como de los campos de datos de las células ATM. Así, como se vio oportunamente, la cabecera de las células aporta el campo HEC que realiza la comprobación de corrección de cada uno de los bits de la cabecera, pero no realiza ninguna verificación de los bits del campo de carga útil de las células. El campo HEC tiene una longitud de 8 bits (para aportar fiabilidad a los 32 bits restantes de las cabeceras) con el que se puede conseguir un código redundante suficientemente potente para detectar y corregir todos los errores de un solo bit, y también es capaz de detectar el 90% de los errores de más de un bit.

El polinomio generador de grado 8 usado en el CRC es $x^8 + x^2 + x + 1$, que es más que suficiente para considerar fiables las cabeceras ATM, y máximo cuando se conoce que en la fibra óptica, que es su principal medio físico de transmisión, los estudios realizados demuestran que el 99,64% de los errores son de un solo bit. Sabemos además que la probabilidad de que se produzca un error en un bit enviado a través de fibra es hoy inferior a $10^{-12}$. Por tanto, la probabilidad de que aparezca un error de más de un bit está en torno a $10^{-15}$.

A la vista de estos números podemos asumir que, aunque la fiabilidad no es absoluta, puede decirse que la probabilidad de recibir células con cabeceras erróneas es prácticamente nula.

Mención a parte merece el caso del campo de datos de las células que, como hemos comentado, no es considerado por el campo HEC al aplicar el código polinómico. Esto es así porque poder garantizar también los 48 bytes del campo de datos de la célula requeriría de un campo HEC superior a 8 bits, lo que supondría usar un octeto más en las cabeceras que pasarían a 6 octetos y uno menos en el campo de datos que quedarían con 47 octetos. La solución podría consistir también en replantear el tamaño total de las células de 53 octetos, pero es conocido el esfuerzo que costó encontrar el consenso hasta llegar a este peculiar tamaño de células.

En lugar de esto lo que propone la tecnología ATM es el uso de CRC aplicado sobre paquetes de células que engloban también a los campos de datos. Esta labor se realiza en la capa AAL como vamos a comprobar a continuación.

### 5.5 CRC aplicados a paquetes de células

Aunque la célula es la unidad de conmutación, multiplexación y transferencia dentro de la red ATM, las aplicaciones pueden usar unidades de transmisión de mayor tamaño y propias de los protocolos de las capas superiores que están sobre la capa AAL. Es sabido que existen varios protocolos en la capa AAL, pensados inicialmente para cada una de las CoS. Estos protocolos son AAL-1, AAL-2, AAL-3/4 y AAL-5. Pues bien, sin entrar en excesivas consideraciones, en este caso nos interesa destacar que, de un modo u otro, las cuatro variantes de AAL aportan un mecanismo de comprobación para aportar fiabilidad a los paquetes de datos que transfieren. Mientras AAL-1 emplea un número de secuencia que hace las veces de suma de comprobación, las otras tres emplean CRCs para garantizar que la información no experimenta errores.

Desde el punto de vista de un emisor, la capa AAL-5 pasa información a la capa ATM en forma de ATM-SDU (Service Data Unit) de 48 octetos. Desde el punto de vista del receptor la capa AAL-5 recibe de la capa ATM unidades en forma de ATM-SDU de 48 octetos. En líneas generales, lo que hace el protocolo AAL-5 es tomar secuencias de mensajes del nodo emisor provenientes de los protocolos superiores y aplicar la segmentación a los paquetes de información para conseguir una secuencia de células de 48 octetos, a las que la capa ATM se encargará de añadir la cabecera para poder ponerlas en la red. Para realizar estas funciones el protocolo que reside en la capa AAL-5 emplea una serie de primitivas y usa un conjunto de servicios que están definidos en la Rec. I.363.5.

