CAPÍTULO 1

INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA A RESOLVER.

El cambio acelerado y dinámico de las Telecomunicaciones hace que los libros de texto, artículos o publicaciones y tecnología utilizada en la educación queden obsoletos en un lapso muy mínimo de tiempo; por lo que nos coloca rápidamente en desventaja con el avance en esta área.

Actualmente la FIME cuenta con infraestructura capaz de dar acceso de Banda Ancha (FDDI) como medios de transporte de información que no es aprovechada en su totalidad por la parte académica como apoyo para el maestro en el área de las Telecomunicaciones.

Por otra parte, debido a la falta de facilidades tecnológicas se dificulta el acceso a bancos de información vía red local o amplia desde un aula de clases.

Es de gran importancia resaltar la necesidad que tiene nuestro plantel de resolver la forma de impartición, utilizando herramientas que nos permitan vincular los conceptos más actualizados y los avances tecnológicos de mayor importancia, ya que es una de las áreas que se encuentra en constante desarrollo.

1.2 OBJETIVO DE LA TESIS.

El principal objetivo es presentar un material por escrito, útil y práctico, que brinde apoyo a los maestros y estudiantes de diversas carreras donde se imparten materias enfocadas a las Telecomunicaciones tanto a nivel Licenciatura como Post-

grado y en especial a la materia de Sistemas de Transmisión de Datos y de la carrera de Ingeniero en Electrónica y Comunicaciones y sobre todo en las materias de nueva creación contempladas en la propuesta de la reforma curricular que son Telecomunicaciones Modernas y Sistema de Comunicación de Datos I y II, esto con el fin de que nuestros egresados compitan no solo a un nivel local, sino en el ámbito nacional e internacional

1.3 HIPÓTESIS.

H_1.- Considero que la deficiencia de la preparación en esta área es debida, en parte, a la escasa bibliografía actualizada que existe y además de que la información se encuentra muy dispersa, esto aunado al rápido cambio de tecnología convierte en una odisea la constante actualización.

H_2.- La incursión en este texto de algunas aplicaciones y otros propuestos permitirá el máximo aprovechamiento hora-estudio del alumno y aumentará el potencial de desarrollo en el área de las Telecomunicaciones.

1.4 LÍMITES DEL ESTUDIO.

Esta es una investigación que se enfoca desde los conceptos básicos hasta sistemas actuales que utilizan la transmisión de información (voz, datos y vídeo) de manera local y remota, así como la aplicación de la red INTERNET como herramienta de trabajo.

El estudio esta enfocado a los equipos que se utilizan en la actualidad y que pueden ser aplicados en la docencia y no en la investigación de nuevas tecnologías aplicadas al mismo propósito aunque se hace una visión a futuro

1.5 JUSTIFICACIÓN DEL TRABAJO DE TESIS.

La Transmisión de Información (voz, datos y video) en estos tiempos, es fundamental para el desarrollo de las actividades educativas, productivas, comerciales y económicas de cualquier país. Por ello, se diseñan y se implantan redes de Telecomunicaciones que permiten que la navegación sea segura y eficiente las 24 horas del día y todos los días del año.

Considerando el avance desmesurado de la tecnología en el área de las Telecomunicaciones en el ámbito mundial y consciente de que la Facultad de Ingeniería Mecánica y Eléctrica no puede permanecer al margen he querido participar activamente con esta aportación para apoyar a los programas de clase de la carrera del Ingeniero en Electrónica y Comunicaciones.

1.6 METODOLOGÍA.

- Descripción de los principios básicos de las Telecomunicaciones.
- Investigación de la situación actual de la infraestructura y tecnología.
- Desarrollo de propuestas de mejora.
- Conclusiones y recomendaciones.

1.7 REVISIÓN BIBLIOGRÁFICA.

Esta tesis esta apoyada en investigación en campo tanto en la UANL como en el ITESM así como apoyado por diferente libros de textos, en los cuales destaca Redes de Computadoras de W. Stalling y Redes de Ordenadores A. Tandembaum, literatura especializada tales como Telecommuication, Bussiness Communicatios Review, Data Comunnication, etc. y Web Site sobre este tema que enuncio a continuación, http://www.rad.com/networks/netterms.htm, http://www.cisco.com y http://www.verilink.com.

CAPÍTULO 2

CONCEPTOS GENERALES

2.1 INTRODUCCIÓN.

El vertiginoso avance tecnológico que han experimentado los campos de la electrónica y la computación en los últimos 50 años, permitieron incrementar la capacidad y velocidad de los sistemas de comunicación de datos. Por esta razón se considera importante conocer el desarrollo de las Telecomunicaciones en sus diversas etapas, así como los distintos mecanismos para su interconexión de la información a lo largo y ancho del mundo.

2.2 MODELO DE REFERENCIA OSI.

El modelo OSI surgió frente a la necesidad imperante de interconectar sistemas de procedencia diversa en los que cada fabricante empleaba sus propios protocolos para el intercambio de señales.

Esté modelo fue creado como tal, es decir, que no necesariamente todos los fabricantes tenían que sujetares a él. Pero al hacerse éste un estándar, todo aquel que no fuera compatible o hecho con basé en OSI de alguna manera iba a quedar relegado en el mercado, ya que por ningún motivo el usuario deseaba seguir obligado a vivir con una sola marca, con todas las desventajas que esto representaba.

Existieron gigantes de las Telecomunicaciones que en un principio se opusieron al desarrollo de su tecnología con base en el modelo OSI, pero conforme vieron sus ventajas y desventajas se sujetaron al nuevo estándar.

El modelo de referencia para la interconexión de sistemas abiertos OSI, *(open systems Interconnection),* fue aprobado, por el organismo internacional ISO, *(Internnational Standarsds, Organization),* en 1984, bajo la norma ISO 7498, después de varios años de arduo trabajo.

Este modelo fue desarrollado por la necesidad de interconectar sistemas de distintos fabricantes por lo que fue hecho con base en necesidades generales de todos los sistemas, de tal forma que los fabricantes pudieran apegarse a estas funciones.

El modelo de referencia OSI proporciona una arquitectura de 7 niveles alrededor de los cuales se pueden diseñar protocolos específicos que permitan a diferentes usuarios comunicarse abiertamente. La elección de los 7 niveles se dividió básicamente en los 3 puntos siguientes:

1.- La necesidad de tener suficientes niveles para que cada uno no sea tan complejo en términos del desarrollo de un protocolo detallado con especificaciones correctas y ejecutables.
2.- El deseo de no tener tantos niveles y provocar que la integración y descripción de éstos lleguen a ser demasiado difíciles.
3.- El deseo de seleccionar fronteras naturales, con funciones relacionadas que se recolectan en un nivel y funciones muy separadas en diversos niveles.

También se tomó en cuenta para el desarrollo del modelo OSI, que cada nivel debe contar con ciertas premisas, las cuales son siguientes:

1.- Cada nivel realiza tareas únicas y específicas y debe ser creado cuando se necesite un grado diferente de abstracción.
2.- Todo nivel debe tener conocimiento de los niveles inmediatamente adyacente y sólo de éstos.
3.- Todo nivel debe servirse de los servicios del nivel anterior, a la vez que los debe de presentar al superior.
4.- Los servicios de un nivel determinado son independientes de su implantación práctica.

5.- Los límites de cada nivel se deben seleccionar, teniendo en cuenta que minimicen el flujo de información a través de las interfaces establecidas.

Es un conjunto completo de estándares funcionales que especifican interfaces, servicios y formatos de soporte para conseguir la interoperabilidad. El modelo OSI se compone por 7 niveles (capas), cada una de ellas con una función especifica. La utilidad principal del modelo OSI radica en la separación de las distintas tareas que son necesarias para comunicar dos sistemas independientes.

Es importante indicar que no es una arquitectura de red en sí misma, sino que exclusivamente indica la funcionalidad de cada una de ellas. El modelo de referencia OSI se constituye como el marco de trabajo para el desarrollo de protocolos y estándares para la comunicación entre dos capas homónimas ubicadas en equipos separados (Fig. 2.1).

Conforme se avanza en la explicación y funcionamiento de cada una de las capas, se identifica como muchos de los términos se duplican de capa en capa. Un nivel representativo ofrece un conjunto de servicios a al entidad de la capa superior; la capa superior se llama Usuario de Servicio y la capa inferior Proveedor de Servicios.

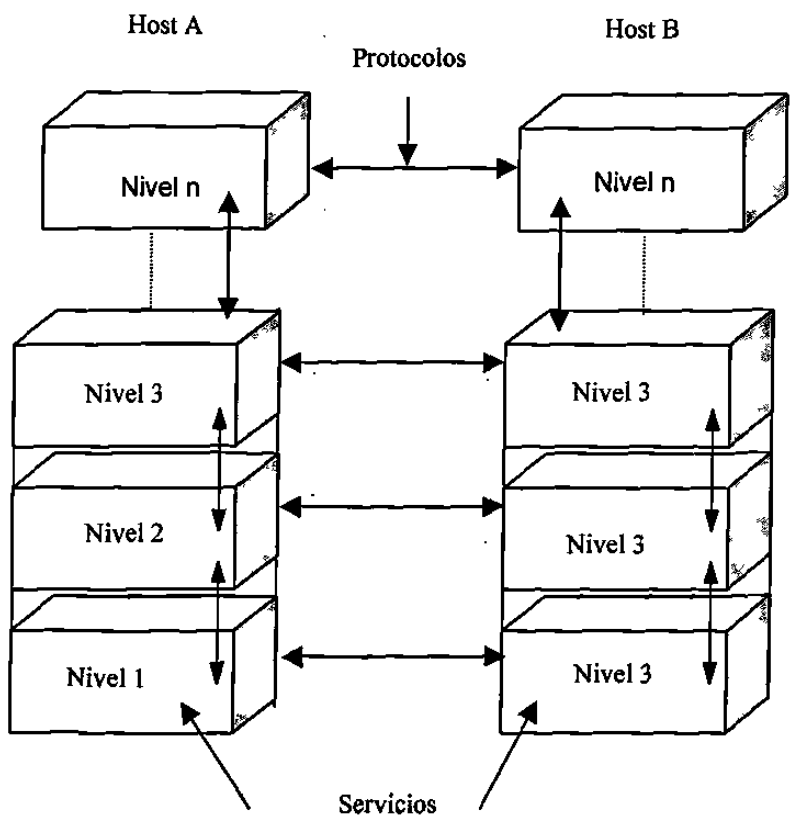


Fig. 2.1 Comunicación entre niveles del modelo OSI

Nivel	Nombre	Función
7	Aplicación	Datos normalizados
6	Presentación	Interpretación de los datos.
5	Sesión	Diálogos de control
4	Transporte	Integridad de los mensajes
3	Red	Enrutamiento de los mensajes
2	Enlace	Detección de errores
1	Físico	Conexión de quipos

Tabla 2.1 Niveles o capas del modelo OSI.

Capa Física.

El nivel físico es el encargado, primordialmente, de la transmisión de los bits de datos (0s ó Is) a través de los circuitos de comunicaciones (Tabla 2.1). El propósito principal de este nivel es definir las reglas para garantizar que cuando la computadora emisora transmite el bit "1", la computadora receptora verifique que un "1" fue recibido y no un "0". Es el nivel de comunicación física de circuitos.

Adicionalmente, esta capa provee los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas entre el dispositivo terminal (DTE) y el punto de conexión de la red (DCE), o entre dos DTE.

- Mecánicos: define el tipo de conector, sus dimensiones físicas, la distribución de pines, etc.
- Eléctricos: concierne alas características eléctricas, como su voltaje, nivel, impedancia, etc.
- Funcionales: define el significado de los niveles de tensión en cada uno de los pines del conector.
- De Procedimiento: define las reglas aplicables a ciertas funciones y la secuencia en que éstas deben incurrir.

Capa de Enlace.

Es el nivel de datos en donde los bits tienen algún significado en la red, y este nivel puede verse como el departamento de recepción y envío de una compañía de manufactura, el cual debe tomar los paquetes que recibe de la Capa de Red y prepararlos de la forma correcta (tramas) para ser transmitidos por el nivel físico. De igual forma sucede cuando recibe paquetes (bits) del nivel físico y tiene que ponerlos en la forma correcta (tramas) para verificar si la información que está recibiendo no contiene errores, si los paquetes vienen en orden, si no faltan paquetes, etc., para entregarlos a nivel de red sin ningún tipo de error.

Dentro de sus funciones se incluyen la de notificar el emisor (la computadora remota) si algún paquete (Trama) se recibe en mal estado (basura); si alguna de las tramas no se recibieron y se requieren que sean enviadas nuevamente (retransmisión), o si una Trama esta duplicada, también cuando la Trama llegó sin problemas. En resumen, es responsable de la integridad de la recepción y envió de la información, así como de saber dónde comienza la transmisión de la trama y dónde termina, y garantizar que tanto la computadora transmisora y como la receptora estén sincronizadas en su reloj y que emplean el mismo sistema de codificación y decodificación.

En esta capa se determina el uso de una disciplina de comunicaciones conocidas como HDLC (*High Level Data Link Control).* El HDLC es el protocolo de línea considerado como un estándar universal, que muchos toman como modelo. Los datos en HDLC se organizan en tramas. La trama es un encuadre que incluye bits de redundancia y control para corregir los errores de transmisión; además, regula el flujo de las tramas para sincronizar su transmisión y recepción, también enmascara a las capas superiores de la imperfecciones de los medios de transmisión utilizados.

Dentro de esta capa se encuentra el protocolo HDLC (3,309), el procedimiento LAP B (7,706) y las normas IEEE 802.2-7 para LAN.

Capa de Red.

El nivel de red es el responsable del direccionamiento de mensajes y de la conversión de las direcciones y nombres lógicos o físicos. También determina la ruta del mensaje desde la computadora emisor hasta la computadora receptora, dependiendo de las condiciones de la red.

Dentro de las funciones de ruteo de mensajes evalúa la mejor ruta que debe seguir el paquete, dependiendo del tráfico en la red, el nivel de servicios, etc. Los problemas de tráfico que controla tienen que ver con el ruteo (*routing),* intercambio (*switching*) y congestionamiento de paquetes de red.

Asimismo, maneja pequeños paquetes de datos juntos para la transmisión a través de la red, así como reestructuración de tramas de datos grandes (números de bits) en paquetes pequeños. En la computadora receptora sé reensamblan los paquetes en su estructura de datos original (Trama).

A la información provienen de la capa de transporte se le agregan componentes apropiados para su ruteo en la red y para mantener un cierto nivel en el control de errores. La información es presentada según el método de comunicaciones para accesar a la red de área local, la red de área extendida (como los enlaces E1) y la conmutación de paquetes (como X.25, etc.)

El diseño de este nivel debe considerar que:

- Los servicios deben ser independientes de la tecnología empleada en la red de datos.
- El nivel de transporte debe ser indiferente al número, tipo y topologías de las redes utilizadas.
- La numeración de la red debe ser uniforme a través de LANs y WANs.

El servicio de red se define en la recomendación X.213 (ISO 8,348 y 8,880 para LANs). Como ejemplo de este nivel, tenemos las recomendaciones X..25, X..32, X.3, X.28, X.29 del CCITT para redes de conmutación de paquetes, la ISO 9,420 protocolo de enrutamiento para LAN y las 8348,8208,8473, 8648 para sistemas de proceso de información.

Capa de Transporte.

El nivel de transporte es llamado ocasionalmente el nivel de *Host to host* o el nivel de *end to end.,* Debido a que en él se establecen, mantienen y terminan las conexiones lógicas para la transferencia de información entre usuarios. En particular de la capa 4 hasta la 7 son conocidas como niveles *end to end* y los niveles 1 a 3 son conocidas como niveles de protocolos.

El nivel de transporte se relacionan más con los beneficios de *end to end,* como son las direcciones de la red, el establecimiento de circuitos virtuales y los procedimientos de entrada y salida a al red. Solamente al alcanzar el nivel superior de transporte (sesión) se abordarán los beneficios que son visibles al usuario final.

Este nivel puede incluir las especificaciones de los mensajes de *broadcast,* los tipos de datagramas, lo servicios de los correos electrónicos, las prioridades de los mensajes, la recolección de la información y su administración y segmentación de la información cuando el tamaño des mayor al máximo del paquete según el protocolo.

Al recibir información del nivel de red, el nivel de transporte verifica que la información esté en el orden adecuado y revisa si existe información duplicada o extraviada. Si la información recibida está en desorden, lo cual es posible en redes grandes cuando se rutean las tramas, el nivel de transporte corrige el problema y transfiere la información al nivel de sesión en donde se le dará un proceso adicional.

Algunos de los principales parámetros de calidad de los que se hacen mención son los siguientes:

- Retardo en el establecimiento de la conexión.
- Falla en el establecimiento de la conexión.
- Protección contra intrusiones.
- Nivele de prioridad.
- Interrupción por congestión.
- Retardo en la liberación de la conexión.
- Error en la liberación, etc.

En este nivel trabajan las recomendaciones X.214 (ISO 8,072) y X.224 (ISO 8,073).

La siguiente figura 2.2 muestra el ordenamiento y funciones de las capas de acuerdo a lo mencionado.

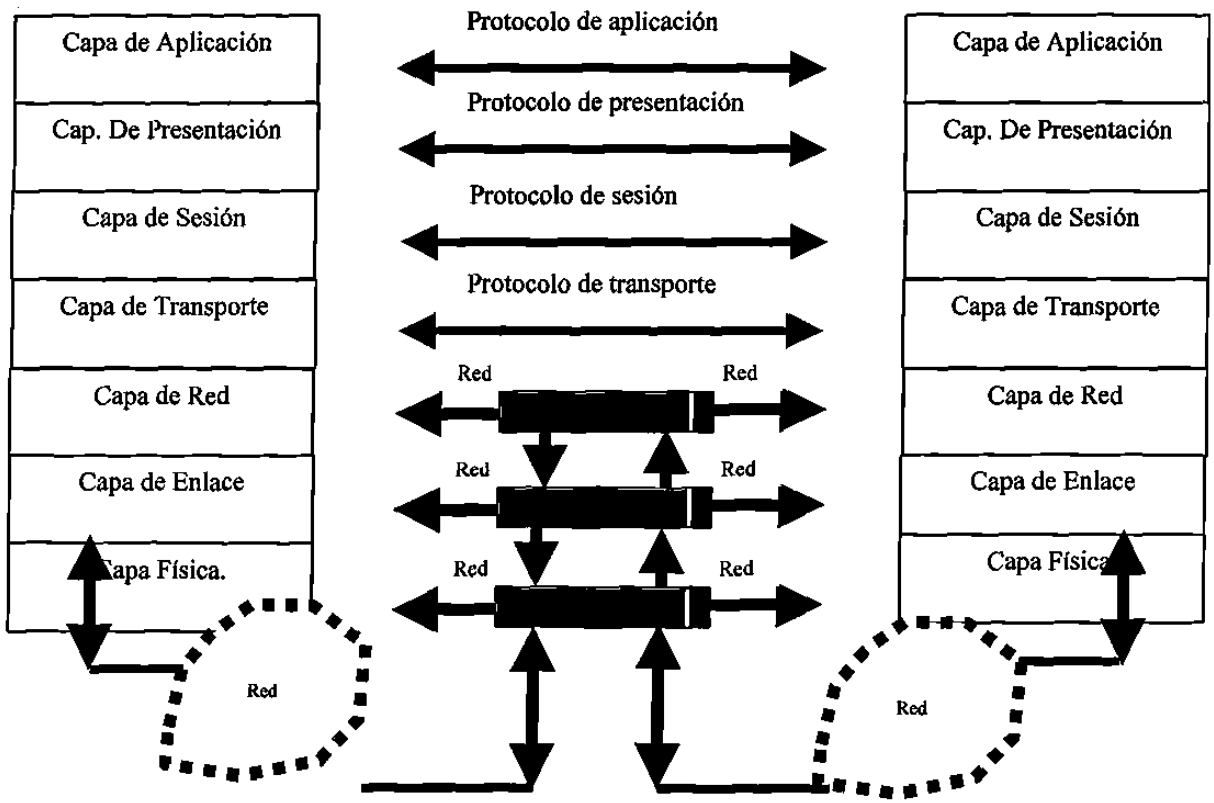


Fig. 2.2 Ordenamiento y funciones de las capas.

Capa de Sesión.

Este nivel es el que permite que 2 aplicaciones en diferentes computadoras establezcan, usen y terminen la conexión llamada sesión. El nivel de sesión maneja el

diálogo que se requiere en la comunicación de 2 dispositivos. Establecer reglas para iniciar y terminar la comunicación entre dispositivos y brinda el servicio de recuperación de errores; es decir, si la comunicación falla brinda el servicio de recuperación de errores; es decir, si la comunicación falla brinda el servicio de recuperación de errores; es decir, si la comunicación falla y ésta es detectada, el nivel de sesión puede retransmitir la información para completar el proceso de la comunicación.

El nivel de sesión es el responsable de iniciar, mantener y terminar cada sesión lógica entre usuarios finales.