AAL-5 está dividida en dos sub-capas, la sub-capa SAR (Segmentation and Reassembly) y encima de ésta, la sub-capa CPCS (Common Part Convergence Sublayer). Existe una tercera sub-capa que puede ser nula y estar sobre CPCS, que se llama SSCS (Service Specific Convergence Sublayer). Cada una de ellas dispone de sus propias funciones, primitivas y servicios. Nosotros nos hemos fijado en la CPCS para comprobar las posibilidades de fiabilidad y de GoS de esta capa. La Figura 5.1 muestra el formato de las PDU (Protocol Data Unit) que es la unidad de transferencia en la sub-capa de convergencia de la parte común de AAL5.

Como podemos observar, las PDU constan de dos partes bien diferenciadas con un campo de datos y una cola.

El campo de datos es de tamaño variable y puede contener de 1 a 65.535 octetos de información.

Para que el campo de datos contenga siempre un número exacto de unidades de células y, por tanto sea múltiplo de 48, se emplea un campo de relleno o padding que puede tener de 0 a 47 octetos.

Por su parte, la cola de la CPCS-PDU cuenta con 8 octetos divididos en los siguientes campos:

El campo CPCS-UU (User to User), de 1 octeto, se emplea para transferir información transparente entre usuarios de la sub-capa CPCS. Este campo en realidad no es usado por la capa AAL y está a disposición de capas superiores como luego veremos.

El campo CPI (Indicador de Parte Común), de 1 octeto, se usa para que las colas de PDU queden alineadas o ajustadas a su tamaño total fijo de 64 bits. En realidad este campo, como el anterior, puede ser usado libremente por los protocolos de capas superiores pues el estándar no le ha encomendado funciones específicas.

El campo Longitud, de 2 octetos, expresa en binario el tamaño real del campo de datos que, como hemos dicho antes, es de tamaño variable. Por tanto, este campo nos permite delimitar el tamaño real de cada PDU. También es usado por los nodos receptores para determinar si una PDU ha experimentado algún tipo de pérdida o ganancia de información. Es decir, sirve también para detectar errores.

El campo CRC, de 4 octetos, es el que realmente se encarga de ofrecer la fiabilidad a todos los bits de la PDU. Este campo se rellena con el resultado de aplicar un CRC de 32 bits y su correspondiente polinomio generador de grado 31 a todo el campo de datos, al relleno y a los primeros 4 octetos de la cola de las PDU. Este último campo es el que acaba aportando la fiabilidad a las PDU individuales y, por tanto, a los campos de datos de las células ATM que no son protegidos por el CRC HEC de las cabeceras de las células.

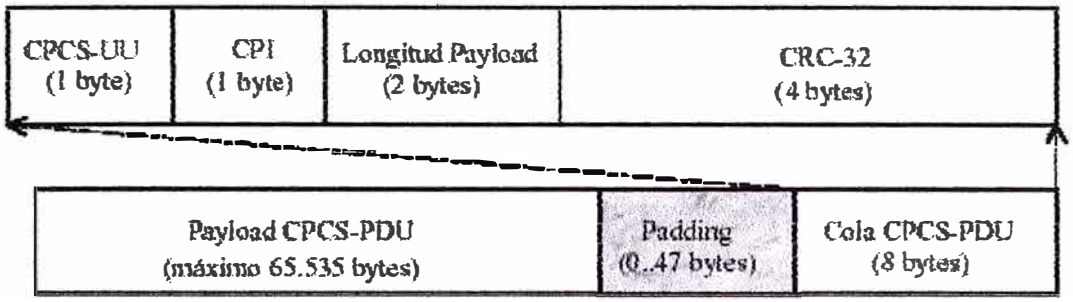


Figura 5.1. Formato de las PDUs de CPCS de AAL-5

Hemos podido comprobar cómo, de un modo u otro, tanto las cabeceras como los campos de datos pueden ser protegidos de los inesperados problemas que la red pueda experimentar. Nos encontramos con que el precio que hay que pagar por esta seguridad es de 8 bits para cada una de las células individuales, y de 32 bits en el caso de cada una de las PDU. Este precio se paga por tanto en forma del overhead que hay que introducir para enviar el código redundante en cada unidad de transferencia, ya sean células o PDU. Pero otro problema añadido es que los errores son sólo solventables extremo-extremo. Tanto el throughput como el goodput se ven afectados para poder disponer de la fiabilidad aportada por HEC y FEC.