Para entender mejor este nivel, se puede pensar en el sistema telefónico. Cuando se levanta el teléfono, espera el tono y marca un número, en ese momento se está creando una conexión física que va desde el nivel uno (físico) como un protocolo de persona a red. Al momento de hablar con la persona en el otro extremo de la línea, se encuentra en una sesión persona a persona. En otra palabras, la sesión es el diálogo de las dos personas que se transporta por el circuito de la conexión telefónica.

También en este nivel se ejecutan funciones de reconocimiento de nombres para el caso de seguridad relacionada a aplicaciones que requieren comunicarse a través de la red.

Se pueden resumir sus funciones de la manera siguiente:

- Establecimiento de la conexión a petición del usuario.
- Liberación de la conexión cuando la transferencia termina.
- Intercambio de datos en ambos sentidos
- Sincronización y mantenimiento de la sesión para proporcionar un intercambio ordenado de los datos entre las entidades de presentación.

En el nivel de sesión están las recomendaciones X.215 (ISO 8,326) y X.225 (ISO 8,327).

Capa de Presentación.

El nivel de presentación define el formato en que la información será intercambiada entre aplicaciones, así como la sintaxis usada entre las mismas. Se traduce la información recibida en el formato del nivel de aplicación a otra intermedio reconocido. En la computadora receptora, la información es traducida del formato intermedio al usado en el nivel de aplicación de dicha computadora y es, a su vez, responsable de la obtención y liberación de la conexión de sesión cuando existan varias alternativas disponibles.

El nivel de Presentación maneja servicios como la administración de la seguridad de la red, como la encirptación y desencriptación, también brinda las reglas para la transferencia de información (*data transfer*) y comprime datos para reducir el número de bits que necesitan ser transmitidos.

En el nivel de presentación se encuadran por ejemplo, las normas para videotex, telefax y teletex y las normas X.225 del CCITT.

Capa de aplicación.

Al ser el nivel más alto del modelo de referencia, el nivel de aplicación es el medio por el cual los procesos de aplicación acceden al entorno OSI. Por ello, este nivel no interactúa con uno más alto.

Proporciona los procedimientos precisos que permiten a los usuarios ejecutar los comandos relativos a sus propias aplicaciones. Estos procesos de aplicación son la fuente y el destino de los datos intercambiados.

2.3 REDES DE DATOS.

El vertiginoso avance tecnológico que han experimentado los campos de la electrónica y la computación en los últimos 50 años, permitieron incrementar la capacidad y velocidad de los sistemas de comunicación de datos. Por esta razón se considera importante conocer el desarrollo de las computadoras en sus diversas etapas, así como los distintos mecanismos para su interconexión.

Actualmente existen varios tipos de redes de cómputo establecidas por las diferentes plataformas tecnológicas desarrolladas por los fabricantes, para entender su arquitectura de una manera sencilla se analizan en este capítulo los conceptos básicos de la computación, así como los elementos que pueden integrar una red. Posteriormente, se tratan a detalle las tecnologías que tienen un papel preponderante en el desarrollo de estas redes.

Breve historia de las computadoras.

En 1834, el inglés Charles Babbage anticipó el nacimiento de lo que hoy se conoce como computadora, inventando una "máquina diferencial" capaz de computar tablas matemáticas mediante un complejo sistema de engranes. En 1834, Lady Ada Augusta Lovelace (auspiciadora económica del invento de Babbage), le sugirió que utilizara las tarjetas perforadas empleadas en los telares electromecánicos para proporcionarle distinta información a su máquina, esto le evitaría tener que cambiar los engranes y mecanismos al hacer un cómputo distinto.

Por otra parte, mientras trabajaba en el perfeccionamiento de su invento, Babbage concibió la idea de una "máquina analítica", capaz de tener una comunicación "inteligente", la llamó "la locura de Babbage". Después sirvió como modelo de inspiración para los futuros inventores de lo que hoy se conoce como computadora.

- **Computadoras Electrónicas.**

La idea de utilizar dispositivos de conmutación, primero eléctricos y después electrónicos, fue motivada por la necesidad de crear un lenguaje sencillo con el que una máquina podría comunicarse con las personas (a través de la representación de señales eléctricas en unos y ceros en un código binario), también porque los dispositivos electrónicos son más veloces que cualquier dispositivo mecánico jamás construido.

- **Primera generación de computadoras (1946-1959).**

Durante la Segunda Guerra Mundial, los militares norteamericanos al requerir mayor velocidad y precisión en los cálculos para dirigir con exactitud la trayectoria de los disparos de sus cañones, patrocinaron un proyecto desarrollado en la Universidad de PennsyIvania para crear una máquina electrónica capaz de efectuar dicho tarea, esta máquina que fue conocida como ENIAC (*Electronic Numerial integrator and Computer)* pesaba aproximadamente 30 toneladas y ocupaba una habitación completa. Su funcionamiento se basaba en la conmutación casi simultánea de cientos de "válvulas electrónicas" que tenían la desventaja de disipar gran cantidad de calor y su vida útil era muy limitada; los tiempos de operación de esta computadora eran del orden de algunos milisegundos.

- **Segunda generación de computadoras (1959-1964).**

Con la invención del transistor como primer dispositivo electrónico de estado sólido, a mediados de la década de los 50, el tamaño de las computadoras, así como los tiempos de procesamiento se redujeron notablemente a aproximadamente 100 microsegundos. Sin embargo, la interconexión entre los distintos componentes los hacia todavía demasiado voluminosa. Durante esta etapa surgen importantes

compañías como IBM, que incorpora lectores de tarjetas y cintas magnéticas a sus computadoras, pero únicamente fabricadas para fines industriales.

- **Tercera generación de computadoras (1969-1971).**

En esta época, el desarrollo de la computación y la electrónica es favorecida por el programa especial norteamericano, con el desarrollo de los primeros circuitos integrados y la primera minicomputadora. Asimismo, aparecen los lenguajes de alto nivel tales como el COBOL y el FORTRAN, que simplifican notablemente la tarea de los programadores y surge el concepto de multiprogramación.

- **Cuarta generación de computadoras (1971 - actualidad).**

1971-72-79 esta etapa se caracteriza por la aparición del primer microprocesador el 8080 de INTEL ™, que permite a la gente común por primera vez experimentar, e incluso hacer su propia computadora. Otros aspectos notables son la aparición del disco flexibles y las Interfaces de entrada/salida.

- **Década de los 80.**

Se comercializan las computadoras personales (PCs) y se genera una gran cantidad de *software* de aplicación especifica y sistemas operativos que permiten concentrarlas en red. Se desarrollan sistemas multiusuarios y emergen las redes de área local o LANs (*Local Area Networks),* que posteriormente serían utilizadas en todo el mundo.

- **Década de los 90.**

Las redes de cómputo se convierten en una necesidad para pequeñas y medianas empresas en el desarrollo de una cultura de sistemas de información. Aparecen

computadoras con mayor velocidad y capacidad de procesamiento. Las computadoras portátiles *(Laptops, handtops)* empiezan a comercializarse rápidamente y evoluciona el concepto de *Telecommuting* (trabajo en casa), edificios inteligentes y oficinas virtuales para tener la capacidad de comunicarse a su red de cómputo desde cualquier parte, y accesar a servicios multimedia, así como a los servicios de *Internet* entre otros.

- **Evaluación de las redes de cómputo.**

El primer paso en la evaluación de las redes de cómputo se inició con el empleo de terminales tontas; utilizadas únicamente para enviar información hacia una computadora central llamada anfitriona o *host.*

Posteriormente, apareció el concepto de tiempo compartido, que consistía en la conexión de terminales tontas a un *host,* (Fig. 2.3) se encontraba enlazado a una macrocomptadora *(mainframe)* que realizaba el procesamiento.

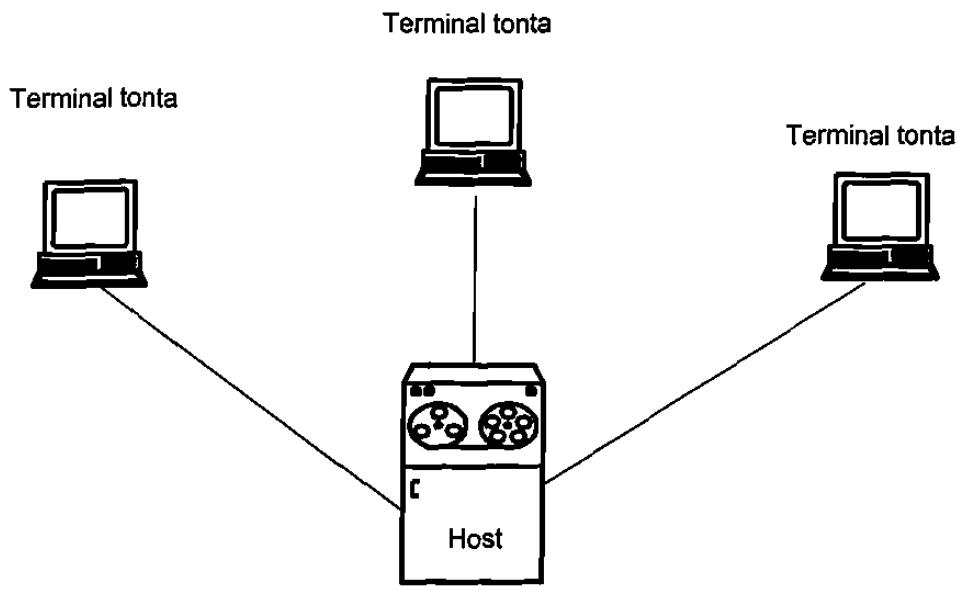


Fig. 2.3 Tiempo compartido.

Empleo de terminales tontas para el envío de información a una computadora central o Host (Fig. 2.4).

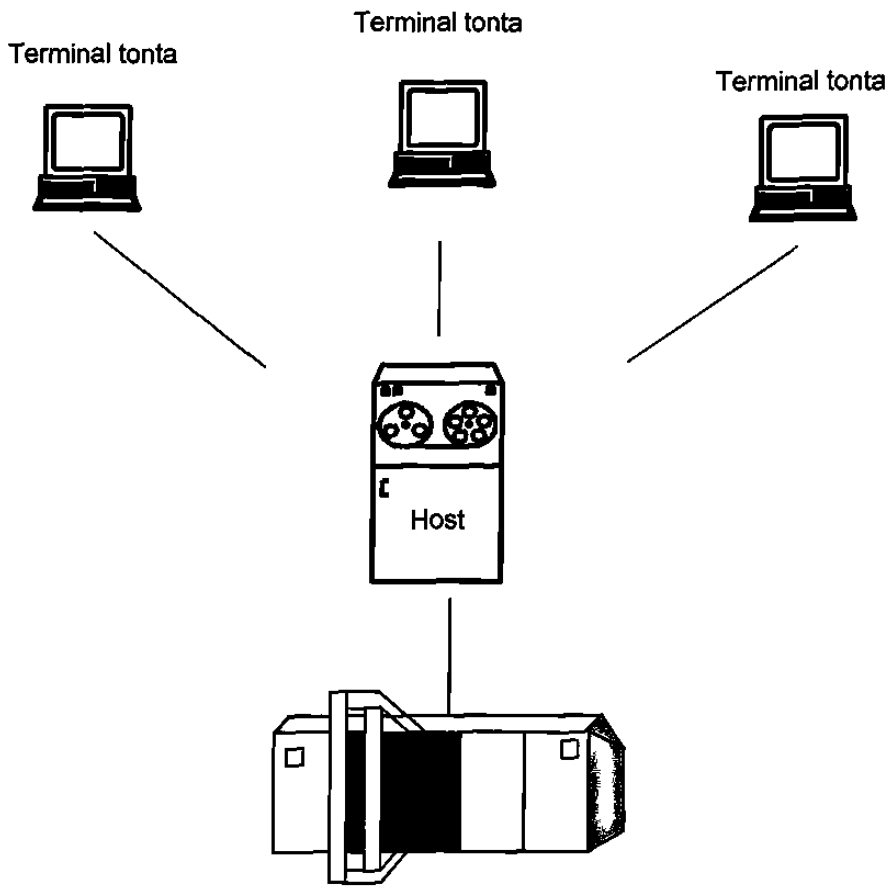


Fig. 2.4 Terminales tontas a un host.

Procesamiento de información bajo el concepto de tiempo compartido.

Con la introducción del procesamiento en tiempo real, el usuario podía ver el resultado del procesamiento de la información en cuando el tecleaba. El incremento en el uso del tiempo compartido por más usuario creó la necesidad el manejo de estándares para lograr agilizar la comunicación con la computadora anfitriona, ya que cada *host* manejaba distintos estándares.

En 1964 se crea el estándar para el intercambio de información ASCII (*American Standard Code for Information Interchange)*, el cual consta de 128 caracteres formados con 7 bits cada uno.

El nacimiento de las microcomptadoras o computadoras personales marcó la pauta de lo que sería la revolución de la computación. La computadora personal le permitió al usuario tener en su escritorio la capacidad del procesamiento de información y el acceso a bases de datos sin tener que depender de ninguna otra máquina.

Una vez desarrollados programas como hojas de cálculo y procesadores de texto, surge la necesidad de conectarse a otros sistemas de cómputo para lo que se diseñó *software* de comunicación con la computadora central, haciendo que la recepción y envío de información *host-PC* fuera más rápida y económica que *host-terminal* tonta.

Con las mejoras en el procesamiento y almacenamiento de información se redujeron cada vez más las diferencias entre las macrocomputadoras, las PCs y las minicomputadoras.

La necesidad de interconexión entre PCs y el hecho de poder compartir recursos e información dio como resultado la aparición de las primeras redes de área loca LANs.

Conforme se extendió la implementación de LANs, la necesidad de comunicarlas se convirtió en un aspecto de gran importancia para las empresas, apareciendo las redes de área amplia WANs (*Wide Area Network)* (Fig. 2.5). En el capítulo 4 se analizan en detalle este tipo de redes.

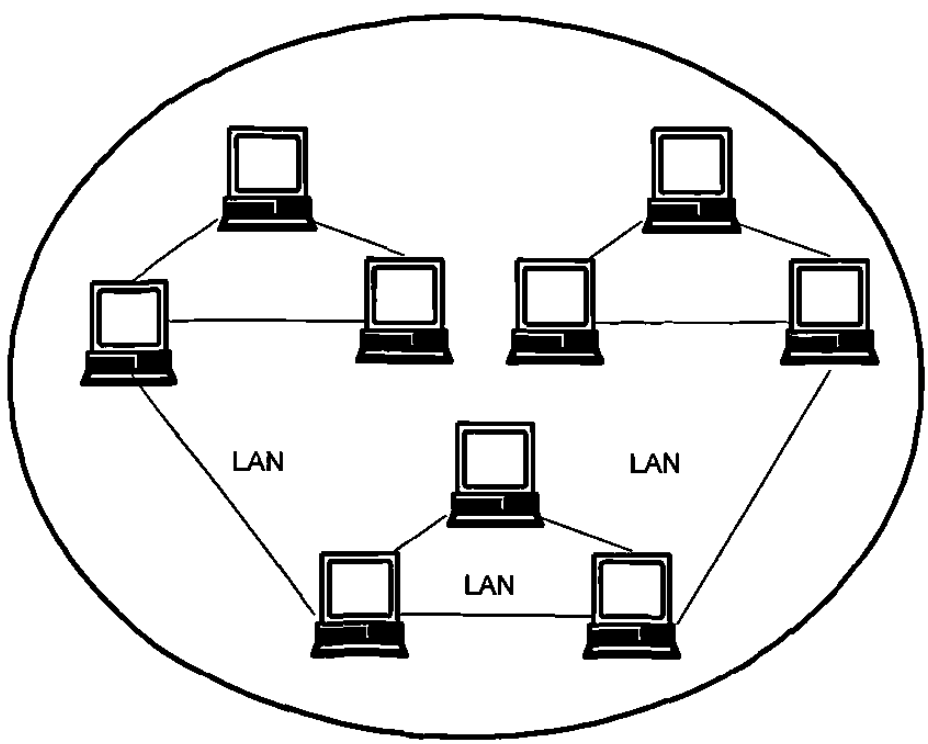


Fig. 2.5 Red de área amplia (WAN).

Para entender una red de cómputo es necesario identificar las partes que la componen y cómo funcionan. El elemento principal de una red lo constituye los sistemas de cómputo, por lo que sus características y funcionamiento son tema de la siuguiente sección.

Clasificación de las tecnologías de red.

El objetivo principal de las redes de cómputo es permitir la comunicación de datos entre los sistemas de computacionales de una organización. Considerando las distancias existentes entre estos sistemas, las tecnologías para redes se clasifican de acuerdo área de cobertura para la que fueron diseñadas como se indica a continuación.

- **Redes de Área Local (Local Area Networks).**

Una LAN provee una comunicación de alta velocidad (4-10 Mbps) y corta distancia (de algunos metros a pocos Kilómetros) entre dispositivos inteligentes como PCs, que permite a los usuarios intercambiar archivos o mensajes y compartir el uso de dispositivos como impresoras, *plotters.* Servidores de archivos o de comunicaciones. En el capítulo 4 se amplían varios aspectos relacionados con la tecnología de LANs.

- **Red de Área Metropolitana (Metropolitan Area Network).**

Las MANs se encuentran entre las LANs y WANs, con una cobertura que comprende desde unos Kilómetros hasta cientos de kilómetros, y una velocidad de transmisión de unos cuantos Kpbs a Gbps, sirve como el *backbone* que interconecta varias LANs distribuidas o puede proveer acceso la red metropolitana o a una red pública de cobertura amplia.

La descripción de algunas tecnologías MANs se incluyen en el capítulo 5.

- **Redes de Área Amplia (Wide Area Network).**

Las primeras redes instaladas emplearon medios de transmisión públicos que permitieron a los sistemas de cómputo comunicarse a través de grandes distancias. Las redes que comunican a un amplio grupo de usuario separados geográficamente son identificadas como redes de área amplia (WAN) (Fig. 2.6).

Las WANs han evolucionado; actualmente los dispositivos conectados a estas redes pueden ser terminales inteligentes, PCs, estaciones de trabajo, minicomputadoras e incluso LANs, .su definición yu funcionamiento se discute en el capítulo 4, mientras que la tecnología de Conectividad se tratan en la sección 2.5. las principales tecnologías desarrolladas para este tipo de redes (X.25, Frame Realy, ATM) se analizan ampliamente en los capítulos 6, 7 y 9.

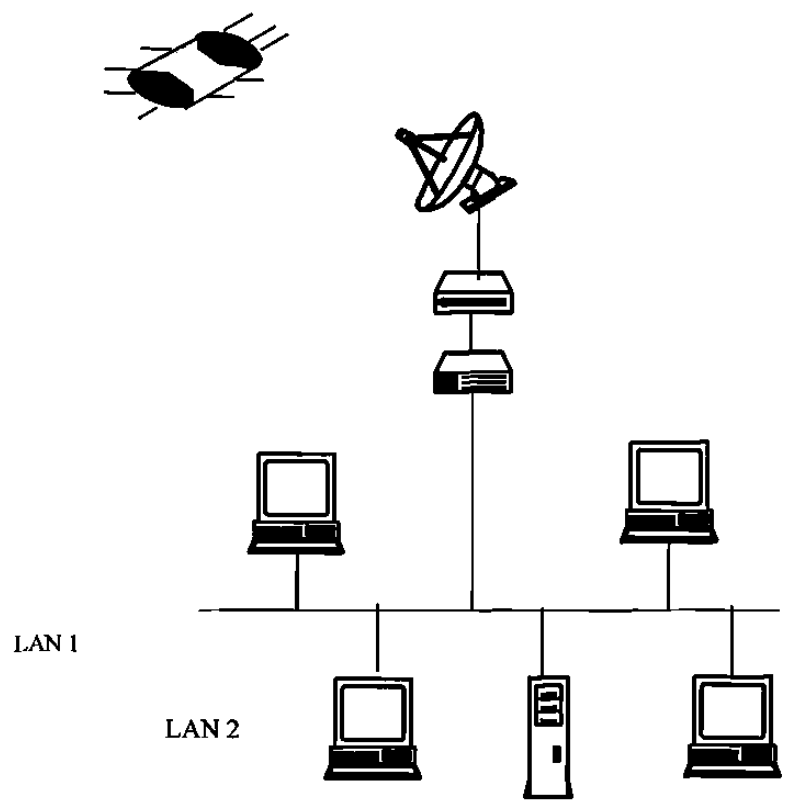


Fig. 2.6 Configuración de una Red de Área Amplia.

CAPÍTULO 3

INTERCONEXION DE REDES

3.1 INTRODUCCIÓN

El crecimiento y cambio constante de diversas áreas han obligado al desarrollo de nuevas tecnologías y estándares en todos los ámbitos de las redes de datos. Estaciones de trabajo con mayor poder de procesamiento, la complejidad de las aplicaciones, el tamaño de los archivos, el centralizado de servidores, así como el incremento de usuarios de red y de estaciones deriva en la necesidad de incrementar el ancho de banda demandante en las redes actuales y propone nuevas tecnologías para llevar esto al cabo.

3.2 IEEE 802

IEEE 802 ha desarrollado el estándar para redes de área metropolitana públicas tratando de conjugar las ventajas de redes de área local (LAN) y redes de área extensa (WAN), proporcionando además de los clásicos servicios de las LANs la posibilidad de canalizar voz y vídeo digitalizados.

Las redes de área local compatibles **IEEE 802.X** (***Ethernet* 802.3**, ***Token Bus* 802.4** y ***Token Ring* 802.5**)

Los criterios del IEEE para el desarrollo del estándar fueron:

- Funcionar bajo un rápido y robusto sistema de señalización.
- Proporcionar unos niveles de seguridad que permitan el establecimiento de Redes Privadas Virtuales (VPN, *Virtual private Network*) dentro de las redes de área metropolitana.

- Asegurar una alta fiabilidad, disponibilidad y facilidad de mantenimiento.
- Permitir una gran eficiencia independientemente del tamaño.

El ámbito de los servicios y la cobertura geográfica de las redes metropolitanas es un campo cuya competencia pertenece a operadores públicos, aunque no sea exclusivo de éstos. Esto se cumple tanto para comunicaciones intercorporativas como intracorporativas. Los motivos principales para esta situación son:

- Ventajas económicas en la compartición de la planta existente para conmutación y transmisión.
- Los impedimentos legales que tienen las compañías privadas para la explotación de servicios portadores.
- Mejores perspectivas de conseguir una interconectividad lo más universal posible mediante una filosofía de interconexión utilizando la red pública.

La red de área metropolitana según el estándar IEEE 802.6 es una alternativa para entornos públicos en los cuales es particularmente bien recibido el tráfico discontinuo que caracteriza a las RALs y el coste efectivo para el cliente se reduce debido a la existencia de una infraestructura para transmisión compartida por muchos usuarios. Además, la tarificación de una red de área metropolitana se basa en el pago por uso básico, así que el usuario paga sólo la capacidad que se usa.

3.3 ETHERNET

Ethernet

Ethernet es la capa física más popular la tecnología LAN usada actualmente. Otros tipos de LAN incluyen Token Ring, Fast Ethernet, FDDI, ATM y LocalTalk. Ethernet es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría los usuarios de la informática

actual. La norma de Ethernet fue definida por el Instituto para los Ingenieros Eléctricos y Electrónicos (IEEE) como IEEE Standard 802.3. Adhiriéndose a la norma de IEEE, los equipo y protocolos de red pueden interoperar eficazmente.

Fast Ethernet

Para redes Ethernet que necesitan mayores velocidades, se estableció la norma Fast Ethernet (IEEE 802.3u). Esta norma elevó los límites de 10 Megabits por segundo (Mbps.) de Ethernet a 100 Mbps. con cambios mínimos a la estructura del cableado existente. Hay tres tipos de Fast Ethernet: 100BASE-TX para el uso con cable UTP de categoría 5, 100BASE-FX para el uso con cable de fibra óptica, y 100BASE-T4 que utiliza un par de cables más para permitir el uso con cables UTP de categoría 3. La norma 100BASE-TX se ha convertido en la más popular debido a su íntima compatibilidad con la norma Ethernet 10BASE-T. En cada punto de la red se debe determinar el número de usuarios que realmente necesitan las prestaciones más altas, para decidir que segmentos del troncal necesitan ser específicamente reconfigurados para 100BASE-T y seleccionar el hardware necesario para conectar dichos segmentos "rápidos" con los segmentos 10BASE-T existentes.

Protocolos

Los protocolos de red son normas que permiten a los ordenadores comunicarse. Un protocolo define la forma en que los ordenadores deben identificarse entre si en una red, la forma en que los datos deben transitar por la red, y cómo esta información debe procesarse una vez que alcanza su destino final. Los protocolos también definen procedimientos para gestionar transmisiones o "paquetes" perdidos o dañados. IPX (para Novell NetWare), TCP/IP (para UNIX, WindowsNT, Windows 95/98 y otras plataformas), DECnet (para conectar una red de ordenadores Digital), AppleTalk (para los ordenadores Macintosh), y NetBIOS/NetBEUI (para redes LAN Manager y WindowsNT) son algunos de los protocolos más populares en la actualidad.

Medios Físicos

Una parte importante en el diseño e instalación de una red Ethernet es la correcta selección del medio físico apropiado al entorno existente. Actualmente, se emplean, básicamente, cuatro tipos de cableados o medios físicos: coaxial grueso ("thickwire") para redes 10BASE5, coaxial fino ("thinwire") para redes 10BASE2, par trenzado no apantallado (UTP) para redes 10BASE-T o 100Base-TX y fibra óptica para redes 10BASE-FL o 100BASE-FX.

Cable Coaxial Grueso

El cable coaxial grueso o Ethernet 10Base-5, se empleaba, generalmente, para crear grandes troncales ("backbones"). Un troncal une muchos pequeños segmentos de red en una gran LAN. El cable coaxial grueso es un troncal excelente porque puede soportar muchos nodos en una topología de bus y el segmento puede ser muy largo. Puede ir de un grupo de trabajo al siguiente, donde las redes departamentales pueden ser interconectadas al troncal. Un segmento de cable coaxial grueso puede tener hasta 500 metros de longitud y máximo de 100 nodos conectados.

Cable Coaxial Fino

El cable coaxial fino, o Ethernet 10Base-2, ofrece muchas de las ventajas de la topología de bus del coaxial grueso, con un coste menor y una instalación más sencilla. El cable coaxial fino es considerablemente más delgado y más flexible, pero sólo puede soportar 30 nodos, cada uno separado por un mínimo de 0.5 metros, y cada segmento no puede superar los 185 metros. Aún sujeto a estas restricciones, el cable coaxial fino puede ser usado para crear troncales, aunque con menos nodos.

Un segmento de cable coaxial fino esta compuesto por muchos cables de diferentes longitudes, cada uno con un conector de tipo BNC en cada uno de los extremos. Cada cable se conecta al siguiente con un conector de tipo "T", donde se necesita instalar un nodo.

Par Trenzado

El cable UTP es similar, o incluso el mismo, al cable telefónico que puede estar instalado y disponible para la red en muchos edificios.

Hoy, los esquemas de instalación de cableado más populares son 10BASE-T y 100BASE-TX, tanto con cable de par trenzado de tipo apantallado como sin apantallar (STP y UTP, respectivamente).

El cable de Categoría 4 soporta velocidades de hasta 20 Mbps., y el de Categoría 3 de hasta 16 Mbps.

Los segmentos UTP están limitados a 100 metros.

Fibra Optica

La norma Ethernet permite segmentos de cable de fibra óptica de dos kilómetros de longitud, haciendo Ethernet a fibra óptica perfecto para conectar nodos y edificios que de otro modo no podrían ser conectados con cableados de cobre.

Topologías

Se diseñan redes Ethernet típicamente en dos configuraciones generales o topologías: "bus" y "estrella".

Una topología de bus consiste en que los nodos se unen en serie con cada nodo conectado a un cable largo o bus.

10BASE-T Ethernet y Fast Ethernet conectan una red de ordenadores mediante una topología de estrella. Generalmente un ordenador se sitúa a un extremo del segmento, y el otro extremo se termina en una situación central con un concentrador. La principal ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos "punto a punto" tiene una rotura, afectará sólo a los dos nodos en ese eslabón. Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera.

Colisiones

Ethernet es un medio compartido, por lo que hay reglas para enviar los paquetes para evitar conflictos y proteger la integridad de los datos. Los nodos en una red Ethernet envían paquetes cuando ellos determinan que la red no está en uso. Es posible que dos nodos en situaciones diferentes pudieran intentar enviar datos al mismo tiempo. Cuando ambos PC's están transfiriendo un paquete, al mismo tiempo, a la red, se producirá una colisión.

Productos Ethernet

La traducción de las normas y tecnologías que hemos descrito anteriormente se convierten en productos específicos que los administradores de las redes usan para construirlas. El texto siguiente explica los productos clave necesarios para construir una red Ethernet.

Transceptores

Para conectar nodos a los diversos medios físicos Ethernet se usan transceptores. La mayoría de los ordenadores y tarjetas de interfaz de red incorporan, en su electrónica, un transceptor 10BASE-T o 10BASE2, permitiéndoles ser conectados directamente a

Ethernet sin requerir un transceptor externo. Otros dispositivos compatibles Ethernet, más viejos, incorporan un conector AUI para permitir al usuario conectarlo a cualquier medio físico, a través de un transceptor externo. El conector AUI consiste en un conector de tipo DB de 15 pines, hembra en el lado del ordenador, macho en el lado del transceptor. Los cables coaxiales gruesos (10BASE5) también usan transceptores para permitir las conexiones.

Para las redes Fast Ethernet, se desarrolló una interfaz llamada MII (Media Independent Interface o interfaz independiente de medios) para ofrecer un modo flexible de soportar medios de 100 Mbps. MII es un modo popular de conectar enlaces 100BASE-FX a los dispositivos Fast Ethernet basados en cobre.

Repetidores

Los repetidores se emplean para conectar dos o más segmentos Ethernet de cualquier tipo de medio físico. Según los segmentos exceden el máximo número de nodos o la longitud máxima, la calidad de las señales empieza a deteriorarse.

Los repetidores Ethernet son necesarios en las topologías de estrella. Como hemos indicado, una red con sólo dos nodos está limitada. Un repetidor de par trenzado permite a diversos segmentos "punto a punto" unirse en una sola red. Un extremo del enlace punto a punto se conecta al repetidor y el otro al ordenador con un transceptor. Si el repetidor está conectado al troncal, entonces todos los ordenadores conectados en los extremos de los segmentos de par trenzado pueden comunicar con todos los servidores del troncal.

Al igual que los diferentes medios de Ethernet tienen diferentes limitaciones, los grandes segmentos creados con repetidores y múltiples segmentos, también tienen restricciones. Estas restricciones, generalmente tienen que ver con los requisitos de sincronización. A pesar de que las señales eléctricas que circulan por los medios Ethernet, viajan a cerca de la velocidad de la luz, aún requieren un tiempo finito para viajar de un extremo de una gran red a otro. Las normas Ethernet asumen que no va a llevar más de un determinado tiempo para que una señal sea propagada entre los extremos más alejados de la red. Si la red es excesivamente grande, esta presunción no

se cumple, y la red no funcionará correctamente. Los problemas de sincronización no pueden ser tomados a la ligera. Cuando las normas Ethernet son violadas, se pierden los paquetes, las prestaciones de la red se ven afectadas, y las aplicaciones se enlentecen y pueden fallar.

Concentradores

Los concentradores son, en definitiva, repetidores para cableado de par trenzado.

Un concentrador, al igual que un repetidor, toma cualquier señal entrante y la repite hacia todos los puertos. Si el concentrador se conecta al troncal, entonces todos los ordenadores situados al final de los segmentos del par trenzado pueden comunicarse con todos los servidores en el troncal.

Lo más importante a resaltar sobre los concentradores es que sólo permiten a los usuarios compartir Ethernet. Una red de repetidores es denominada "Ethernet compartido". El número y tipo de concentradores en cualquier dominio de colisión para Ethernet 10 Mbps. está limitado por las reglas siguientes (Tabla 3.1):

Tipo de Red	**Máx. nº de Nodos por Segmento**	**Distancia Máx. por Segmento**
10Base-T	2	100 m.
10Base-2	30	185 m.
10Base-5	100	500 m.
10Base-FL	2	2000 m.

Tabla 3.1 Red Ethernet

Fast Ethernet ha modificado las reglas de repetidores, dado que el tamaño del paquete mínimo tarda menos tiempo para transmitirse que en Ethernet. En redes de Fast Ethernet, hay dos clases de repetidores, Clase I y Clase II. La tabla siguiente es la

distancia (diámetro) característica para combinaciones de estos tipos de repetidores Ethernet (Tabla 3.2):

Fast Ethernet	**Cobre**	**Fibra**
Ningún Repetidor	100 m.	412 m. *
Un Repetidor de Clase I	200 m.	272 m.
Un Repetidor de Clase II	200 m.	272 m.
Dos Repetidores de Clase II	205 m.	228 m.
* 2 Km. en modo Full Duplex		

Tabla 3.2 Fast Ethernet

Aumentando la Velocidad

Mientras los repetidores permiten que la LAN se extienda más allá de las limitaciones normales, aún existe el límite en la cantidad de nodos que pueden conectarse. Los puentes ("bridge") y conmutadores ("switch"), permiten a la LAN crecer significativamente. Proporcionando más flexibilidad para topologías de red y mejores prestaciones, los puentes y conmutadores seguirán ganando popularidad entre los administradores de redes.

Puentes

La función de un puente es interconectar redes separadas. Los puentes pueden conectar tipos de redes diferentes (como Ethernet y Fast Ethernet) o redes del mismo tipo. Los puentes trazan las direcciones de Ethernet de los nodos que residen en cada segmento de la red y permiten sólo el tráfico necesario para atravesar el puente. Cuando un paquete es recibido por el puente, el puente determina el segmento fuente y destino. Si ambos segmentos son el mismo, el paquete se descarta ("se filtra"); si los segmentos son diferentes, el paquete es "remitido" al segmento correcto. El filtrado y la

regeneración de paquetes remitidos permite a la tecnología de los puentes, dividir una red en dominios de colisión separados. Ello permite emplear distancias mayores y más repetidores en el diseño de una red.

Protocolo Spanning Tree

El Algoritmo Spanning Tree Protocol es una norma del software (especificaciones IEEE 802.1d) para describir cómo los puentes y conmutadores pueden comunicarse para evitar bucles en la red.

En algunos casos, los administradores de la red diseñan bucles en redes con puentes, de forma que si un puente o conmutador falla, el algoritmo Spanning Tree calculará la ruta alternativa en la configuración de la red. Para que esto funcione correctamente, todos los conmutadores y puentes de la red deben de soportar este protocolo.

Error! Bookmark not defined.**Conmutadores Ethernet**

Los conmutadores ("switch") Ethernet son una ampliación del concepto de puentes. Los conmutadores LAN tienen, básicamente, dos arquitecturas, "store and forward" (almacenar y remitir) y "cut through" (cortar y atravesar). Inicialmente, los modelos "cut through", tenían una ventaja de velocidad porque cuando un paquete entra en el conmutador, sólo se examina la dirección del destino antes de remitirlo a su segmento de destino. Un conmutador "store and forward", por otro lado, acepta y analiza el paquete completo antes de remitirlo a su destino.

Cada uno de los segmentos conectados a un conmutador Ethernet tiene el ancho de bando completo de 10 Mbps., compartido por menos usuarios, lo que resulta en unas mejores prestaciones (en oposición a los concentradores que sólo permiten compartir el ancho de banda de una sola red Ethernet).

Los nuevos conmutadores ofrecen enlaces de gran velocidad, como FDDI, Fast Ethernet o ATM, que pueden usarse para comunicar conmutadores o proporcionar

anchos de banda superiores a servidores particularmente importantes que tienen mucho tráfico. Una red compuesta de varios conmutadores unidos mediante enlaces se denomina "troncal colapsado".

Encaminadores

Los routers o encaminadores trabajan de una manera similar a los conmutadores y puentes ya que filtran el tráfico de la red.

Administración de la Red

Conforme se agregan más dispositivos a la red, aumenta la importancia del problema de su gestión.

Gestión serie: Para acceder a un dispositivo se emplea un terminal o puerto serie de un PC. La limitación de esta solución de gestión es que no se conecta una red aunque los servidores serie están cambiando esta situación.

Gestión Telnet: Para los dispositivos que soportan las conexiones IP, es normalmente posible realizar telnet a un puerto de gestión en esos dispositivos. El uso de telnet permite administración sobre la red pero tiene la limitación de que si el dispositivo desconectado o averiado, no podrá hacerse la conexión telnet.

SNMP (Protocolo de Administración de Red Simple o "Simple Network Management Protocol") esta basado en IP y define un conjunto de objetos que los administradores pueden interrogar en los dispositivos de red. Estos objetos se definen como atributos MIB (Base de Información de Gestión o "Management Information Base") y puede ser propietarios o adecuarse a las normas establecidas.

RMON (MIB de Monitorización Remota o "Remote Monitoring MIB") proporciona un nivel más alto de información que SNMP. Cuando un dispositivo lo soporta, RMON se ejecuta continuamente y permite al administrador de la red ver estadísticas, configurar condiciones de alarma que puedan emitir "trampas" o anotarse en una tabla y marcar ciertos eventos cuando tienen lugar.

Servidores

Los servidores son dispositivos que permiten compartir archivos, dispositivos u otros recursos para los usuarios de la red.

Los servidores de impresión son dispositivos que conectan una impresora a la red y permiten a los usuarios de la red acceder a la impresora. Los servidores de terminales de Lantronix permiten a los terminales conectarse directamente a una red y acceder a cualquier servidor disponible. Los servidores de acceso remoto proporcionan soporte de encaminamiento (routing) para conectividad WAN y LAN sobre líneas de comunicaciones dedicadas o normales.

Servidores de Impresoras

Los servidores de impresión permiten compartir las impresoras entre los nodos en la red. Soportando tanto interfaces paralelo o serie (a veces ambos), un servidor de impresión acepta trabajos de impresión de cualquier nodo de la red usando cualquiera de los protocolos soportados y gestiona la impresión de esos trabajos en la impresora apropiada.

La última generación de servidores de impresión soporta múltiples protocolos, tiene múltiples opciones de conexión paralelo y serie y, en algunos casos, es lo bastante pequeño como para encajar directamente en el puerto paralelo de la propia impresora.

Servidores de Terminales

La proliferación de ordenadores personales y estructuras cliente-servidor ha reducido la presencia de terminales y servidores de terminales.

Los dispositivos que se conectan a una red a través de un servidor de terminales pueden ser compartidos entre los terminales y servidores, tanto local como remotamente. Un solo terminal puede conectarse simultáneamente a varios servidores (en sesiones

coexistentes múltiples), y puede conmutar entre ellos. También pueden usarse servidores de terminales para unir a través de la red dispositivos que sólo tienen conexiones serie.

Los servidores de terminales, por supuesto, también permiten usarse para cualquier otro dispositivo serie, como por ejemplo, para crear baterías de modems, o para funciones más sofisticadas como la conversión de protocolos, el balanceo de la carga de trabajo entre diferentes servidores, etc.

Servidores Delgados Universales

Mientras los servidores de terminales y servidores de impresión cumplen las demandas particulares de conexión de terminales e impresoras, emergen otro tipo de dispositivos que las organizaciones buscan para incorporar en la red - los dispositivos de tipo "Servidor Delgado Universal" (Universal Thin Server).

Los tradicionales servidores de terminales e impresoras, con su alta densidad de puertos serie, pueden servir sólo aquella parte de la demanda para la conectividad serie a Ethernet donde todos los dispositivos están físicamente próximos. ¿Pero qué ocurre con un solo lector de tarjetas o dispositivo de la fábrica localizados en una área sin ningún otro dispositivo? La solución a este problema es un servidor Ethernet con un solo puerto serie, que puede permitir acceder al puerto serie de ese dispositivo desde la red.

3.4 TOKEN RING

Las redes en anillo no son nada nuevo, pues se han utilizado desde mucho para redes tanto locales como de área amplia. Entre muchas características atractivas está que un anillo no es realmente un medio de difusión, sino un conjunto de enlaces punto a punto individuales que, coincidentemente, forman un círculo. Los enlaces punto a punto implican una tecnología bien entendida y probada en el campo que puede operar en par trenzado, cable coaxial y fibra óptica. La ingeniería de anillos es casi completamente digital. En contraste por ejemplo, el 802.3 tiene una componente analógica considerable

para la detección de colisiones.

Un anillo también es equitativo y tiene un límite superior conocido de acceso a canal. Por estas razones , IBM escogió el anillo como su LAN y el IEEE ha incluido el estándar Token Ring como el 802.5.

Un asunto fundamental en el diseño y análisis de cualquier red en anillo es la "longitud física" de un bit. Si la tasa de datos del anillo es de R Mbps, se emite un bit cada 1/R μseg. Con una velocidad de propagación de señal típica de unos 200 m/μseg, cada bit ocupa 200/R metros del anillo. Esto significa por ejemplo, que un anillo de 1Mbps cuya circunferencia es de 1000 metros puede contener solo 5 bits a la vez.

En un token ring (anillo con ficha) circula un patrón de bit especial, llamado ficha (token) alrededor del anillo cuando todas las estaciones están inactivas. Cuando una estación quiere transmitir un marco, debe tomar la ficha y retirarla del anillo antes de transmitir. Esta acción se lleva acabo invirtiendo un solo bit de la ficha de 3 Bytes, lo que instantáneamente la convierte en los tres primeros bytes de un marco de datos normal.