### 5.6 Automatic Repeat Request (ARQ)

ARQ es una técnica de bucle cerrado basada en la retransmisión de datos que no han sido recibidos correctamente debido a los problemas que ya hemos comentado en los puntos anteriores. En realidad, las técnicas ARQ se usan conjuntamente con los CRC ya que, cuando un CRC detecta un error que no es capaz de solventar, necesitará de un mecanismo de solicitud de retransmisión de la trama errónea desde el emisor.

ARQ será la técnica que usaremos para notificar al emisor de las retransmisiones que debe realizar.

En el caso de aplicaciones de tiempo no real la retransmisión de información incorrecta o perdida se puede confiar a técnicas ARQ que se han demostrado como poco apropiadas para servicios de tiempo real o con requerimientos de baja latencia por el elevado retardo que introducen las retransmisiones. ARQ ofrece dos variantes y ambas requieren que emisor y receptor intercambien algún tipo de información de estado por lo que incurren en

retardos para el nodo receptor, implosión[5] en el nodo emisor y excesivo overhead en la red.

En la primera variante de ARQ el receptor devuelve mensajes de confirmación positiva (ACK+) incluso cuando ha recibido correctamente los datos. Este es el mecanismo tradicionalmente usado para aportar fiabilidad en las transmisiones unicast. Para poder implementar este protocolo es necesario que las tramas que va a procesar tengan un número de secuencia que sirva para identificarlas en la recepción y en el proceso de retransmisión. Este planteamiento responde claramente al modelo de protocolos de la capa de enlace (también de transporte) orientados a conexión y con acuse de recibo que ofrecen fiabilidad a la capa de red. El carácter orientado a conexión elimina, incluso, la posibilidad de tramas repetidas que, en el caso de ser no orientado a conexión, pueden aparecer en los time-out de los ACK. En el caso de ATM este es un protocolo que puede aportar fiabilidad, pero nos encontramos con tres grandes inconvenientes: el primero -solventable- es el de la no existencia de números de secuencia en las células ATM que impide la posibilidad de retransmisión de células concretas; el segundo -más grave- el de la elevada latencia y degeneración del goodput provocados por tener que confirmar desde el receptor la llegada de cada célula del emisor; y el tercero -inabordable en multicast- el problema de implosión que provoca que los emisores se vean inundados con los acuses de recibo de los receptores. Parece claro que este protocolo de confirmación positiva está pensado para unidades de transferencia mucho más grandes que el tamaño de una célula y que además dispongan de un mecanismo de numeración que permita establecer la secuencia de llegadas y detectar las pérdidas cuando se altera la secuencia.

En la segunda variante de ARQ el receptor devuelve mensajes de acuse de recibo negativos (NACK) sólo cuando se han producido errores o pérdidas de datos. Es claro que este mecanismo de detección y recuperación de errores solventa o aminora el segundo y tercer problemas comentados en NACK+. En este caso no se sobrecarga al emisor ni a la red con acuses de recibo innecesarios, ya que sólo se generarán cuando el receptor detecta problemas y solicita la retransmisión de la trama perdida o errónea. Desde luego, para poder implementarlo es necesario que las tramas dispongan de un número de secuencia que sirva de referencia para las retransmisiones. Por otro lado, la técnica NACK aporta menor fiabilidad cuando las peticiones de retransmisión se pierden.

[5] La implosión es el efecto negativo que experimentan las fuentes emisoras de tráfico cuando deben atender las solicitudes de retransmisión de células perdidas o erróneas. En el caso de las transferencias multipunto la implosión genera importantes problemas.

Además de las intuitivas ventajas a favor de NACK, ACK+ es no escalable en el caso de protocolos multicast ya que a medida que va creciendo el número de receptores el funcionamiento se va degradando. Debemos destacar, no obstante, que exitosos protocolos p-p como TCP, HDLC y TP4 y otros tantos multicast/broadcast usan el planteamiento ACK+ para conseguir la fiabilidad.