Debido a que solo hay una ficha, sólo una estación puede transmitir en un instante dado, resolviendo por tanto el problema de acceso al canal de la misma manera que lo resuelve al token bus.

Una implicación del diseño del token ring es que el anillo mismo debe tener un retardo (delay) suficiente para contener una ficha completa que circule cuando todas las estaciones están inactivas.

3.5 REDES FDDI (ANSI X3T9.5 / ISO 9384)

Descripción funcional

El Interfaz de Datos Distribuidos por Fibra FDDI (*Fiber Distributed Data Interface*) es un conjunto de especificaciones compatibles con el modelo OSI, del cual cubren los niveles 1 y 2 parcialmente, para permitir el establecimiento de comunicaciones en red a velocidades de transmisión en el rango de los **100 Mbits/s.**

El estándar FDDI se está convirtiendo actualmente en el sistema más extendido para entornos privados que requieren conectividad entre múltiples edificios y para la interconexión de estaciones de trabajo y grandes ordenadores. FDDI se comporta de manera óptima en aquellos entornos en los cuales son esenciales la gestión de red y la recuperación de fallos.

Actualmente algunos operadores están empleando redes públicas FDDI como un paso previo a redes del estándar IEEE 802.6, con el fin de interconectar redes locales localizadas en distintos edificios dentro de: Campus Universitarios, Parques Tecnológicos, Complejos Industriales, etc.

No obstante, FDDI no puede ser considerada, desde el punto de vista de red pública, como la solución perfecta para interconectar redes locales de diferentes corporaciones. Diseñada en principio para redes privadas, no tiene mecanismos internos para la medición de paquetes transmitidos, tiempo de conexión, etc., parámetros sin los cuales es difícil una facturación del servicio.

Para resolver esto, se ha desarrollado **un servicio de gestión de red SMT** (*Station ManagemenT*, Gestión de Estación) que se incluye en FDDI. Además, toda la información que circula por el anillo puede ser leída en cualquier nodo violando la norma básica de seguridad de la información (esto puede resolverse empleando técnicas de cifrado).

Tecnología FDDI

El estándar FDDI ha sido desarrollado por el ANSI en el Comité X3T9.5; la norma es la ANSI X3T9.5 y ha sido adoptada por la Organización Internacional de Normalización (ISO) bajo la denominación ISO 9384.

El Interfaz de Datos Distribuida por Fibra (FDDI) es una red de fibra óptica a 100 Mbits/s, con topología en anillo doble, utilizando técnicas de conmutación de paquetes con protocolo de paso de testigo como método de acceso.

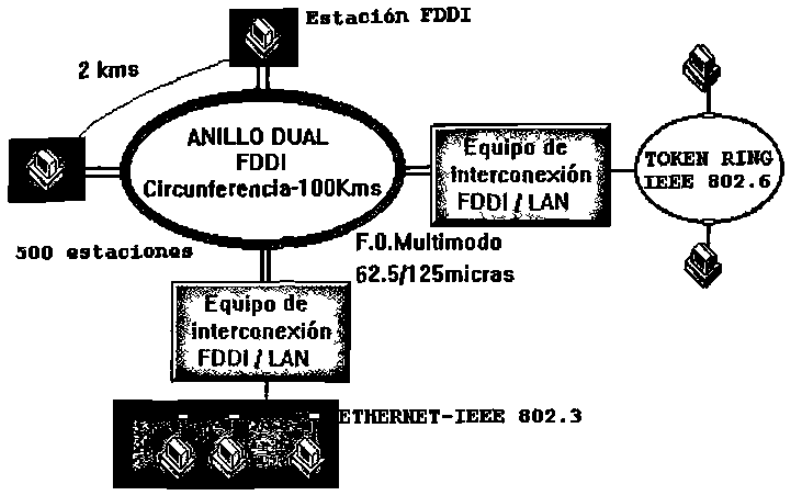


Fig 3.1 Anillo dual FDDI.

- **Topología funcional**

  La infraestructura física es un anillo de fibra óptica de doble canal. Uno de estos canales es el camino principal de comunicaciones, mientras que el otro se utiliza para funciones de gestión de la red y como alternativa de seguridad, para el caso de que se produzcan anomalías en el camino principal. No obstante, para abaratar los costes de conexión a una red FDDI, la norma contempla, también, la posibilidad de conectarse solamente al camino principal.

- **Método de acceso**

  FDDI utiliza un método de acceso por paso de testigo (***Token***) con tiempo de transmisión restringido. Los canales que forman un anillo tienen sentidos de rotación diferentes, con lo cual los datos y los testigos circulan simultáneamente en direcciones opuestas, por cada uno de los canales independientes.

  El anillo doble está formado por una serie de nodos conectados a un medio de transmisión de fibra óptica de tal forma que constituyen un doble bucle cerrado. Cuando una estación conectada al anillo

desea enviar un paquete de información a otra estación, la primera operación que debe realizar es capturar el testigo, que es una secuencia de símbolos que forman un paquete especial que está circulando por la red y que ofrece la oportunidad de trasmitir paquetes a la estación que lo posea.

Cada paquete consta de una secuencia de símbolos organizados según unos campos que indican, por ejemplo, el comienzo del paquete, la dirección de la estación destino y origen, campos de control, y, por supuesto, el campo principal que contiene la información que desea enviarse.

- **Transmisión de datos**

Una vez que la estación emisora está en posesión del testigo, que previamente ha retirado de la red, podrá enviar sus datos debidamente empaquetados, pudiendo enviar más de un paquete en función del tiempo asignado para transmisión. Este mecanismo controla el tiempo máximo que una estación puede retener el testigo. Una vez enviado el último paquete, la estación "libera" el testigo para que pueda ser usado por la estación siguiente.

El paquete enviado es repetido de una estación a otra hasta que llega a la estación destino. Esta reconoce que el paquete le pertenece ya que analiza el campo de dirección destino y lo compara con el suyo. Una vez reconocida su dirección, la estación copia el paquete y lo vuelve a retransmitir pero indicando en el campo de control que ha sido recibido (correcta o incorrectamente). El paquete seguirá circulando por el anillo hasta que llega a la estación origen que es la encargada de retirar el paquete de la red, ya que en caso contrario el paquete estaría dando vueltas indefinidamente.

En el caso de que el paquete llegue con la indicación de que fue recibido incorrectamente por el destino, la estación origen deberá retransmitirlo de nuevo.

- **Medio de transmisión**

El grupo normalizador de FDDI ha elegido el cable multimodo de fibra óptica como soporte físico, con una longitud de onda normalizada de 1.300 nm. El estándar especifica el uso de la fibra multimodo 62'5/125 μ de índice gradual. Sin embargo, pueden emplearse otros tipos de fibra (p.ej:50/125, 85/125, 100/140 μ).

Para todos estos tipos de fibra se especifica un ancho de banda de al menos 500 MHz x km y una atenuación no mayor de 2.5 dB/km. Recientemente se han empezado trabajos sobre una variante FDDI que utiliza fibra monomodo (PMD-SMF), a 100 Mbit/s, para enlaces a distancias mayores a 2 km, y especifica el empleo de diodos láser para transmisión, obteniéndose enlaces de 60 a 100 km. La especificación aún está incompleta, pero se vienen empleando conversores multimodo/monomodo (no contemplados en el estándar) para instalaciones donde ya existe fibra monomodo.

La fibra óptica ofrece las ventajas de una anchura de banda prácticamente ilimitada, inmunidad al ruido, un alto nivel de seguridad y opera a una velocidad diez veces mayor que una red de área local convencional.

- **Distancia entre nodos**

Para minimizar costes (dispositivos ópticos y cable), la norma FDDI especifica la utilización de trasmisores tipo LED y fibra multimodo. Con esta tecnología "barata", por el empleo de dispositivos

económicos en emisión y recepción, la distancia máxima de los enlaces es de 2 km (limitada por la dispersión modal y cromática).

- **Extensión**

  Con estas elecciones técnicas, se pueden configurar redes de hasta 50 km de diámetro, en donde la distancia máxima entre nodos de conexión es de 2 km. Pueden conectarse a la red hasta 500 nodos; puesto que estos nodos pueden ser puentes de acceso hacia redes ***Ethernet*** y ***Token Ring***, el número de ordenadores usuarios de una red FDDI puede alcanzar varios miles de unidades.

Gestión

FDDI es una red de control distribuido, por lo que no hay ninguna estación que se encargue de sincronizar la transmisión. Cada estación transmite los datos con su propio reloj y además debe ser capaz de extraer los datos de la señal recibida, teniendo en cuenta que éstos vienen generados según el reloj de la estación precedente. Cada uno de los nodos controla las condiciones del anillo, y detecta el estado inactivo o de fallo.

Tipos de nodos

Las redes FDDI pueden estar configuradas con dos tipos de elementos funcionales o nodos de red y pueden conectarse al anillo de dos formas diferentes (Tabla 3.3):

Tipo de conexión	Elemento funcional estación	Concentrador
Doble	DAS	DAC
Simple	SAS	SAC

Tabla 3.3 Elementos funcionales de FDDI.

- Las estaciones son nodos que transmiten al y reciben datos del anillo FDDI:
- Estaciones de trabajo, minis y grandes ordenadores.
- Puentes (Bridges) y Encaminadores (Routers).

Pueden conectarse al anillo mediante un enlace doble (Estaciones de doble acceso, DAS, *Double Access Station*), o a través de un concentrador mediante un enlace simple (Estaciones de acceso simple, SAS, *Simple Access Station*). En caso de ruptura del enlace simple correspondiente, las estaciones SAS quedan incomunicadas.

- Los concentradores actúan como dispositivos que permiten conectar múltiples estaciones u otros concentradores al anillo FDDI. Si el concentrador se conecta al anillo se denomina DAC, en caso contrario SAC. Ofrecen la facilidad de interconectar en la misma red estaciones DAS y SAS, estableciendo topologías en árbol (Fig. 3.2).

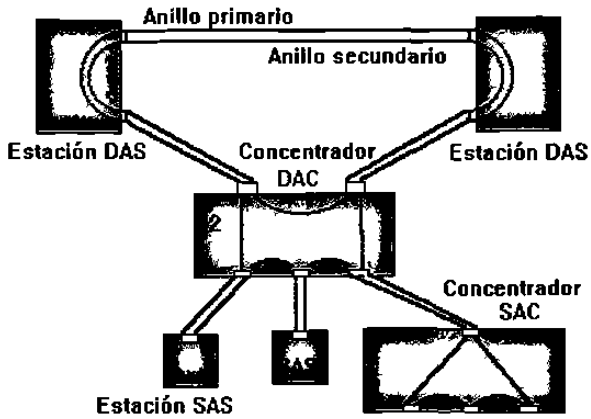


Fig. 3.2 Estaciones DAC y SAS.

Reconfiguración frente a fallos

Una de las principales características de la red FDDI es su tolerancia a fallos por rotura del enlace de fibra óptica. La posibilidad de reconfiguración del anillo se debe a que es un anillo doble y al empleo de "puentes" ópticos que se activan en caso de pérdida del enlace, este tipo de puentes sólo está disponible en estaciones o concentradores con conexión doble. La figura 3.3 muestra una red FDDI reconfigurada después de una rotura de cable.

Fig. 3.3 Red FDDI reconfigurada.

Seguridad y Privacidad

La utilización de fibra óptica en una red FDDI permite alcanzar grados de seguridad óptimos y detectar cualquier tipo de intrusismo en el medio de transmisión.

Aunque la privacidad de los datos no es una característica funcional que se requiera en un entorno de red privada, siempre es posible utilizar técnicas de cifrado de datos que permiten obtener un mayor grado de privacidad.

Arquitectura de red

A continuación se incluye una clasificación de las distintas configuraciones a nivel funcional que soportan las redes de área metropolitana:

- **Redes Terminales (*back-end*):**

  Permiten la transferencia rápida de información entre la Unidad Central de Proceso (UCP) y dispositivos de almacenamiento masivo (discos ópticos, unidades de cintas) y periféricos de alta velocidad (impresoras, trazadores).

- **Redes Dorsales (*backbone*):**

  Conectan redes de área local de velocidades menores. La velocidad de transmisión de la red de área metropolitana permite manejar una carga agregada de múltiples redes conectadas sin establecer cuellos de botella ni degradar sus respectivas prestaciones. Las redes de área local compatibles **IEEE 802.X** (***Ethernet* 802.3**, ***Token Bus* 802.4** y ***Token Ring* 802.5**) se interconectan mediante puentes o encaminadores con salida al nodo dered MAN. La red dorsal permite establecer enlaces con las redes pública de área extensa (X.25, ***frame relay***) o con redes privadas del tipo SNA mediante pasarelas específicas.

- **Redes Frontales (*front-end*):**

  Conectan grandes ordenadores, minis y ordenadores personales, estaciones de trabajo, terminales gráficos de alta resolución CAD/CAM, impresoras láser, etc. Esta configuración (Fig. 3.4) se asemeja al entorno de red local, pero con unas prestaciones muy superiores comparada con ***Ethernet*** o ***Token Ring***.

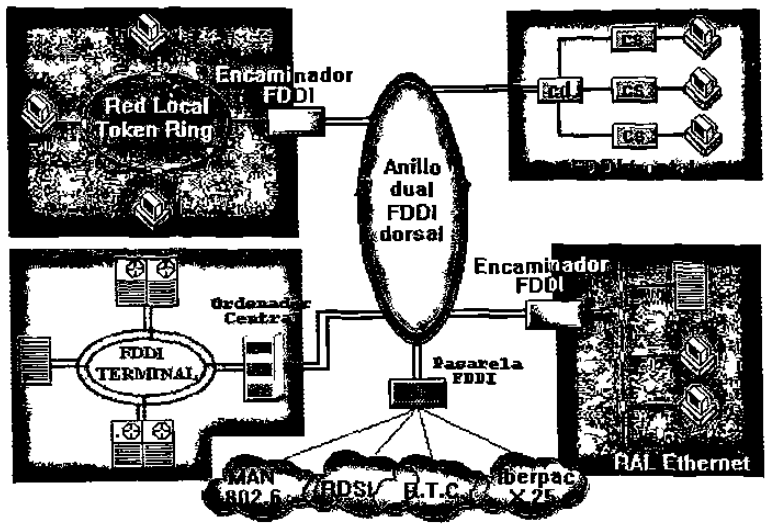


Fig. 3.4 Anillo dual FDDI dorsal.

Servicios ofrecidos

La tecnología FDDI permite utilizar servicios no orientados a conexión, puesto que el método de acceso por paso de testigo temporizado posibilita el envío de datos a la red sin la necesidad de reservar previamente el medio para efectuar la transmisión. Dentro de los servicios prestados se encuentran aplicaciones para tráfico síncrono y asíncrono.

Para el tráfico síncrono, los datos son enviados en modo paquete, indicándose las direcciones de los nodos origen y destino. El retardo máximo de los paquetes es función de los parámetros de temporización del testigo y por tanto se puede cuantificar.

El servicio para aplicaciones que requieren tráfico asíncrono permite el uso de diferentes niveles de prioridad a nivel de paquetes de datos.

El desarrollo de circuitos integrados VSLI que incorporan los diferentes niveles de la norma FDDI, han permitido la rápida introducción de este estándar en el campo de la comunicaciones entre redes de área local. Hoy en día se encuentran productos comerciales (puentes, encaminadores y pasarelas) que permiten dicha interconexión. Así mismo, numerosos fabricantes de ordenadores, están comercializando sus productos con interfaz de conexión hacia redes FDDI.

A pesar de que la tecnología FDDI representa un gran avance en las comunicaciones de área local, algunas de las aplicaciones que se piensa podrá soportar la RDSI (Red Digital de Servicios Integrados) de banda ancha no son susceptibles de circular por redes FDDI. Por ejemplo, la TV de alta definición requerirá un ancho de banda de 150 Mbit/s por canal, lo cual supera el máximo permitido en FDDI.

Para soportar los servicios isócronos, tales como tráfico de voz a 64 Kbits/s, el grupo normalizador FDDI ha desarrollado el estándar FDDI-II que permite trabajar en modo conmutación de circuitos.

3.6 ATM

ATM es un protocolo de transmisión de última generación, cuya sigla corresponde al método denominado Modo de Transferencia Asíncrona.

Básicamente, es la tecnología que administra el ancho de banda asignado a cada una de las señales que circulan por la red, sean éstas voz, datos o imágenes, de manera que el usuario final la reciba en forma integrada.

En el símil de una autopista, vendría a ser el factor que regula el tránsito de miles de vehículos, haciéndolo expedito, rápido y eficaz.

En términos técnicos, ATM consiste en un protocolo en el cual la información a transmitir es almacenada en celdas de 53 bytes de largo, de los cuales 5 se usan en el control de la transmisión y los 48 restantes para el envío de información útil.

La tecnología ATM comprende un tendido físico (cable de cobre, cable coaxial, enlace de microondas, enlace satelital o cable de fibra óptica), elementos de conmutación (switch), concentradores de acceso (HUB), dispositivos de adaptación (routers, codecs, etc), y dispositivos de interfaz (Tarjetas de comunicación, cámaras de vídeo, centrales telefónicas, etc.).

El modo más corriente de acceso a ATM es la fibra óptica, un cable de silicio del grosor de un cabello humano, a través del cual viaja un rayo láser de alta densidad o un haz infrarrojo, el que transmite bits (ceros o unos) mediante una codificación parecida a la del alfabeto Morse.

El protocolo ATM posee una capacidad de transmisión miles de veces superior a la de los medios convencionales, tales como el cable de cobre, el cable coaxial o el enlace satelital.

Para transmitir datos o señales e audio o video sobre un cable de fibra óptica, es necesario digitalizar previamente la señal. De eso se encarga un procesador situado en el interior del dispositivo de interfaz, sea una cámara de vídeo, una central telefónica, etc.

ATM es un protocolo con mínima capacidad de control de errores y de flujo, lo que reduce el coste de procesamiento de las celdas ATM y reduce él numero de bits suplementarios requeridos en cada celda, posibilitando su funcionamiento a altas velocidades. El uso de ATM a altas velocidades se ve apoyado adicionalmente por el empleo de celdas de tamaño fijo, ya que de este modo se simplifica el procedimiento necesario en cada nodo ATM.

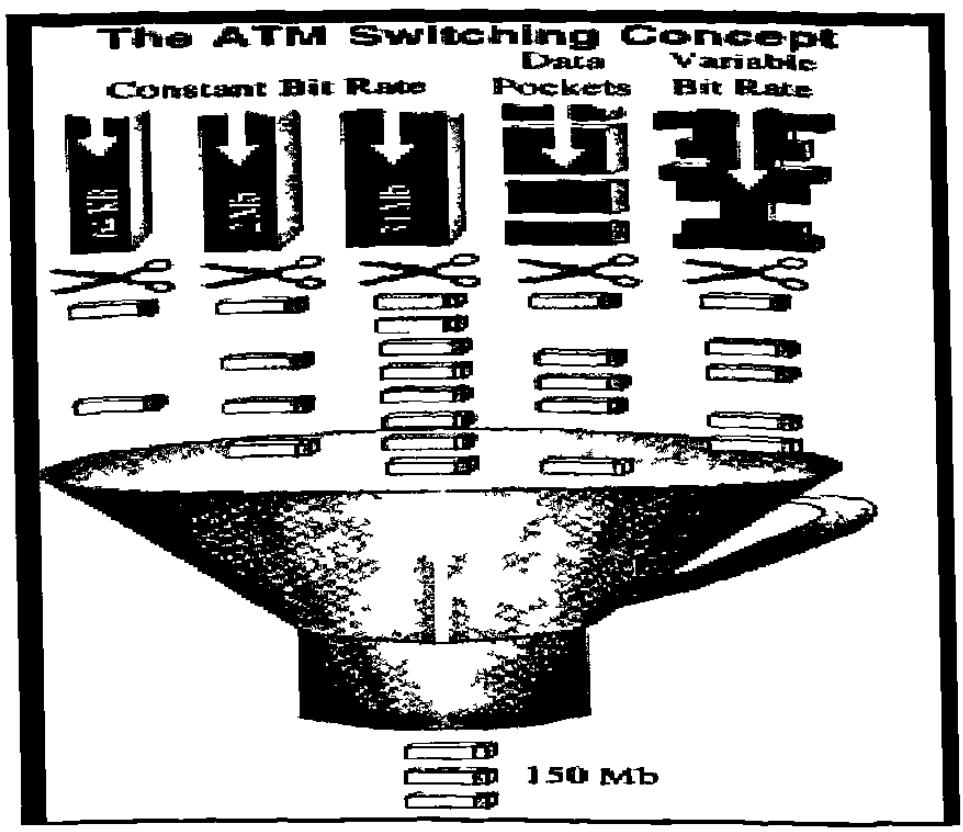


Fig. 3.5 Switch Atm

Las compañías de telecomunicaciones están investigando las conexiones con fibra óptica que atraviesan países y océanos a velocidades de Gigabits/sec, y les gustaría poder transportar en un único camino tanto trafico en tiempo real, como voz e imágenes de vídeo las cuales pueden aceptar algunas perdidas pero no retrasos, como trafico que no sea en tiempo real, como ficheros y datos de ordenadores que pueden aceptar retrasos pero no perdidas. El problema de transportar estos datos con diferentes características en una misma red aparece con el ancho de banda que necesita cada conexión ya que para imágenes de vídeo se requiere un alto ancho de banda por un corto periodo de tiempo y, por ejemplo para transmitir ficheros las necesidades son contrarias. Debido a estas necesidades de ancho de banda, el modo STM (Modo de Transferencia Sincrona) resulta ineficiente y se empieza a pensar en ATM.