### 5.7 Forward Error Correction (FEC)

FEC es una interesante alternativa a las dos variantes de ARQ pues ofrece fiabilidad sin incrementar la latencia extremo-extremo. Su principio de funcionamiento se basa en la codificación de paquetes en el emisor con información redundante junto con los datos, de forma que sea posible reconstruir los paquetes originales en el receptor, reduciendo, o incluso eliminando, las retransmisiones y el negativo efecto de la implosión sobre los emisores. Para que el método sea eficiente, el tamaño de la información redundante debe ser menor que los datos de información que se desea hacer fiables. FEC consiste en el uso de esquemas de codificación compleja que añaden redundancia a nivel de bit. Los códigos aportan distinta capacidad de corrección de errores según la redundancia que se añada. Algunos ejemplos de estos códigos son Hamming, Golay y BCH.

FEC permite la recuperación sin necesidad de retransmisiones, y su uso tiene sentido cuando las aplicaciones sean sensibles a los retardos que puedan provocar las retransmisiones. Este método tiene un buen comportamiento cuando las pérdidas son dispersas en el tiempo. Una evaluación del comportamiento de FEC (tanto en fuentes FEC como en las que no lo son) con tres modelos de tráfico distinto, demuestra que, mientras para los modelos de tráfico homogéneo FEC no es efectivo, en el caso de las fuentes de vídeo (tráfico heterogéneo de vídeo o tráfico a ráfagas) FEC reduce las pérdidas en varios órdenes de magnitud. A cambio, debe incrementarse el tráfico en la red en una magnitud del orden del número de células redundantes generadas por el código FEC[6].

En cuanto a las necesidades de buffers de almacenamiento en los codificadores y decodificadores, hay que citar que pueden ser las mismas, tanto con FEC como sin el. En el caso del buffer de los receptores depende del método que se emplee, ya que si se usa reensamblado de células en grandes unidades, deberá aportarse un buffer de

[6] Destacar que FEC es capaz de doblar su potencia como código corrector reemplazando errores por erasures que, como sabemos, tienen el error en una posición conocida.

reensamblado que sea suficientemente grande como para mantener ese bloque de células. En cambio, si el nodo receptor opera en modo cut-through, y cada célula contiene suficiente información de cabecera para determinar su posición, una célula de entrada podrá ser colocada en la aplicación del nodo receptor sin necesidad de buffers intermedios para la decodificación.

RSE (código Reed-Solomon basado en código corrector de ráfagas de erasures) es un conocido sistema FEC que, partiendo de d células de datos como entrada, genera r células redundantes, dando como salida d+r células según muestra la Figura 5.2.

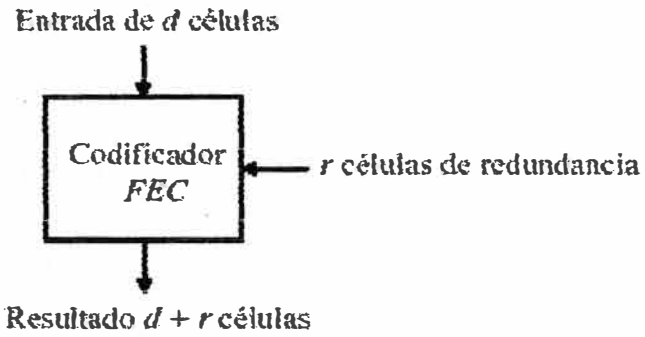


Figura 5.2. Funcionamiento FEC

El total de las d+r células son transmitidas al receptor que sólo necesitará decodificarlas si se reciben menos de las d células de datos originales. Sólo d, de las d+r células, son suficientes para recuperar las d células ATM iniciales. En ATM la unidad de detección de error y de recuperación de pérdidas es el bloque, que se define como un grupo de d células a partir de las cuáles se generan las r células redundantes. Un bloque de d+r células se pierde cuando se pierden más de r de las d+r células.