Fue propuesto por Bellcore (la parte de AT&T que se dedica a la investigación) en USA y en Europa por varias compañías de telecomunicaciones lo que dará dos posibles standards para ATM. La principal idea fue decir que en vez de identificar una conexión por un numero de cubos, identificar la conexión en cada cubo reduciendo la longitud de estos. Al reducir su longitud, si un cubo es perdido en un momento de congestión, los datos perdidos no son muchos y en algunos casos podrán ser fácilmente recuperados. Esto se precia mucho a la computación de paquetes y se llamo conmutación de paquetes de longitud fija a alta velocidad.

Dos puntos finales en una red ATM están asociados con una vía llamada identificador del camino virtual (VCI) en vez de por un numero de cubos como era el caso de las redes STM. El VCI es transportado en la cabecera de los paquetes por lo que ya no es necesario que lleven una etiqueta como en el caso de STM.

¿Por qué existe actualmente tanto interés acerca de ATM?
Podemos decir cuatro razones principales:

1. ATM se ha originado por la necesidad de un standard mundial que permita el intercambio de información, sin tener en cuenta el tipo de información

transmitida. Con ATM la meta es obtener un standard internacional. ATM es una tecnología que va creciendo y es controlada por un consenso internacional, no por la simple vista o estrategia de un vendedor.

2. Desde siempre, se han usado métodos separados para la transmisión de información entre los usuarios de una red de área local (LAN) y los de una red de gran tamaño (WAN). Esta situación traía una serie de problemas a los usuarios de LAN's que quieran conectarse a redes de área metropolitana, nacional y finalmente mundial. ATM es un método de comunicación que se puede implantar tanto en LAN's como en WAN's. Con el tiempo, ATM intentara que las diferencias existentes entre LAN y WAN vayan desapareciendo.
3. Actualmente se usan redes independientes para transportar voz, datos e imágenes de vídeo debido a que necesitan un ancho de banda diferente. Por ejemplo, él trafico de datos tiende a ser "algo que estalla", es decir, no necesita comunicar por un periodo extenso de tiempo sino transmitir grandes cantidades de información tan rápido como sea posible. Voz y vídeo, por otra parte, tienden a necesitar un trafico mas uniforme siendo muy importante cuando y en el orden en que llega la información. Con ATM, redes separadas no serán necesarias. ATM es la única tecnología basada en estándar que ha sido diseñada desde el comienzo para soportar transmisiones simultaneas de datos, voz y vídeo.
4. ATM es un standard para comunicaciones que esta creciendo rápidamente debido a que es capaz de transmitir a una velocidad de varios Megabits hasta llegar a Gigabit. Tecnología de ATM

La tecnología ATM es basada en poderosas y, flexibles conceptos.

1. Cuando necesitamos enviar información, el emisor "negocia" un camino en la red para que su comunicación circule por él hacia el destino. Una vez asignado el camino, el emisor especifica el tipo, la velocidad y otros atributos de la comunicación.

2. Otro concepto clave es que ATM está basado en el uso de conmutadores. Hacer la comunicación por medio de un conmutador (en vez de un bus) tiene ciertas ventajas:
   - Reserva de ancho de banda para la conexión
   - Mayor ancho de banda
   - Procedimientos de conexión bien definidos
   - Velocidades de acceso flexibles.

Si usamos ATM, la información a enviar es dividida en paquetes de longitud fija. Estos son mandados por la red y el destinatario se encarga de poner los datos en su estado inicial. Los paquetes en ATM tienen una longitud fija de 53 bytes. Siendo la longitud de los paquetes fija, permite que la información sea transportada de una manera predecible. El hecho de que sea predecible permite diferentes tipos de trafico en la misma red.

Los paquetes están divididos en dos partes, la cabecera y payload. El payload (que ocupa 48 bytes) es la parte del paquete donde viaja la información, ya sean datos, imágenes o voz. La cabecera (que ocupa 5 bytes) lleva el mecanismo direccionamiento.

ATM tiene bastantes beneficios:

- Una red para todo tipo de trafico.
- Capacita nuevas aplicaciones.
- Compatibilidad con las actuales redes físicas.
- Incrementa la capacidad de migración.
- Simplifica el control de la red.
- Largo periodo de vida de la arquitectura.

1. Una única red ATM dará cabida a todo tipo de trafico (voz, datos y vídeo). ATM mejora la eficiencia y manejabilidad de la red.
2. Capacita nuevas aplicaciones debido a su alta velocidad y a la integración de los tipos de tráfico, ATM capacitara la creación y la expansión de nuevas aplicaciones como la multimedia.

3. Compatibilidad-porque ATM no esta basado en un tipo especifico de transporte físico, es compatible con las actuales redes físicas que han sido desplegadas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.
4. Simplifica el control de la red ATM esta evolucionando hacia una tecnología standard para todo tipo de comunicaciones. Esta uniformidad intenta simplificar el control de la red usando la misma tecnología para todos los niveles de la red.
5. Largo periodo de vida de la arquitectura Los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizado el ATM. ATM ha sido diseñado desde el comienzo para ser flexible en:
   - Distancias geográficas
   - Numero de usuarios
   - Acceso y ancho de banda(hasta ahora, las velocidades varían de Megas a Gigas).

¿Dónde se encuentra ATM?

ATM a pasado de la teoría a la realidad con productos y servicios disponibles hoy en día. EL ATM forum ha patrocinado demostraciones de interoperatibilidad para demostrar la tecnología y continua reuniéndose para discutir sobre la evolución de ATM.

EL ATM coexiste con la actual tecnología LAN/WAN. Las especificaciones de ATM están siendo descritas para asegurar que el ATM integre las numerosas tecnologías de red existentes, a varios niveles (ie, Frame Relay, Ethernet, TCP/IP).

Equipos, servicios y aplicaciones están disponibles hoy en día y están siendo actualmente usadas en redes.

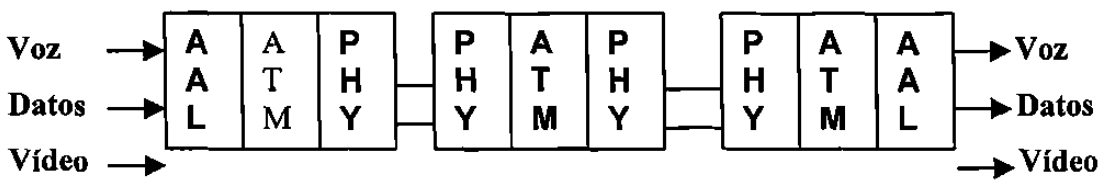
La industria de la telecomunicación se dirige al ATM.

ATM FORUM

El ATM Forum se inicio en octubre de 1991 un conjunto de 4 empresas de ordenadores y telecomunicaciones. Desde su comienzo, ha visto un crecimiento sin precedentes, hasta (jun. 1994) tiene alrededor de 500 miembros. Los actuales miembros están agrupados en proveedores el equipo, los que fabrican los conductores, los proveedores de servicio, los transportadores y los usuarios finales.

El ATM Forum es un consorcio de compañías que escribe especificaciones para acelerar la definición de la tecnología ATM. Estas especificaciones son luego pasadas al ITU-T(lo que era antes CCITT Comite Consultivo Internacional de Telefonia y Telegrafia) para su aprobación. El ITU-T reconoce Totalmente el ATM Forum como un grupo de trabajo creíble.

Arquitectura de ATM (Fig. 3.6).



- (AAL): Capa de Adaptación: Inserta y extrae la información del payload.
- (ATM): Adhiere y remove los 5 bytes del header
- (PHY): Convierte a un apropiado formato eléctrico o óptico.

ATM es una arquitectura estructurada en capas (Fig. 3.7) que permite que múltiples servicios como voz y datos vayan mezclados en la misma red. Tres de las capas han sido definidas para implementar los rasgos del ATM.

La capa de adaptación garantiza las características apropiadas del servicio y divide todos los tipos de datos en payload de 48 bytes que conformaran el paquete ATM.

La capa intermedia de ATM coge los datos que van a ser enviados y añade los 5 bytes de la cabecera que garantiza que el paquete se envía por la conexión adecuada.

La capa física define las características eléctricas y las interfaces de la red. ATM no esta ligado a un tipo especifico de transporte físico.

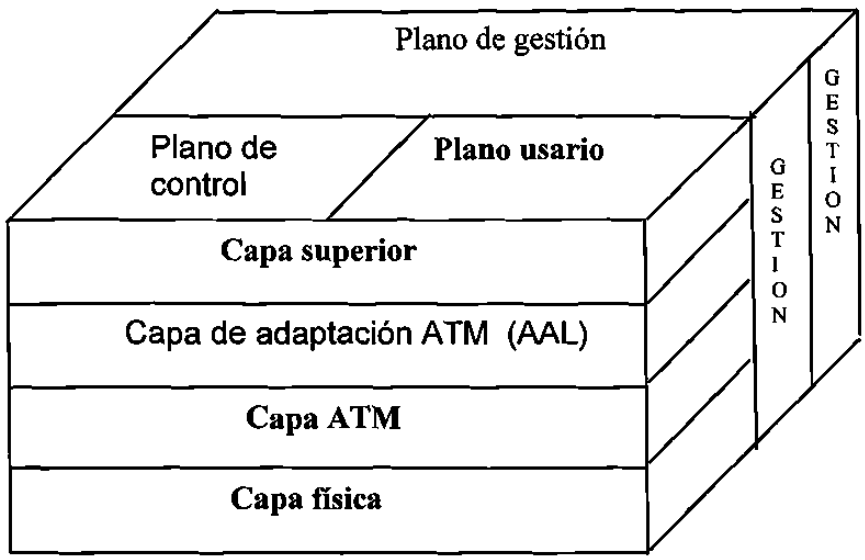


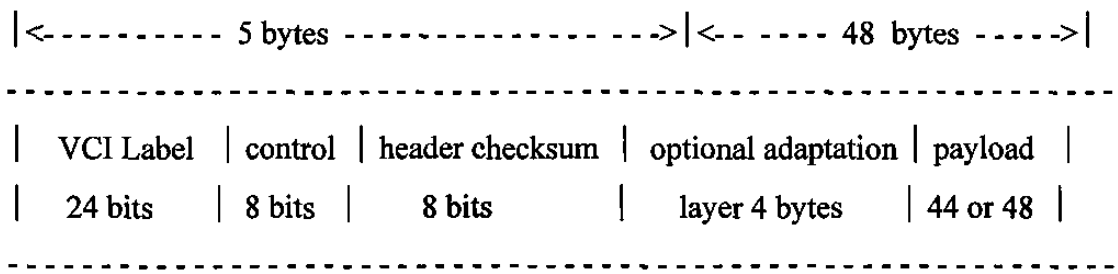
Fig. 3.7 Modelo de referencia del protocolo ATM.

El modelo de referencia del protocolo hace mención a tres planos separados:

- Plano de Usuario: permite la transferencia de información de usuario, y hace uso de controles (control de flujo y de errores).
- Plano de Control: realiza el control de llamadas y las funciones de control de conexión.
- Plano de Gestión: incluye gestión de plano, que realiza funciones de gestión relacionadas con un sistema como un todo y proporciona la coordinación entre todos los planos, y gestión de capa, que realiza funciones de gestión relativas a los recursos y a los parámetros residentes en las entidades del protocolo.

Paquetes de ATM

La longitud de los paquetes en ATM es de 53 bytes. Los primeros 5 bytes corresponden a la cabecera y los restantes 48 al payload:

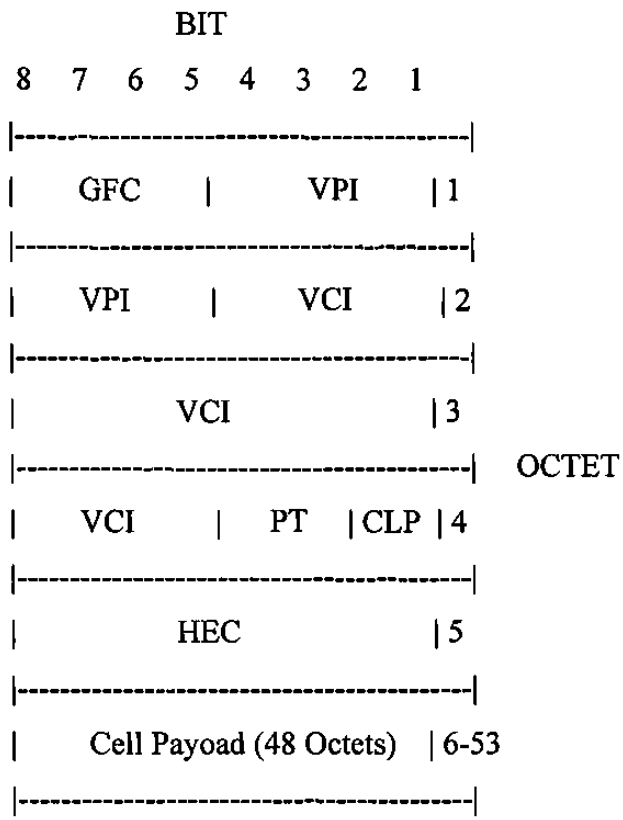


Los 48 bytes del payload pueden contener 4 bytes indicando la capa de adaptación y los 44 bytes o los 48 bytes restantes llevando datos. Esto se especificara con un bit que se encuentra en el campo de control de la cabecera. El campo de control donde la cabecera también contiene un bit que indica si el paquete es de control o es un paquete normal y también posee otro bit para indicar si el paquete se puede eliminar en caso de congestión o no.

Estructura de Un Paquete ATM

ATM UNI Cell Structure

La siguiente figura 3.8 corresponde a la estructura de un paquete de ATM:



CFC - Generic Flow Control

VCI - Identificador del canal virtual

CLP - Celda de Baja Prioridad

VPI - Identificador del camino virtual

PT - Tipo de Payload

HEC - Control de error en la cabecera

Fig. 3.8 Paquete de ATM.

Un paquete en ATM es la información básica transferida en las comunicaciones B-ISDN de ATM. Los paquetes tienen una longitud de 53 bytes. Cinco de estos bytes forman la cabecera y los 48 bytes que quedan forman el campo de información del usuario llamado "payload". La siguiente estructura corresponde a la cabecera de un paquete **NNI (Interfaz red – red)** (Fig. 3.9):

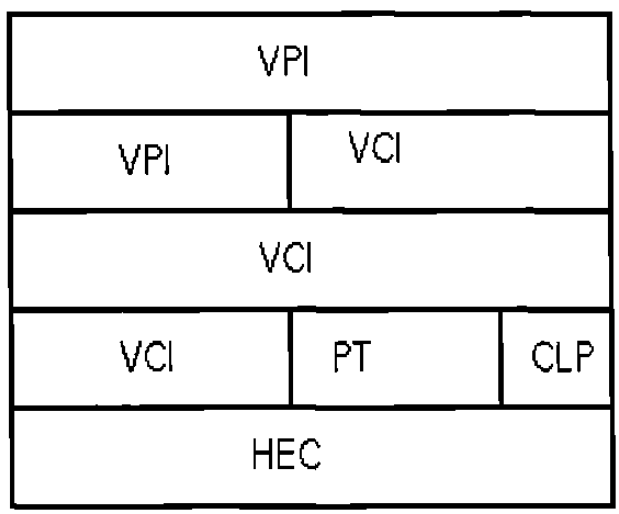


Fig. 3.9 Cabecera de un paquete NNI.

La siguiente estructura corresponde a la cabecera de un paquete **UNI(interfaz usuario – red) (Fig. 3.10)**:

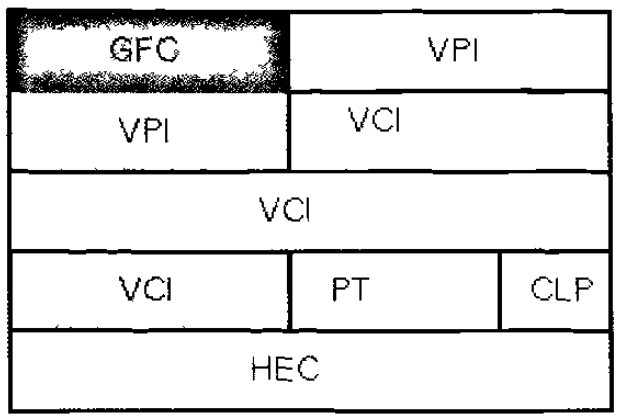


Fig. 3.10 Cabecera de paquete UNI.

La cabecera se divide en los campos GFC, VPI, VCI, PT, CLP y HEC. Los tamaños de estos campo difieren mínimamente entre el NNI y el UNI. Los tamaños de los campos son los siguientes:

Control de Flujo Genérico (GFC):

Aunque la función primaria de este campo es el control del acceso físico, a menudo se usa para reducir celda en servicios CBR, asigna capacidad de feria para servicios VBR, y para hacer control de trafico en flujos VBR.

Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI):

La función de los campos VPI/VCI es indicar él numero de canal/camino virtual, por lo cual los paquetes que pertenezcan a la misma conexión pueden ser distinguidos.

Se asigna un único VPI/VCI para indicar el tipo de paquete que viene, paquetes sin asignar, paquetes OAM de la capa física.

Tipo de Payload (PT)

El campo **PT** deberá informar si la información del usuario ha llegado o los paquetes ATM han sufrido congestión.

Cell de Baja Prioridad (Cell Loss Priority) (CLP)

El campo **CLP** se usa para decir al sistema si el paquete debe ser descartado o no en momentos de congestión. Los paquetes ATM con CLP= 0 tienen una prioridad menor que los paquetes ATM con CLP= 1. Por lo tanto, cuando se produce congestión, los paquetes que tienen el campo CLP= 1 antes son quitados antes que los que tienen el campo CLP= 0.

Header Error Control(HEC):

HEC es un byte de CRC de la cabecera que es usado para detectar y corregir errores en los paquetes.

La Capa Fisica

Las especificaciones de la capa física no son una parte de la definición de ATM pero los comités la consideran como si lo fuera: T1S1 ha estandarizado en SONET la capa física preferida y la clasificación STS hace referencia a las velocidades de las conexiones de SONET (ejem. STS –3c soporta 155.5 Mbit/sec, STS – 12 soporta 622

Mbit/sec, y STS-48 soporta 2.4 Gbit/sec) siendo posibles velocidades superiores e inferiores.

El SDH especifica como los paquetes son estructurados y transportados sincronamente a lo largo de conexiones de fibras ópticas.

Control de trafico en ATM

Una red ATM necesita tener unas capacidades para controlar él trafico dando cabida a las distintas clases de servicios y a supera posibles errores que se pueden producir dentro de la red en cualquier tiempo (ejem. Un problema con la capa física). La red tiene que tener las siguientes capacidades para controlar él trafico.

- Recursos de dirección de la red.
- Control de admisión de una conexión.
- Uso de parámetros de control y de parámetros de control de red.
- Control de Prioridad.
- Control de Congestión.

Procedimientos De Control De Trafico Y Su Impacto En La Direccion De La Red

Los procedimientos de control de trafico en redes ATM actualmente no están completamente estandarizados. Pero la meta de estos procedimientos es:

- Conseguir una buena eficiencia en la red.
- Dar calidad al servicio requerido por el usuario.

Con un método que es generalmente aplicable. Por lo tanto, unos controles de tráfico mas sofisticados y unas acciones para los recursos de la red están siendo tenidas en cuenta.

El problema fundamental en las redes ATM es los comportamientos de los paquetes en los procesos de llegada. Se ha visto que la calidad del servicio depende

mucho de este comportamiento. Por lo tanto, es necesario usar modelos de trafico para evaluar la ejecución.

Recursos de dirección de la red

Un instrumento de recurso de dirección de la red que puede ser usado para el control de tráfico es la técnica de los caminos virtuales. Agrupando varios canales virtuales un camino virtual, otras formas de control pueden ser simplificadas (ejem. Cac y upc). Los mensajes para el control de tráfico pueden ser mas fácilmente distribuidos en un canal virtual que estará dentro de un camino virtual.

Control de admisión de una conexión

El control de admisión de una conexión es la colección de acciones tomadas por la red durante la fase de instalación para establecer si un camino/canal virtual puede ser aceptado por la red.

Una conexión sola puede ser establecida si los recursos disponibles de la red son suficientes para establecer la conexión con la calidad que requiere el servicio. La calidad de servicio de los canales existentes no debe ser afectada por la nueva conexión.