RSE es capaz de corregir erasures pero no errores. A cambio, su algoritmo es más sencillo y puede emplearse el mismo hardware en el codificador y en el decodificador. También trata las células de datos como texto plano sin ningún tipo de modificación, por lo que no es necesario esperar a que acabe todo el proceso de codificación para iniciar su transmisión, por lo que la decodificación es más rápida, al contrario que otros códigos que se encargan de cifrar los datos, aportando a éstos mayor seguridad. RSE puede ser implementado en un solo circuito y alcanzar throughputs entre 400 Mbps y 1 Gbps en función del tamaño de símbolo que se emplee. Usar símbolos de mayor tamaño (16 ó 32 bits en lugar de 8) supone alcanzar tiempos de codificación mucho menores, lo que afecta positivamente a la eficiencia de RSE.

Aunque existen distintas propuestas sobre el lugar de los árboles de distribución multicast en los que se debe aplicar la técnica FEC, lo que sí está demostrado es que este mecanismo decrementa la pérdida de paquetes en los árboles y, por tanto, también decrementa o amortigua el efecto negativo de la implosión en los emisores que es el mayor inconveniente para obtener la fiabilidad en las transmisiones multicast.

En grupos pequeños de usuarios se ha empleado FEC parcial, pero la eficacia de este método se aprecia a medida que se incrementa el número de receptores del grupo multicast, o cuando desciende el número de enlaces compartidos.

Diversos estudios realizados demuestran que, cuando se aplica FEC a todos los enlaces de un árbol multicast, se observa lo siguiente:

Para grupos pequeños la mejora de FEC incrementa cuando el número de receptores incrementa y el número de enlaces compartidos decrece.

Para grupos grandes la mejora de FEC es mayor que para grupos pequeños y es independiente del número de receptores.

Cuando FEC se aplica a cualquiera de los enlaces del árbol multicast de una LAN o WAN se obtienen los siguientes resultados:

Para grupos pequeños la mayor mejora de FEC se consigue cuando se aplica en la parte donde los enlaces tienen mayor probabilidad de pérdidas.

Para grupos grandes esto sólo es cierto con un número bajo de receptores de la LAN. Si el número de receptores de la LAN es grande, FEC debería aplicarse a los enlaces de la LAN.

Minimizando el grado de solapamiento entre los paths de un árbol multicast se obtendrá un servicio multicast más fiable.

Las comunicaciones multicast fiables son el área donde FEC puede ser más beneficioso que ARQ ya que éste escala mal cuando crece el número de receptores por los siguientes motivos:

El emisor debe cargar con la respuesta de un gran número de ACK o NACK provenientes desde los receptores (fenómeno de la implosión de los ACK).

Como el número de receptores crece, la probabilidad de pérdidas entre distintos receptores deja de estar relacionada entre sí, lo que causa que, si no todos, al

menos una gran mayoría de los paquetes deba ser retransmitido con gran impacto en el rendimiento de las comunicaciones.

Aunque FEC suele implementarse mediante técnicas hardware usando codificadores y decodificadores, también es implementable mediante software sin pagar demasiado overhead. En el caso de IP, se emplean incluso técnicas de separación de canales apartando por uno de ellos las retransmisiones de datos con un servidor dedicado a esas retransmisiones y, por otro, la escucha de receptores que tienen pérdidas.

Hace ya algún tiempo que se intentaron aprovechar los beneficios de la recuperación de errores FEC en las redes ATM. Sin embargo, parece que se ha prestado escasa atención a estas investigaciones. Las propuestas estándares de ITU-T distinguen entre AAL-1 y AAL-5 como las capas adecuadas donde aplicar las técnicas FEC para la recuperación de errores. Tanto AAL-1 como AAL-5 emplean SSCS con FEC como control de errores para servicios en tiempo real. A continuación se va a describir brevemente la propuesta AAL-5.

## 5.8 FEC aplicado a AAL-5

Las investigaciones para incluir técnicas FEC en AAL-5 proponen una capa FEC-SSCS (FEC Service Specific Convergence Sublayer) situada en la parte superior de AAL-5 y/o AAL-3/4, justo encima de la capa CPCS (Common Part Convergence Sublayer), tanto en emisores como receptores con la intención de obtener un rendimiento más elevado con menor latencia y mayor fiabilidad en la entrega de datos extremo-extremo.