Dos clases de parámetros están previstos para mantener el control de admisión de una conexión:

- Un conjunto de parámetros que describen las características del trafico en el origen.
- Otro conjunto de parámetros para identificar la calidad que el servicio requiere.

El control de admisión de conexión es la primera línea de defensa de autoprotección de la red ante una carga excesiva. En esencia, cuando un usuario solicita una nueva VCC o VPC, debe especificar (implícita o explícitamente) las características de tráfico para la conexión en ambas direcciones.

Parámetros de tráfico usados en la definición de calidad de servicio de vcc/vpc.

Parámetro	Descripción	tipo de tráfico
Velocidad de pico de celdas (PCR)	Límite superior de tráfico que puede Presentarse en una conexión ATM.	CBR, VBR
Variación del retardo de celdas (CDV)	Límite superior de la variabilidad en El patrón en recepción de celdas Observado en un único punto de De medida en referencia a la Velocidad de pico de celdas.	CBR, VBR
Velocidad sostenible de celdas (SCR)	Límite superior de la velocidad Promedio de una conexión ATM, Calculado sobre la duración de una Conexión.	VBR
Tolerancia a la aparición de ráfagas	Límite superior de la variabilidad en El patrón de recepción de celdas observando en un único punto de medida en referencia a la velocidad sostenible de celdas.	

Uso de parámetros de control Y parámetros de control de la red

El uso de parámetros de control (UPC) y los parámetros de control que tiene la red (NPC) hacen la misma función en diferentes interfaces. La función de los UPC es desarrollada en las interfaces del usuario, mientras que la función de los NPC se realiza en los nodos de la red.

El propósito principal de los UPC/NPC es de proteger los recursos de la red ya que puede llegar a afectar la calidad de servicio de otra conexión ya establecida.

El uso de parámetros supervisores incluye las siguientes funciones:

- Verificar la validez de los valores de los VPI/VCI.
- Supervisión del volumen de tráfico de la red.
- Supervisión de todo el volumen de tráfico aceptado en un nuevo acceso.

El uso de parámetros de control puede simplificar el rechazo de paquetes que llevan errores en sus parámetros de tráfico. Una medida menos rigurosa puede consistir en marcar los paquetes erróneos y dejarlos en la red si no causan daño.

Control de prioridad

Los paquetes de ATM tienen un bit de prioridad de perdida en la cabecera del paquete así el cual puede tomar por lo menos dos valores diferentes. Una conexión sencilla de ATM puede tener ambos valores cuando la información transmitida esta clasificada en partes mas o menos importantes.

Control de congestión

El control de congestión es un estado de los elementos de la red en el cual él trafico sobrepasa los recursos de la red y esta no es capaz de garantizar la calidad de los servicios a las conexiones establecidas.

El control de congestión es un medio de minimizar los efectos de la congestión impidiendo que estos se propaguen. Pueden emplear CAC y/o UPC para evitar situaciones de congestión.

Canales y Caminos Virtuales

ATM provee dos tipos de conexiones para el transporte de datos: Caminos virtuales y Canales virtuales.

Un canal virtual es una tubería unidireccional formado por la suma de una serie de elementos de la conexión. Un camino virtual esta formado por la suma de una serie de elementos de la conexión. Un camino virtual esta formado por una conexión de estos canales.

Cada camino y cada canal tienen un identificador asociado. Todos canales dentro de un camino sencillo tienen que tener un identificador de canal distinto pero pueden tener el mismo identificador de canal si viajan en caminos diferentes. Un canal individual puede por lo tanto ser inequívocamente identificado por su numero de canal virtual y por él numero de camino virtual.

El número de canal y camino virtual de una conexión puede diferir del origen al destino si la conexión se conmuta dentro de la red. Los canales virtuales que queden dentro de un camino virtual sencillo en una conexión tendrán los mismos identificadores de canales virtuales. La secuencia de paquetes es mantenida a través de un canal virtual. Cada canal y camino virtual han negociado un QOS asociado. Este par metro incluye valores para controlar la perdida y retardo de paquetes.

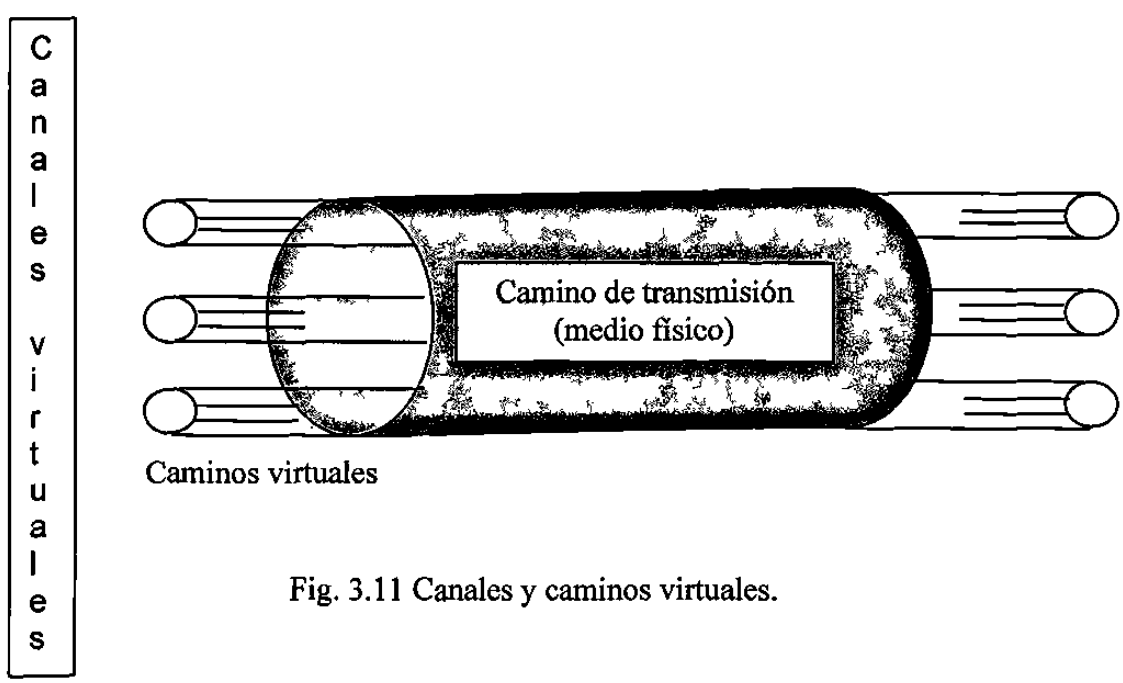


Fig. 3.11 Canales y caminos virtuales.

El concepto de camino virtual se desarrolló en respuesta a una tendencia en redes de alta velocidad en la que el costo de control está alcanzado una elevada proporción del costo total de la red.

El uso de caminos virtuales presenta varias ventajas:

- Arquitectura de red simplificada: las funciones de transporte de red pueden ser diferenciadas en las relativas a una conexión lógica individual (canal virtual) y en aquellas relacionadas con un grupo de conexiones lógicas (camino virtual.
- Incremento en eficiencia y fiabilidad: la red gestiona entidades agregadas menores.
- Reducción en el procesamiento, y tiempo de conexión pequeño: gran parte del trabajo se realiza cuando se establece el camino virtual. Reservando capacidad en un camino virtual con anticipación a la llegada de llamadas posteriores, se pueden establecer nuevos canales virtuales con funciones de control sencillas realizadas en los extremos del camino virtual.
- Servicios de red mejorados: el camino virtual se usa internamente a la red y es también visible al usuario final. Así, el usuario puede definir grupos de usuarios cerrados o redes cerradas de haces de canales virtuales.

Conexión de un canal/camino virtual:

Existen cuatro formas en que un canal/camino virtual pueden sé instalados.

1) El canal/camino virtual se puede reservar con la red como en el caso de conexiones permanentes o semipermanentes.
2) Una nueva conexión puede ser instalada por medio de procedimientos de señalamiento a través de un canal de señalamiento virtual.
3) Una conexión puede ser instalada como el resultado de un procedimiento de señales hechas por el usuario.
4) Una nueva conexión de un canal virtual puede ser instalada dentro de una conexión de camino virtual existente entre dos nodos de la red.

Durante la instalación el usuario negocia un QOS con la red y los parámetros de trafico son configurados.

Relación entre ATM y B-ISDN

Se puede resumir en una frase: ATM hace posible el B-ISDN en una realidad. Esto no nos da una idea acertada de la relación: El ISDN (Integrated Services Digital Network) se desarrollo durante los 80's. Tomo una canal básico que podía operar a 64kbps (canal B) y combinaciones de otros (canales D) para formar la base para las redes de comunicaciones.

Sin embargo, al mismo tiempo, la demanda de comunicaciones a alta velocidad (FDDI LAN y DQDB LAN) y comunicaciones de vídeo aumentaba rápidamente.

Por esto se creo Broadband-ISDN la cual solo es una extensión de ISDN por lo cual las funciones de comunicaciones entre redes, vídeo teléfono, videoconferencia, etc., son tratadas como en el ISDN tradicional. Esta diversidad de servicios precisan unas velocidades de 155Mbps, 622Mbps y 2.4Gbps y unas determinadas transmisiones y conexiones para esas velocidades. Mientras que SDH se usaba para las transmisiones, la conmutación de paquetes apareció como la solución al problema de las conexiones.

Las conexiones para broadband no son sencillas de realizar debido a la necesidad unos anchos de banda de varias decenas de bps que pueden llegar a 100 Mbps para transmitir ciertas señales. Esto nos puede llevar entre varios segundos a varias horas. Como ATM resuelve estos problemas, B-ISDN pueden existir como una realidad y llegar a ser implementado en un futuro en redes.

Emulación de redes LAN ATM

Un ejemplo de una LAN ATM núcleo que incluye enlaces hacia el mundo exterior. En este ejemplo, la red ATM local consta de cuatro conmutadores

interconectados con enlaces punto a punto de alta velocidad operando a las velocidades de transmisión de datos estándares de 155 y 622 Mbps. En la configuración preexistente hay otras tres redes LAN, cada una de ellas con una conexión directa a uno de los conmutadores ATM. La velocidad de transmisión de datos desde un conmutador ATM conectado a una LAN se ajusta a la velocidad de datos de esta LAN.

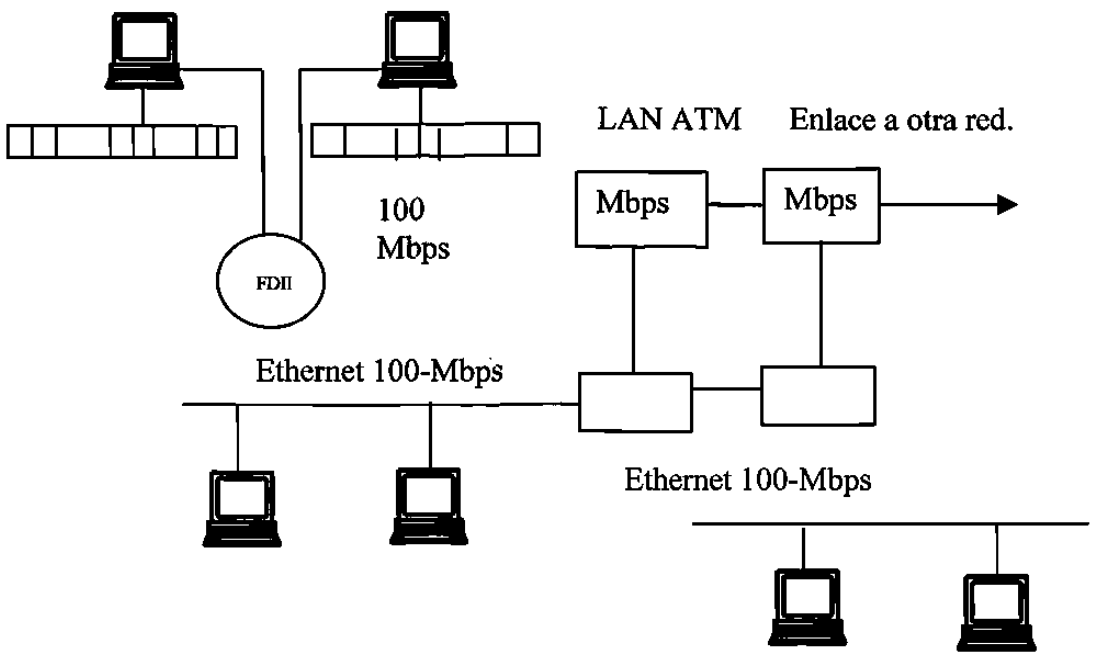


Fig. 3.12 Configuración de red LAN ATM

Arquitectura del Protocolo

La arquitectura del protocolo involucrado en la emulación de redes LAN ATM.

En este caso vemos la interacción de un sistema de conexión ATM con un sistema final conectado a una LAN tradicional. El puente lógico debe ser capaz de convertir tramas MAC en celdas ATM y viceversa. Ésta es una de las funciones clave en la emulación de redes LAN ATM.

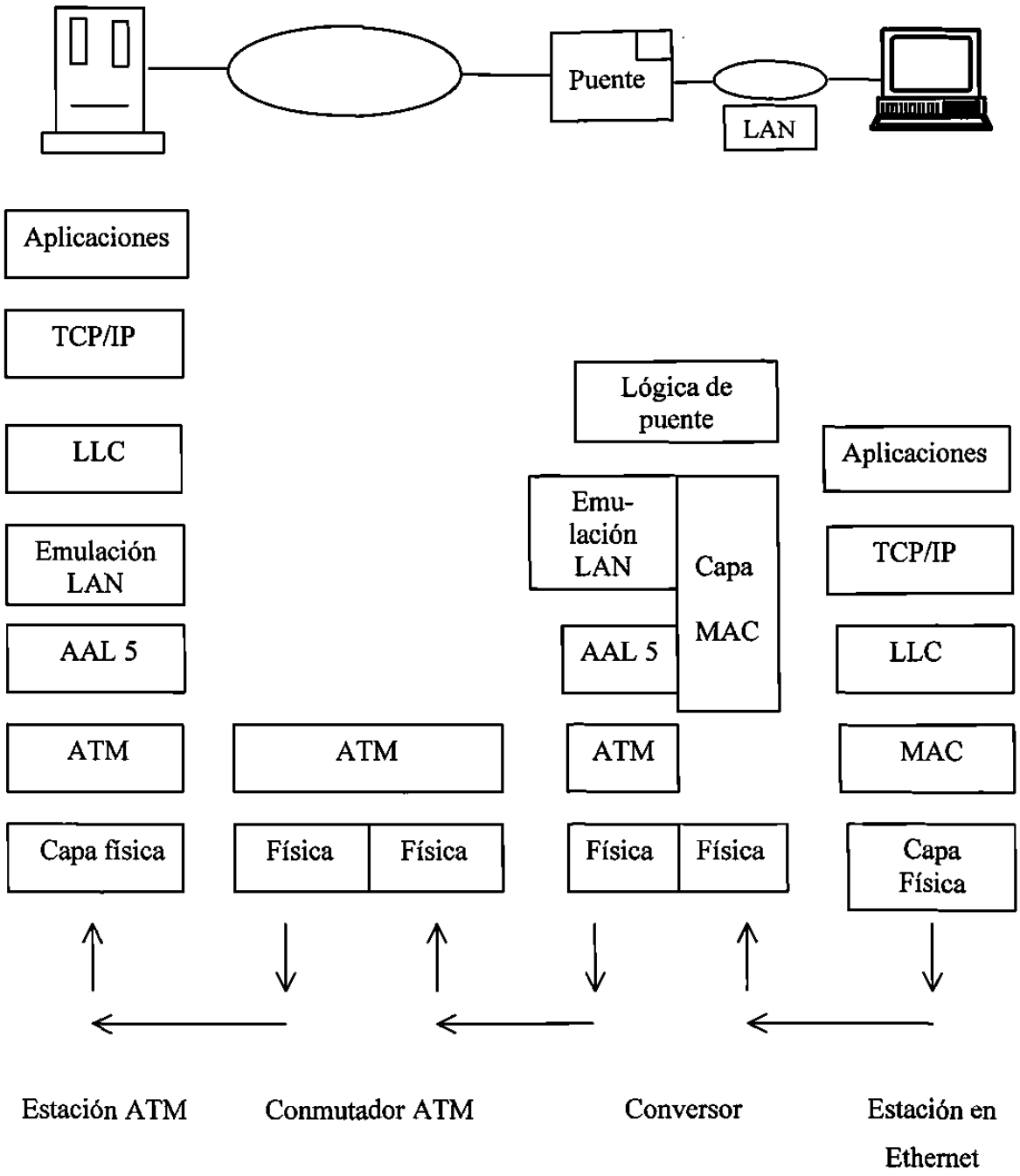


Fig. 3.13 Arquitectura del protocolo.

Redes LAN emuladas

Es posible configurar varias LAN emuladas lógicamente independientes. Una LAN emulada admite un único protocolo MAC, del que se encuentran definidos actualmente des tipos: Ethernet/IEEE 802.3 y IEEE 802.5 (anillo con paso de testigo). Una LAN emulada consta de una combinación de:

- Sistemas finales en una o más LAN tradicionales.
- Sistemas finales conectados directamente a un conmutador ATM.

Cada sistema final en una LAN emulada debe tener una única dirección MAC. El intercambio de datos entre los sistemas finales a través de la misma LAN emulada involucra el uso del protocolo MAC, y es transparente a las capas superiores.

La capa de adaptación de ATM:

AAL - Para que con ATM se soporten varios tipos de servicios con diferentes características y requerimientos de sistema, se necesita algo para adaptar las diferentes clases de aplicaciones a la capa intermedia de ATM. Esta función es desarrollada por AAL. Cuatro tipos de AAL eran originalmente recomendados por CCITT. Dos de estos (3 y 4) han sido unidos en uno (como se muestra en la tabla 3.4).

	Clase A	Clase B	Clase C	Clase D
Relación de temporización entre el origen y el destino	Requerido		Requerido	
		Variable		
Tasa de bits	Constante			
Modo de conexión	Orientado a conexión			No orientad a conexión
Protocolo AAL	Tipo 1	Tipo 2	Tipo3/4 Tipo 5	Tipo 3/4

Tabla 3.4 Tipos de AAL.

AAL1 - Soporta los servicios orientados a conexión que requieren tasas constantes de bits y tiene unos requerimientos de tiempo y retardo específicos.

AAL2 - Soporta los servicios orientados a conexión que no requieren tasas constantes de bits. En otras palabras, aplicaciones con tráfico variable.

AAL3/4 - Este AAL satisface los servicios que requieren una tasa de bits variable y son orientados a conexión así como los que no son orientados a conexión. Originalmente existían el **AAL3** y **AAL4** pero han sido unidos en uno solo cuyo nombre pasa a ser **AAL3/4.**

ALL5 - Soporta servicios orientados a conexión que requieren una tasa de bits variable.

La capa de Adaptación de ATM yace entre el ATM layer y las capas mas altas que usan el servicio ATM. Su propósito principal es el de resolver cualquier disparidad entre un servicio requerido por el usuario y atiende los servicios disponibles del ATM layer. La capa de adaptación introduce la información en paquetes ATM y controla los

errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

1) Que la información que esta siendo transportada dependa o no del tiempo.
2) Tasa de bit constante/variable.
3) Modo de conexión.

Estas propiedades definen ocho clases posibles, cuatro se definen como B-ISDN Clases de servicios. La capa de adaptación de ATM define 4 servicios para equiparar las 4 clases definidas por B-ISDN:

AAL-1

AAL-2

AAL-3

AAL-4

La capa de adaptación se divide en dos subcapas:

1) Capa de convergencia .

En esta capa se calculan los valores que debe llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.

2) Capa de Segmentación y reensamblaje:

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

AAL1:

AAL-1 se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada.

Capa de convergencia:

Las funciones provistas a esta capa difieren dependiendo del servicio que se proveyó. Provee la corrección de errores.

Capa de segmentación y reensamblaje:

En esta capa los datos son sementados y se les añade una cabecera. La cabecera contiene 3 campos (ver diagrama).

Número de secuencia usado para detectar una inserción o perdida de un paquete. Número de secuencia para la protección usado para corregir errores que ocurren en él numero de secuencia. Indicador de capa de convergencia usado para indicar la presencia de la función de la capa de convergencia.

ALL 2

AAL-2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse.

Capa de convergencia

Esta capa provee para la corrección de errores y transporta la información del tiempo desde el origen al destino.

Capa de segmentación y recuperación:

El mensaje es segmentado y se le añade una cabecera a cada paquete. La cabecera contiene dos campos.

Número de secuencia que se usa para detectar paquetes introducidas o perdidas. El tipo de información es:

- BOM, comenzando de mensaje
- COM, continuación de mensaje
- EOM, fin de mensaje

O indica que el paquete contiene información de tiempo u otra.

El payload también contiene dos de campos:

Indicador de longitud que indica él numero de bytes validos en un paquete parcialmente lleno.

CRC que es para hacer el control de errores.