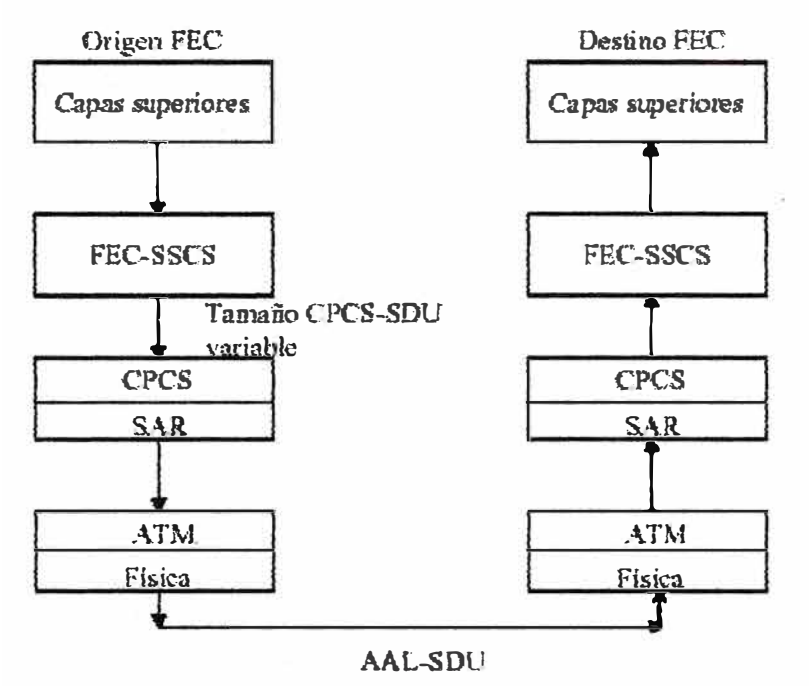


Figura 5.3. Protocolo FEC-SSCS

Según muestra la Figura 5.3, cuando la entidad CPCS destino detecta un error (bit erróneo y/o célula perdida) al recibir una AAL-SDU, la entidad FEC-SSCS intenta recuperar el dato original enviado desde la CPCS fuente usando el algoritmo FEC.

La propuesta distingue tres modos de operación relacionados con los tres tipos de errores distintos que es capaz de recuperar:

SEC (Symbol Error Correction): Sólo recupera bits erróneos en los símbolos (unidades de datos definidas por el algoritmo FEC, típicamente de 8 ó 16 bits). La desaparición de símbolos o células no es tratada.

SLC (Symbol Loss Correction): Sólo recupera símbolos que han desaparecido por pérdidas de células. No se recuperan bits erróneos.

SEAL (Symbol Error And Loss correction): Recupera bits erróneos en los símbolos, y detecta la ausencia de símbolos porque la red haya tirado células.

Cada uno de estos modos de operación puede ser elegido por la aplicación de la capa superior que, como puede observarse en el modelo de referencia del protocolo, cuenta con las primitivas necesarias entre cada una de las capas. Los tres modos de operación ofrecen servicios como: indicación de pérdida de células; indicación de bit erróneo; negociación de los parámetros del algoritmo de FEC; ajuste de la longitud de los datos redundantes que se están enviando; tamaño variable de CPCS-SDU y uso de técnicas pipeline en las fuentes FEC-SSCS al transferir las FEC-SSCS-PDU.

## 5.9 FEC-SSCS en modo ATM Nativo

Las propuestas estándares, tanto ITU-T como ATM-Forum, distinguen entre diferentes métodos de corrección de errores, sin embargo, ninguna de ellas procesa directamente células ATM nativas de 53 octetos, incurriendo en la ineficiencia que supone el tener que gestionar PDUs y arrastrar, en algunos casos, importantes overheads que pueden hacer del método FEC ineficiente en algunos casos.

Por ejemplo el método de corrección de errores en los bits para AAL-1 emplea en la CS emisora códigos de Reed-Solomon de 4 octetos que se añaden a los 124 octetos de datos que entran provenientes de la capa superior. El método es capaz de corregir dos octetos con errores en cada trama FEC de 128 octetos, e incurre en un overhead del 3,1 % y un retardo en el receptor de aproximadamente 3 células. En la CS emisora cada PDU es un bloque FEC formado por 47 tramas FEC de 128 octetos cada una.

En el método de corrección de errores en bits y pérdidas de células, los bloques de 128 (124 de datos + 4 de FEC) octetos resultantes se envían al entrelazador de octetos para generar la matriz de entrelazado que está formada por 47 líneas de 128 columnas cada una. Cada línea equivale a una SAR-PDU y la matriz completa es una CS-PDU.

El tercer método de corrección tampoco gestiona células ATM nativas, lo que acaba generando PDU que es necesario adaptar en las capas AAL-5 y acaban provocando el overhead que podría evitarse trabajando en modo ATM nativo.

Del mismo modo, la propuesta del draft del ATM-Forum para AAL-5 tampoco se centra en la obtención de PDU cercanas a los tamaños de células ATM nativas que eviten el desaprovechamiento del throughput.

## 5.10 Técnicas híbridas FEC Y ARQ

Tradicionalmente, la mayoría de investigaciones en materia de protocolos multicast fiables se han centrado en la recuperación de errores mediante técnicas ARQ. Sin embargo, el inconveniente de este método es su escasa escalabilidad cuando el número de componentes del grupo multicast empieza a crecer. Para solventar este inconveniente se han propuesto en la literatura diversas técnicas para aportar a ARQ la escalabilidad que le falta, entre ellas las dos siguientes: establecimiento de asincronía entre receptores con la intención de evitar la implosión y, por otro lado, la aplicación de jerarquías a los

árboles de distribución multicast. No obstante, la falta de escalabilidad hace que ARQ sea usado en protocolos unicast y se ha propuesto FEC para incrementar la fiabilidad en las comunicaciones multipunto.

Partiendo de la premisa de la imposibilidad de conseguir la fiabilidad total, hay que destacar que, en comunicaciones punto-a-punto, se ha logrado haciendo que el receptor envíe mensajes ACK positivos al emisor. Para los paquetes de datos recibidos se emplea confirmación positiva y confirmación negativa para los paquetes perdidos. En ambas situaciones sigue existiendo la implosión que, en el caso del multicast fiable, se evita haciendo que los receptores envíen NACK al emisor cuando se han perdido algunos datos.

ARQ es un mecanismo de control de errores basado en retransmisiones, de utilidad en situaciones donde existan grupos pequeños, en aplicaciones no interactivas, cuando predominan las pérdidas en enlaces compartidos de los árboles multicast, o cuando la probabilidad de pérdidas no es homogénea. FEC, en cambio, es interesante cuando existen grupos grandes, predominan las pérdidas individuales, la probabilidad de pérdidas es homogénea o los buffers son limitados.

Importantes ideas justifican la aplicación de FEC como la técnica apropiada para las transferencias multicast fiables en redes IP. No obstante, muchas de las ideas pueden ser aprovechables para las redes de tecnología ATM.

La aplicación de técnicas correctoras de errores al tráfico multipunto a través de métodos híbridos FECARQ es, sin lugar a dudas, una de las partes más complejas por todas las implicaciones del multipunto. La idea general va en la línea de aplicar FEC entre emisor y receptores pero teniendo en cuenta que en determinados puntos de la red puede tener sentido aplicar ARQ, por ejemplo, cuando no quede otro remedio que retransmitir en los extremos. Hemos analizado este problema y consideramos que si es así se evitaría la implosión hacia arriba en el árbol formando subgrupos para que, cuando un conmutador vecino al que ha detectado el error haya sido capaz de reconstruir un error, no sea necesario retransmitirlo desde el origen. En esta situación hay que considerar los problemas de la heterogeneidad de receptores y de los distintos tramos de red.