AAL 3

AAL-3 se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL-3 puede ser dividido en dos modos de operación:

1) **Fiable:** En caso de perdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.
2) **No fiable**: La recuperación del error es dejado para capas mas altas y el control de flujo es opcional.

Capa de convergencia

La capa de convergencia en AAL 3 es parecida al ALL 2. Esta subdividida en dos secciones:

1)Parte común de la capa de convergencia. Esto es provisto también por el AAL-2 CS. Añade una cabecera y un payload a la parte común.

La cabecera contiene 3 campos:

- Indicador de la parte común que dice que el payload forma parte de la parte común.
- Etiqueta de comienzo que indica el comienzo de la parte común de la capa de convergencia.
- Tamaño del buffer que dice al receptor el espacio necesario para acomodar el mensaje.

El payload también contiene 3 campos:

Alineación es un byte de relleno usado para hacer que la cabecera y el payload tengan la misma longitud. Fin de etiqueta que indica el fin de la parte común del CS(capa de convergencia). El campo de longitud tiene la longitud de la parte común del CS.

2) Parte especifica del servicio. Las funciones proveídas en esta que capa dependen de los servicios pedidos. Generalmente se incluyen funciones para la recuperación y detección de errores y puede incluir también funciones especiales.

Capa de segmentación y reensamblaje.

En esta capa los datos son partidos en paquetes de ATM. Una cabecera y el payload que contiene la información necesaria para la recuperación de errores y reensamblaje se añaden al paquete. La cabecera contiene 3 campos:

1) Tipo de segmento que indica que parte de un mensaje contiene en payload. Tiene uno de los siguientes valores:

BOM: Comenzando de mensaje.

COM: Continuación de mensaje.

EOM: Fin de mensaje.

SSM: Mensaje cinco en el segmento.

2) Número de secuencia usado para detectar una inserción o una perdida de un paquete.

3) Identificador de multiplexacion. Este campo se usa para distinguir datos de diferentes comunicaciones que ha sido multiplexadas en una única conexión de ATM.

El payload contiene dos de campos:

1) Indicado de longitud que indica el número de bytes útiles en un paquete parcialmente lleno.

2) CRC es para el control de errores.

ALL 4:

AAL-4 se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y o fiable. AAL-4 provee la capacidad de transferir datos fuera de una conexión explícita.

AAL5

El estudio del AAL de tipo 5, cada vez más popular, especialmente para aplicaciones ATM en LAN. Este protocolo se introdujo para ofrecer un transporte eficiente para protocolos de capas superiores orientados a conexión.

AAL tipo 5 se introdujo con los siguientes fines:

- Reducir el coste suplementario de procesamiento del protocolo.
- Reducir la transmisión suplementaria.
- Asegurar la adaptabilidad a los protocolos existentes.

CAPÍTULO 4

RED DE TELECOMUNICACIONES EN LA UANL

4.1 INTRODUCCIÓN

La red de telecomunicaciones de la UANL esta formada por un sistema integral de comunicaciones que provee a las dependencias y facultades de la UANL los servicios de Transmisión de Datos, Internet, Telefonía Digital y Videoconferencia manteniendo al más alto nivel en el manejo de información.

La red de la UANL esta formada por:

- La red de transmisión de datos.
- La red de telefonía digital.
- La red de videoconferencia.

4.2 INFRAESTRUCTURA

La UANL cuneta con varios Campus educativos interconectados con diferentes medios de transporte de información utilizando tecnología de vanguardia que a continuación se enuncian:

- 400 Km de cableado de fibra óptica entre facultades y dependencias de los principales Campus (Cd Universitaria, Biblioteca Raúl Rangel Frias, Unidad Mederos y Campus Salud).

- 4 enlaces metropolitanos de microondas digital (4 E1 por cada enlace) para satisfacer los servicios de voz, datos y video de los Campus Universitarios.
- 1 enlace internacional E1 a UUNET para el servicio a Internet.
- Un enlace E1 a Avantel MCI para el servicio a Internet.
- ISDN de Telmex y Avantel para los servicios de videoconferencia.
- Infraestructura de conexión por módem para la comercialización de Internet.

4.3 TOPOLOGIA

- 4 Campus cada uno con un Backbone de FDDI que une a todas las facultades y dependencias de cada uno de los diferentes Campus de la red UANL para el Área Académica.
- Un Backbone de FDDI para el complejo de edificios de Rectoria para el Área Administrativa.
- Redes locales tributarias de FDDI y Ethernet.
- Enlaces de microondas digital a los 4 Campos Universitarios.

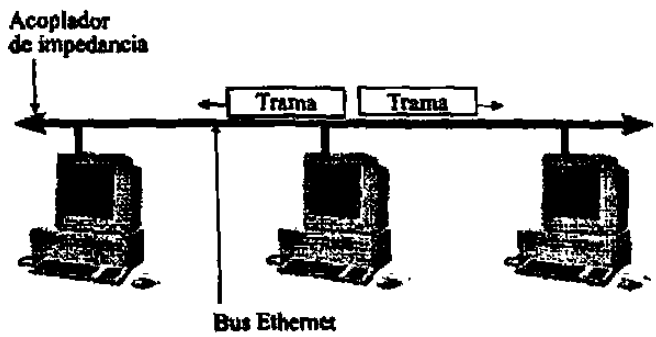
4.4 TECNOLOGIAS INVOLUCRADAS

4.4.a Ethernet.

La norma IEEE 802.3 define un modelo de red de área local utilizando el protocolo de acceso al medio CSMA/CD con persistencia de 1, es decir, las estaciones están permanentemente a la escucha del canal y cuando lo encuentran libre de señal efectúan sus transmisiones inmediatamente (1-persistente). Esto puede llevar a una colisión que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio y vuelvan a intentarlo.

IEEE 802.3 tiene su predecesora en el protocolo ALOHA; posteriormente, la compañía XEROX construyó una red CSMA/CD de casi 3 Mbps de velocidad de

transferencia. denominada Ethernet, que permitía conectar hasta 100 estaciones a lo largo de un cable de 1 km de longitud. En una fase posterior, las compañías DEC (Digital Equipment Corporation) e Intel, junto con Xerox, definieron un estándar para Ethernet de 10 Mbps (Figura 4.1) en la que está basada la norma IEEE 802.3 que nos ocupa.



Fig, 4.1 Estándar para Ethernet de 10 Mbps.

4.4.b FDDI.

FDDI significa por sus siglas en inglés Interface de Datos Distribuidos por Fibra óptica, el FDDI fué desarrollado bajo las reglas del American National Institute (ANSI)

Con el FDDI se cuenta Con una solución estándard para compañias que necesitan de una red flexible, robusta y de alto rendimiento con equipos de diversas marcas.

Es una tecnología de comunicaciones basada en estándares que ofrece:

- Interoperabilidad.
- Mayor velocidad (100 Mbps).
- Crecimiento transparente.
- Implementación a nivel físico.
- Soporte de aplicaciones con uso intensivo de la red.
- Soporte de aplicaciones con uso intensivo de la red.
- Soporte de áreas geográficas muy amplias.

- Mayor seguridad para la red.
- Arquitectura con tolerancia de fallas.

El uso de FDDI nos proporciona como usuarios lo siguiente:

- Incremento en el numero de usuarios de la red.
- Gran expresión de las redes distribuidas.
- Estaciones de trabajo mas poderosas.
- Aumento de redes tipo cliente-servidor.
- Backbones tradicionales casi saturados.
- Incremento en la capacidad y rendimiento de la red.
- Alta disponibilidad.
- Mayores distancias y mayor seguridad.
- Rendimiento determinado.

4.5 MEDIOS DE TRANSMISION

4.5.a Cables trenzados.

Constituyen el modo más simple y económico de todos los medios de transmisión. Sin embargo, presentan una serie de inconvenientes. en todo conductor, la resistencia eléctrica aumenta al disminuir la sección del conductor, por lo que hay que llegar a un compromiso entre volumen y peso, y la resistencia eléctrica del cable. Esta última está afectada directamente por la longitud máxima. Cuando se sobrepasan ciertas longitudes hay que recurrir al uso de repetidores para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, si no están apantallados, son muy sensibles a interferencias y diafonías producidas por la inducción electromagnética de unos conductores en otros (motivo por el que en ocasiones percibimos conversaciones telefónicas ajenas a nuestro teléfono). Un cable apantallado es aquel que está protegido de las interferencias eléctricas externas, normalmente a través de un conductor eléctrico externo al cable, por ejemplo una malla.

Un modo de subsanar estas interferencias consiste en trenzar los pares de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos. Esta es la razón por la que este tipo de cables se llaman de pares trenzados. Con este tipo de cables es posible alcanzar velocidades de transmisión comprendidas entre 2 Mbps y 100 Mbps en el caso de señales digitales.

Es el cable más utilizado en telefonía y télex. Existen dos tipos fundamentalmente:

Cable UTP.

UTP son las siglas de Unshielded Twisted Pair. Es un cable de pares trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente, o incluso impidiendo, la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios. En la Figura 1 se pueden observar los distintos pares de un cable UTP.

Cable STP.

STP son las siglas de Shielded Twisted Pair. Este cable es semejante al UTP pero se le añade un recubrimiento metálico para evitar las interferencias externas. Por tanto, es un cable más protegido, pero menos flexible que el primero. el sistema de trenzado es idéntico al del cable UTP. La resistencia de un cable STP es de 150 ohmios.

Estos cables de pares tienen aplicación en muchos campos. El cable de cuatro pares (Figura 4.2) está siendo utilizado como la forma de cableado general en muchas empresas, como conductores para la transmisión telefónica de voz, transporte de datos, etc. RDSI utiliza también este medio de transmisión.

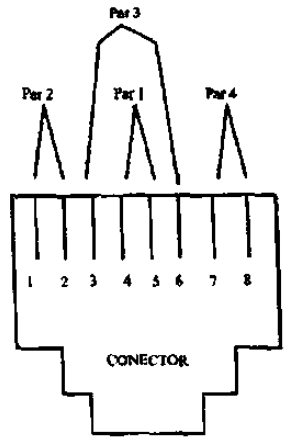


Fig 4.2 Cable de 4 pares.

Estructura de cables para un cable UTP en una red Ethernet o para una conexión RDSI, dependiendo de la elección de los pares.

En los cable de pares hay que distinguir dos clasificaciones:

La Categorías: Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.

Las Clases: Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características (Tabla 4.1).

CLASES	Clase A	Clase B	Clase C	Clase D
Ancho de banda	100 kHz	1 MHz	20 MHz	100 MHz
En categoría 3	2 km	500 m	100 m	no existe
En categoría 4	3 km	600 m	150 m	no existe
En categoría 5	3 km	700 m	160 m	100 m

Tabla4.1 Clases de distancias permitidas.

Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados.

Dado que el UTP de categoría 5 es barato y fácil de instalar, se está incrementando su utilización en las instalaciones de redes de área local con topología en estrella, mediante el uso de conmutadores y concentradores.

Las aplicaciones típicas de la categoría 3 son transmisiones de datos hasta 10 Mbps (por ejemplo, la especificación 10baseT); para la categoría 4, 16 Mbps, y para la categoría 5 (por ejemplo, la especificación 100BaseT), 100 Mbps.

En concreto, este cable UTP de categoría 5 viene especificado por las características de la Tabla 4.2.

Velocidad de transmisión de datos	Nivel de atenuación
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

(especificaciones TSB-36) referidas a un cable estándar de 100 metros de longitud.

Tabla 4.2 Cable UTP categoría 5.

Nivel de atenuación permitido según la velocidad de transmisión para un cable UTP.

Es posible utilizar la lógica de las redes FDDI (Fiber Distributed Data Interface) utilizando como soporte cable UTP de categoría 5 en la clase D, ya que la velocidad de transmisión es de 100 Mbps como en FDDI. Por esta razón se le suele llamar TPDDI, Twisted Pair Distributed Data Interface.

4.5.b Cable Coaxial .

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas más capacidad de las transmisiones digitales.

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro (Figura 4.3). Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

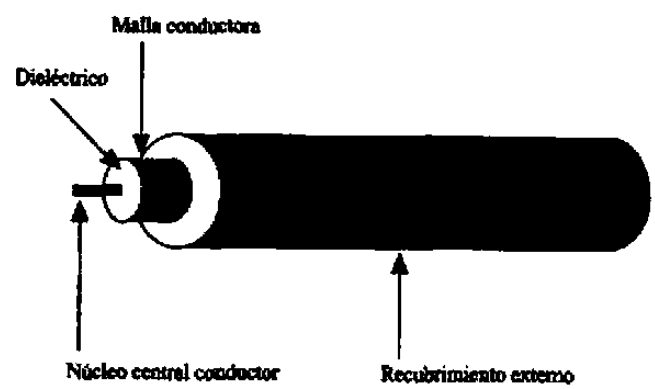


Fig. 4.3 Aislante dieléctrico.

Sección de un cable coaxial.

Es capaz de llegar a anchos de banda comprendidos entre los 80 Mhz y los 400 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica seríamos capaces de tener, como mínimo. del orden de 10.000 circuitos de voz.

4.5.c Fibra óptica .

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas. Cuando la señal supera frecuencias de 10^{10} Hz hablamos de frecuencias ópticas. Los medios conductores metálicos son incapaces de soportar estas frecuencias tan elevadas y son necesarios medios de transmisión ópticos.

Por otra parte, la luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente para ser utilizada en las transmisión de datos. Son necesarias fuentes especializadas:

Fuentes láser. A partir de la década de los sesenta se descubre el láser, una fuente luminosa de alta coherencia, es decir, que produce luz de una única frecuencia y toda la emisión se produce en fase.

Diodos láser. Es una fuente semiconductora de emisión de láser de bajo precio.

Diodos LED. Son semiconductores que producen luz cuando son excitados eléctricamente.

La composión del cable de fibra óptica consta de un núcleo, un revestimiento y una cubierta externa protectora (Figura 4.4). El núcleo es el conductor de la señal luminosa y su atenuación es despreciable. La señal es conducida por el interior de éste núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterio como la adicción de nuevas señales externas.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

Fibra monomodo. Permite la transmisión de señales con ancho de banda hasta 2 GHz.

Fibra multimodo de índice gradual. Permite transmisiones de hasta 500 MHz.

Fibra multimodo de índice escalonado. Permite transmisiones de hasta 35 MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda.

Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en

grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas.

Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad.

Fig. 4.4 Sección longitudinal de una fibra óptica.

Este tipo de sistemas se utilizan en ocasiones en las redes de área local por la comodidad y flexibilidad que presentan: no son necesarios complejos sistemas de cableado, los puestos se pueden desplazar sin grandes problemas, etc. Sin embargo, adolecen de baja velocidad de transmisión y de fuertes imposiciones administrativas en las asignaciones de frecuencia que pueden utilizar: son sistemas cuyos parámetros de transmisión están legislados por las Administraciones públicas. En algunos casos se requieren permisos especiales, según la banda de frecuencia que utilicen.

CAPÍTULO 5

PROYECTOS DE INTERNET II EN LA UANL

5.1 INTRODUCCIÓN

Siguiendo el desarrollo mundial de redes de datos de mayor capacidad y velocidad, para utilizarlas en aplicaciones de alta tecnología, la Universidad Autonoma de Nuevo León en un esfuerzo en conjunto con la comunidad universitaria del pais, toman la iniciativa de desarrollar una red de alta velocidad y unirse a la red internacional denominada Internet2, con el fin de dotar a la Comunidad Científica y Universitaria de la UANL y de México de una red de telecomunicaciones que le permita crear una nueva generación de investigadores, dotándolos de mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología a nivel mundial.

5.2 INTERNET II EN LA UANL

Con el fin de disponer de medios y servicios que permitan un avance substancial en la investigación y la educación, es necesario contar con una infraestructura que permita evaluar y utilizar los adelantos tecnológicos presentes y futuros en voz, datos y vídeo.

Para tal efecto, en la UANL, se conforma un grupo de académicos e ingenieros en tecnología, para participar en colaboración con otras instituciones académicas de nivel superior en México, en el desarrollo de una red cómputo con capacidades avanzadas separada de la Internet comercial, con fines educativos llamada Internet 2.

Es así que la UANL participa en el desarrollo una asociación civil denominada CUDI, organismo que representa jurídicamente los intereses de las Universidades e

Instituciones que conforman el proyecto de Internet 2 en México, semejante a la de organismos internacionales dedicadas a coordinar los trabajos de Internet2 a nivel internación.

5.3 IPV6.

Introducción.

El protocolo IP (Internet Protocol) fue diseñado para interconexión de redes. IP se ocupa de la transmisión de bloques de datos, llamados datagramas de origen a destino, donde orígenes y destinos son hosts identificados por direcciones de una longitud fija. IP también se encarga de la fragmentación y reensamblado de datagramas, si éste fuera necesario.

El .protocolo IP implementa dos funciones básicas: Direccionamiento y fragmentación. El módulo internet usa las direcciones contenidas en la cabecera de los datagramas para hacer llegar a estos a sus destinos. Asimismo, existen otros campos en la cabecera que permiten gestionar la fragmentación y posterior reensamblado de datagramas, para poder transmitir a través de redes que trabajen con tamaños de paquete pequeños. El módulo internet reside en cada host integrado en la internet, y en cada gateway interconectando redes. Estos módulos siguen reglas comunes para interpretar las direcciones y para realizar la fragmentación/reensamblado de datagramas.

Adicionalmente, estos módulos (especialmente en los gateways) están provistos de mecanismos para tomar decisiones sobre el enrutamiento de los datagramas.

Problemas del Internet Actual

Desde su creación, IPv4 suscitó numerosas discusiones sobre la concepción de la cabecera. Para más informaciones El problema más conocido concierne al espacio de direccionamiento.

Las direcciones IP están actualmente encapsuladas en 32 bits. Esto permite 4.E09 direcciones, lo que parecía suficiente al principio, cuando lo más común era que hubiese un ordenador por campus.

Hoy en día, el número de ordenadores personales conectados hace que este numero sea demasiado corto, sobre todo porque numerosas direcciones estan gastadas por el mecanismo de asignación jerárquica.

La generalización de las máquinas conectadas en red ("toasternet problem" o "paradigm shift") va a agravar todavía más este problema.

Otro problema viene dado por el aumento cada vez mayor del tamaño de las tablas de encaminamiento de Internet. El encaminamiento en una gran red debe ser jerárquico, con una profundidad tan grande como la amplitud de la red.

El encaminamiento IP es jerárquico únicamente a tres niveles : red, subred y máquinas.

Los routers de las grandes redes de interconexión deben tener una entrada en sus tablas para todas las redes IP existentes.

Este problema es parcialmente resuelto por el "Supernetting" o CIDR (Classless Internet Domain Routing).

IPv4 no permite indicar de manera práctica el tipo de datos transportados (TOS, Type Of Service, en IPv4), y por tanto, la gestión de la urgencia o el nivel de servicio deseado.

Esto es necesario particularmente en aplicaciones de tiempo real (como video), y en general para todo tipo de servicios (se desea generalmente que el tráfico de las News sea menos prioritario que el de Telnet).

Representación de direcciones:

Hay tres formas convencionales de representar las direcciones IPv6 :

1) La forma la más aceptada es x:x:x:x:x:x:x:x, donde las x representan los valores hexadecimales de los ocho bloques de dos octetos cada uno.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:8:800:200C:417A

Hay que destacar que no es necesario escribir todos los ceros que hay por delante de un nombre hexadecimal en un campo individual, pero se ha de tener por lo menos una cifra en cada campo.

2) El método de alocación de las direcciones IPng demuestra que es cómodo "colocar" bits a 0 en medio de las direcciones. Para una escritura fácil, una sintaxis adecuada sería suprimir estos ceros. La expresión de dos "::" indicaría uno o varios grupos de 16 bits iguales a 0. Por ejemplo, la dirección multicast siguiente:

FF01:0:0:0:0:0:43

Se representarría de la manera siguiente:

FF01::43

3) Otra forma alternativa, a veces más comoda cuando estamos en un entorno mixto de nodos IPv6 e IPv4, es x:x:x:x:x:x:d.d.d.d, donde los 'x' son valores hexadecimales (6 grupos de 16 bits) y los 'd' son valores decimales (4 grupos de 8 bits en la representación estándar de IPv4). Ejemplos:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:1:129.144.52.38

O con el formato comprimido,

::13.1.68.3

::1:129.144.52.38

Formato de la cabecera Ipv4.

Un datagrama es la unidad básica de transferencia entre la internet, y se descompone en cabecera y datos.

La estructura de un datagrama internet (Tabla 5.1) es la siguiente:

Versión	Long.cab.	Tipo de servicio	Longitud total	
Identificación			Flags	Offset fragmento
Tiempo de vida		Protocolo	FCS cabecera	
Dirección IP fuente				
Dirección IP destino				
Opciones				Relleno
DATOS				

Tabla 5.1 Estructura de un datagrama de internet.

Versión.

Este campo ocupa 4 bits, e indica el tipo de formato de datagrama. Para el formato descrito, su valor es 4 (IP versión 4).