En general, podemos considerar el escenario que se muestra en la Figura 5.4, donde se indica que la mayor parte de pérdidas de células se producen en las troncales de las

redes y no en los nodos extremos de la comunicación. Para amortiguar las pérdidas se puede usar FEC, pero cuando se detecten pérdidas en los receptores emplearíamos NACK para avisar al conmutador correspondiente, que se encargará de las retransmisiones lo más locales posibles. Para evitar la implosión en el emisor, propondríamos la existencia de buffers en los conmutadores que permitan que entre conmutadores vecinos puedan realizarse las retransmisiones (mediante NACK) sin necesidad de afectar al emisor hasta que no sea necesario.

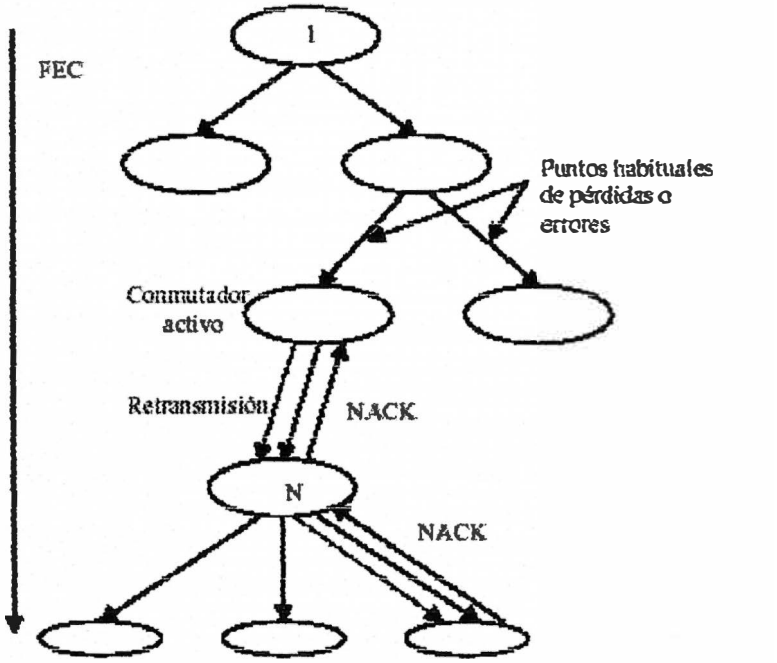


Figura 5.4. FEC-NACK híbrido en multicast

## CONCLUSIONES

1. Las celdas ATM aportan un mecanismo de control de errores basado en el campo HEC. Sin embargo, los errores producidos en las transferencias a través de la red no son el principal problema que pueden experimentar las células. Un problema más grave, y menos predecible, es el de la congestión provocada en los conmutadores cuando se les exige un rendimiento superior al que son capaces de ofrecer. Es decir, los conmutadores pueden experimentar congestiones cuando las fuentes de tráfico no cumplen sus contratos de tráfico y producen, individualmente o de forma conjunta, más células por segundo que las que alguno de los conmutadores intermedios es capaz de procesar.

2. Los circuitos virtuales permanentes ATM complican aún más la asignación de direcciones. Debido a que un administrador configura manualmente cada circuito virtual permanente, un host solo conoce el par de circuitos VPI/VCI. El software en el host no conoce la dirección IP ni la dirección de Hardware ATM del extremo remoto. Un mecanismo de asignación de direcciones IP debe proporcionar la identificación de una computadora remota conectada a un PVC así como la creación dinámica de SVC para destinos conocidos.

3. Si la red ATM va a ser únicamente una red IP, entonces Classical IP over ATM, es una de las opciones. Por el contrario, si existen otros protocolos adicionales a IP, entonces LAN Emulation sería la opción.

## BIBLIOGRAFÍA


1. Routing LAN Protocols – Información Cisco.
2. Andrew Tanenbaum "Redes de Computadoras" Ed. Prentice Hall, 1997.
3. http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html
4. José Luis González Sánchez, Tesis Doctoral "Protocolo Activo Para Transmisiones Garantizadas Sobre una Arquitectura Distribuida y Multiagente en Redes ATM".
5. Anthony Alles "Red ATM", Cisco Systems, Inc.
6. Douglas E. Comer "Redes Globales de Información con Internet y TCP/IP" Ed. Prentice Hall, 1996.