Longitud de la cabecera.

Este campo ocupa 4 bits, y especifica la longitud de la cabecera medida en palabras de 32 bits, el mínimo valor posible para una cabecera correcta es 5 (5 32, 160 bits), ya que el campo de opciones puede estar presente o no.

Tipo de servicio.

Este campo ocupa 8 bits, e indica como deberá ser tratado el datagrama. Este campo se divide a su vez en cinco subcampos, de la forma siguiente:

Es posible que en uno o varios nodos del camino no exista alguna de las facilidades solicitadas, así, estos bits son más una ayuda a los algoritmos de encaminamiento que una petición de servicio.

Longitud del datagrama.

Este campo ocupa 16 bits, e indica la longitud total del datagrama, incluyendo la cabecera y los datos, la longitud se indica en octetos. Con esto, se permite especificar una longitud de hasta 65536 octetos, sin embargo, los datagramas largos resultan intratables a muchos hosts y redes. El mínimo tamaño que debería aceptar un host es de 576 octetos. Se recomienda que los hosts sólo envíen datagramas de más de 576 octetos y tienen la seguridad de que el destinatario podrá aceptarlos.

El tamaño de 576 octetos se elige para permitir un tamaño razonable del bloque de datos para ser transmitido junto con la cabecera. Así, este tamaño permite un tamaño para el bloque de datos de 512 octetos, junto con 64 octetos para la cabecera. El tamaño máximo de una cabecera es de 64 octetos, y una cabecera normal ronda los 20 octetos, proporcionando un margen de actuación.

Para que el datagrama se transmita de un nodo a otro de la red, deberá ser transportado en un paquete de la red física subyacente. La idea de transportar un datagrama en una trama de red se denomina encapsulamiento.

Para la red física subyacente, el datagrama IP es como cualquier mensaje intercambiado entre dos ordenadores, sin que reconozca ni el formato de datagrama ni la dirección de destino IP.

En el caso ideal, todo el datagrama IP cabría en una sola trama de red, haciendo que la transmisión fuese eficiente. Pero como el datagrama puede atravesar en su camino diferentes tipos de redes físicas, no existe una longitud máxima de datagrama que se ajuste a todas ellas. A la longitud máxima de transferencia de datos por trama de una red física se le conoce como unidad de transferencia máxima (MTU, Maximum Transmision Unit).

Cuando un datagrama se envía por una red con un MTU menor que su longitud, entonces el datagrama se divide en partes denominadas fragmentos. Al proceso se le conoce como fragmentación, y será comentado posteriormente.

Identificación.

Este campo ocupa 16 bits, y contiene un número entero que identifica al datagrama. Este número se asigna con un contador secuencial en la máquina origen que va asignándolos según nuevos datagramas. Este campo es indispensable en el proceso de reensamblado de fragmentos, cuando un datagrama fue fragmentado.

Flags.

Incluye varios flags de control :
Bit 0: Reservado, debe ser 0
Bit 1: (DF) 0 = el datagrama puede fragmentarse,
1 = el datagrama NO puede fragmentarse
Bit 2: (MF) 0 = es el último fragmento
1 = existen más fragmentos

El primer bit significativo (bit 1) del campo flags es el de no fragmentación, se llama así porque si está activo implica que el datagrama no puede fragmentarse.

El bit de menor peso del campo flags (bit 2), es el bit de más fragmentos. Este bit es útil para la máquina destino, que así puede determinar si ha recibido todos los fragmentos correspondientes a un datagrama. Cuando el bit está a cero, indica que es el útimo fragmento del datagrama.

Offset del fragmento.

Este campo ocupa 13 bits, y especifica el desplazamiento desde el comienzo del campo de datos del datagrama original hasta el comienzo del campo de datos del fragmento, expresado en múltiplos de 8 octetos.

Tiempo de vida.

Este campo ocupa 8 bits, e indica cuanto tiempo, en segundos, está el datagrama autorizado a permanecer en el sistema internet. La idea es simple: cuando una máquina pone un datagrama en la internet, le asigna un tiempo máximo de existencia del mismo. Los gateways y hosts que van procesando el datagrama deben ir decrementando el campo tiempo de vida, y descartarlo de la internet cuando el tiempo haya expirado.

Protocolo.

Este campo ocupa 8 bits, e indica cuál fue el protocolo de alto nivel que ha creado los datos que están en el campo datos.

FCS cabecera.

Este campo ocupa 16 bits, y asegura la integridad de la cabecera. La máquina origen ejecuta una serie de operaciones matemáticas sobre el conjunto de la cabecera y pone el resultado en este campo. El receptor hará la misma operación y comparará el resultado para asegurarse de que los datos de la cabecera son correctos.

Dirección IP origen.

Este campo ocupa 32 bits, e indica la dirección IP de la máquina origen.

Dirección IP destino.

Este campo ocupa 32 bits, e indica la dirección IP de la máquina destino.

Opciones.

Este campo tiene una longitud variable, y puede estar o no presente en la cabecera del datagrama. Esta opcionalidad se refiere a datagramas en particular, no a la implementación específica, cualquier módulo Internet debe implementar esta funcionalidad, tanto en hosts como en gateways.

Clase	Número	Longitud	Descripción
0	0	1 octeto	Fin de la lista de opciones.
0	1	1 octeto	Sin operación.
0	2	11 octetos	Seguridad y restricciones de acceso.
0	3	Variable	Encaminamiento de datagramas por rutas específicas.
0	7	Variable	Grabación de ruta.
0	9	Variable	Encaminamiento dirigido.
2	4	Variable	Grabación de tiempo.

Tabla 5.2 Datagrama de internet.

Relleno.

La cabecera de un datagrama IP esta alineada a 32 bits. Este campo se usa para asegurar que sea así. El sobrante hasta conseguir un tamaño múltiplo de 32 (bits), se rellena con 0's.

Formato de la cabecera IPv6

El formato de la cabecera IPv6 es el siguiente:

Versión	Prioridad	Etiqueta de flujo	
Longitud carga		Siguiente cabecera	Límite de saltos
Dirección origen " "			
Dirección destino " "			

Tabla 5.3 Formato de la cabecera de Ipv6

Versión.

Este campo ocupa 4 bits, e indica la versión de IP. Para el formato descrito, la versíon es la 6, para IPv6 (también llamada IPng, Internet Protocol Next Generation).

Este campo ocupa 128 bits, y corresponde a la dirección de destino. Se describirá con detalle en apartado Direccionamiento IPv6.

- Prioridad.

Este campo ocupa 4 bits, e indica la prioridad que el remitente desea para los paquetes enviados, respecto a los demás paquetes enviados por él mismo. Los valores de prioridad se dividen en dos rangos, de 0 a 7, paquetes para los cuales el remitente espera una respuesta en caso de congestión (p.e. tráfico TCP). Y de 8 hasta 15, paquetes que no deben ser respondidos en caso de congestión, el valor más bajo (8), se usaría cuando el remitente está dispuesto a que sus paquetes sean descartados en caso de congestión (p.e. Video en alta calidad). Y el valor más alto (15), cuando el remitente está muy poco dispuesto a que algún paquete sea descartado (p.e. Audio de baja calidad).

- Etiqueta de flujo.

Este campo ocupa 24 bits, y es usado por el remitente para indicar que sus paquetes sean tratados de forma especial por los routers, como en servicios de alta calidad o en tiempo real. En este punto, se entiende el flujo como un conjunto de paquetes que requieren un tratamiento especial.

Todos los paquetes pertenecientes al mismo flujo deben tener valores similares en los campos dirección origen, dirección destino, prioridad, y etiqueta de flujo.

- Longitud de la carga.

Este campo ocupa 16 bits, e indica la longitud del resto del paquete que sigue a la cabecera, en octetos. Si su valor es cero, indica que el tamaño de la carga vendrá especificado como Carga Jumbo, en una opción salto a salto.

- Siguiente cabecera.

Este campo ocupa 4 bits, e identifica el tipo de cabecera que sigue a la cabecera IPv6. Es coherente con los valores del campo protocolo en IPv4.

- Límite de saltos.

Este campo ocupa un octeto. Es decrementado en una unidad por cada nodo que redirige el paquete hacia su destino. El paquete es descartado si el valor del campo llega a cero. Este campo sustituye al campo tiempo de vida, de IPv4.

- Dirección origen.

Este campo ocupa 128 bits, y corresponde a la dirección de origen.

- Dirección destino.

Este campo ocupa 128 bits, y corresponde a la dirección destino

El tránsito hacia Ipv6.

Uno de los aspectos más importante durante el proceso IPng es el de la migración de IPv4 a IPv6.

La transición debe de hacerse de forma gradual, sin afectar a los servicios de IPv4 que se prestan en la actualidad.

En IPv6 el método propuesto se basa primordialmente en dos elementos básicos:

- La red de doble Capa-IPTunelado (Tunneling).
- La red de doble Capa-IP

Permite que a ipv6 se le añadan hosts, servidores DNS y routers, sin ningún cambio o ruptura en el soporte actual de ipv4.

La transición de la nueva generación de ip hace uso de un esquema de transición a largo plazo, que permite que los hosts se actualicen gradualmente, mientras al mismo tiempo de manera paralela, los DNS son actualizados y son capaces de trabajar con direcciones ipv6 y con direcciones ipv4 (Fig. 5.1) .

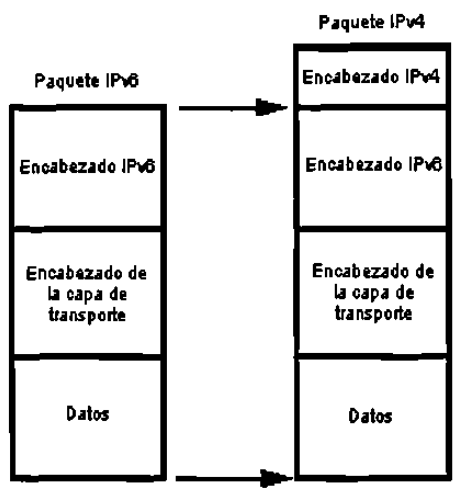


Fig. 5.1 Encapsulado Ipv6 en Ipv4

Tunneling de Ipv6 sobre Ipv4: Los hosts pueden transportar el trafico de ipv6 a través de topologías de enrutamiento de ipv4 por encapsulamiento.

Para enviar un paquete en un túnel, un nodo primero crea un encabezado de encapsulamiento Ipv4, y enseguida, transmite el paquete encapsuladoLa dirección destino del paquete de encapsulamiento Ipv4 especifica el túnel para el nodo que recibe

el paquete encapsulado extraído del encabezado de encapsulamiento Ipv4, actualiza el encabezado Ipv6, y después procesa el paquete incluido Ipv6 como cualquier otro paquete recibido.

Ejemplo de Tunelamiento (Fig. 5.2).

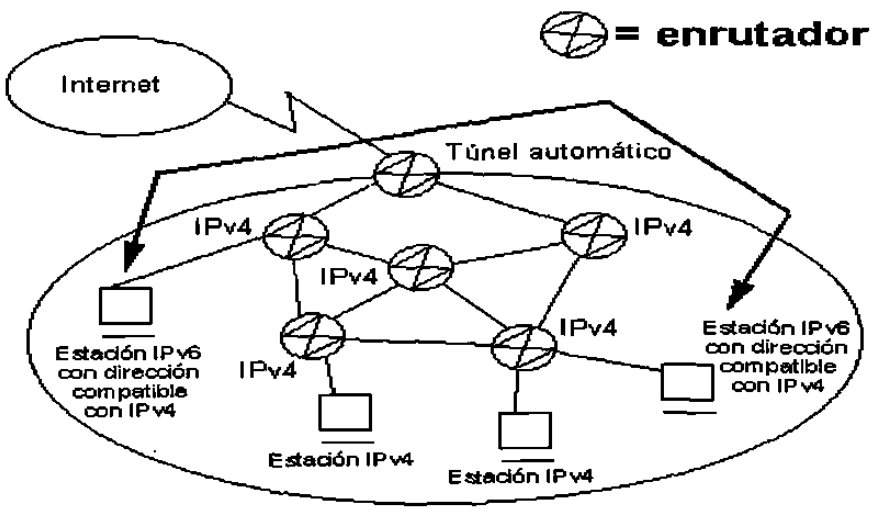


Fig. 5.2 Túnel automático.

Conclusiones.

IPv6, la nueva generación de Internet Protocol, además de ampliar la capacidad del campo de direcciones, IPv6 está diseñada para superar otras limitaciones de la versión actual, como la calidad de servicio y la configuración de enrutadores y hosts.

Pero la adopción de IPv6 requiere ciertos cambios en las aplicaciones, los protocolos de encaminamiento y los servidores de direcciones, según afirman los desarrolladores y fabricantes que están actualmente envueltos en la red de prueba de IPv6 6bone. Pero lo que realmente puede dificultar y entorpecer la migración a IPv6 son las aplicaciones, pues no podrán trabajar con el nuevo protocolo si antes no se adaptan a él.

IPv6 proporciona un campo de direcciones de 128 bits que incrementa exponencialmente el número de dispositivos que puede soportar el protocolo en

comparación con IPv4. Algunos observadores predicen incluso que las direcciones de la versión 4 se agotarán dentro de cinco u ocho años.

Esa es una de las razones por las que Internet Engineering Task Force (IETF) publicó un RFC donde se recogen sugerencias para afrontar la migración.

Los métodos de migración recomendados por el IETF son la utilización de dos pilas de protocolos y encapsulamiento.

El primero se refiere a la disposición de nodos IP capaces de soporta tanto protocolos IPv6 como IPv4. El enfoque de encapsulamiento (efecto túnel) se basa en transmitir paquetes IPv6 sobre las infraestructuras IPv4 actuales.

Los usuarios que quieran evitarse preocupaciones y deseen seguir usando IPv4, pueden utilizar NAT (Network Address Transalation) para ampliar el número de direcciones disponibles. Los servidores NAT, permiten a los usuarios aumentar el uso de las direcciones estableciendo una distinción entre direcciones de red privada y direcciones Internet. Para ahorrar direcciones Internet, NAT las asigna sólo a aquellos usuarios Internet activos, de modo que cuando éstos desconectan de la Red la dirección regresa a un pool compartido. Así, las organizaciones pueden satisfacer sus necesidades de conexión a Internet con un número mucho más reducido de direcciones. Esta solución está indicada especialmente para aquellas empresas que consideren que la mejora ofrecida por IPv6 no compensa el esfuerzo que supone adoptarlo.

5.4 QoS

Calidad de Servicio (Quality of Service) se refiere a la capacidad de una red para proporcionar mejores servicios al tráfico de la red seleccionado sobre varias tecnologías, incluyendo la Frame Relay, ATM (Modo de Transferencia Asíncrono), Ethernet, redes 802.1, SONET, y las redes ruteadas por IP que pueden usar cualquiera o todas estas tecnologías subyacentes. Las metas principales de QoS incluyen banda ancha dedicada, jitter controlado y latencia (requeridos por trafico en tiempo real e interactivo), y mejora las características de pérdida.

QoS incluye soluciones de hardware y software, estas clasifican la petición del paquete IP en diferentes clases de trafico y asignan los recursos apropiados al tráfico directo, basados en varios criterios incluyendo el tipo de aplicación, usuario o ID de la aplicación, fuente o dirección IP del destinatario, hora del día, y otras variables especificadas por el usuario.

La arquitectura básica de QoS incluye tres piezas fundamentales para la implementación de la Calidad de Servicio, estas son:

- QoS dentro de un solo elemento de la red (por ejemplo, colas, scheduling, y las herramientas de configuración del trafico)
- Técnicas de señalización para coordinar QoS punto a punto entre los elementos de la red.
- La política de QoS, la administración y las funciones de contabilidad, controlan y administran el tráfico punto a punto a través de la red.

Tres niveles básicos de QoS punto a punto puede proporcionarse por una red heterogénea, estos son:

- Servicio Best-effort.
- Servicios Diferenciados.
- Servicios Garantizados.

Servicio Best-effort.

También conocido como ausencia de QoS, el servicio best-effort es la conectividad básica sin garantías.

Servicios diferenciados (Differentiated service).

También llamado soft QoS; Algún tráfico se trata mejor que el resto (manejo más rápido, más ancho de banda en promedio, una tasa de perdida mas baja que el promedio). Ésta es una preferencia estadística, no una garantía.

El servicio garantizado (también llamado hard QoS).

Una reservación absoluta de recursos de la red para tráfico específico.

Herramientas de control de congestiones.

1.FIFO
2.PQ
3.CQ
4.WFQ

Para manejar los elementos de la red y el desbordamiento de el trafico de llegada, se debe usar un algoritmo de la formación de colas de espera para ordenar el tráfico, y entonces determinar algún método de prioritización.

Cada algoritmo de encolamiento está diseñado para solucionar cada problema específico de tráfico en la red; esto tiene un efecto particular sobre el performance de la red.

FIFO (First Input First Output).

En esta estructura simple, las colos FIFO almacenan los paquetes involucrados cuando la red esta congestionada y los envía en el orden en el que llegaron, esto cuando la red ya no esté tan congestionada. FIFO es el algoritmo usado por default para el encolamiento, ya que no requiere configuración, pero tiene severas deficiencias. La más importante, FIFO no toma ninguna decisión sobre la prioridad del paquete; el orden de llegada determina el ancho de banda, prontitud, y la asignación del buffer. Tampoco proporciona protección contra aplicaciones corruptas. El FIFO es un primer paso

necesario para el control de el tráfico de la red, pero las redes inteligentes de hoy necesitan de algoritmos más sofisticados.

PQ (Prioritizing Traffic).

PQ asegura que el tráfico importante consiga el manejo más rápido a cada punto dónde se usa. Fue diseñado para dar estricta prioridad al tráfico importante. La cola de prioritización pueden prioritizar flexiblemente según el protocolo de la red (por ejemplo IP, IPX, o AppleTalk), interface entrante, el tamaño del paquete, la dirección fuente/destino, y así sucesivamente. En PQ (Fig. 5.3) cada paquete es colocado en una de las cuatro colas -alta, mediana, normal y baja- basado en una prioridad asignada. los paquetes que no son clasificados por este mecanismo de prioridad son puestos en la cola normal; véase la figura. Durante la transmisión, el algoritmo da un trato absolutamente preferencial a las colas de mayor prioridad sobre las colas de menor prioridad. PQ es útil para hacer seguro él trafico de misión crítica que cruza varios WAN's obteniendo prioridad en el manejo.

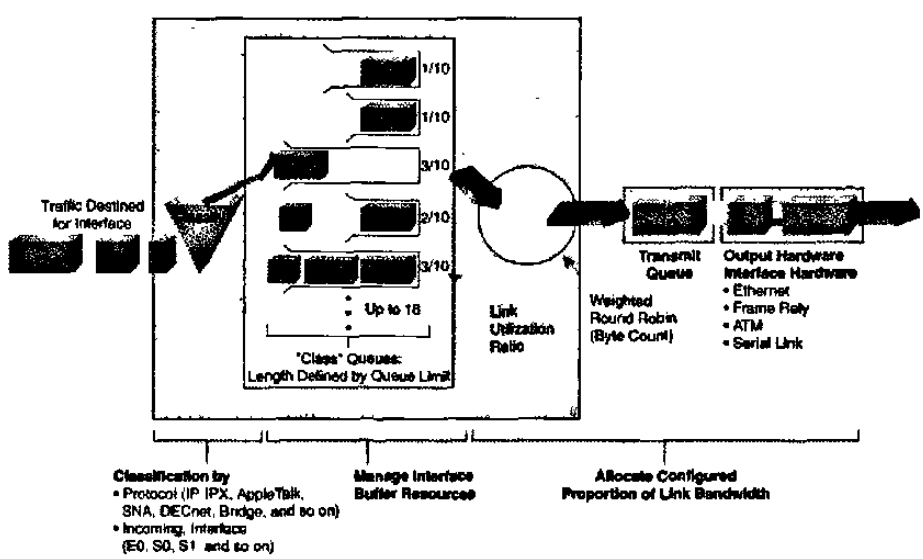


Fig. 5.3 PQ (Prioritizing Traffic).

CQ (Custom Queuing)

CQ fue diseñado para permitir a varias aplicaciones u organizaciones compartir la red entre las aplicaciones con mínimos anchos de banda específicos y requisitos de latencia. En estos ambientes el ancho de banda debe compartirse proporcionalmente entre las aplicaciones y los usuarios. CQ maneja el trafico asignando una cantidad especificada de espacio de la cola a cada clase de paquetes y después dar servicio a las colas en round-robin; vease la figura.

Herramientas para evitar la congestión.

WRED (Weighted Random Early Detection)

Los algoritmos de Random Early Detection (RED) fueron diseñados para evitar congestiones en las internetworks antes de que se vuelva un problema. RED trabaja supervisando la carga de tráfico a los puntos en la red y desecha probabilisticamente los paquetes si la congestión empieza a aumentar.

El resultado es que la fuente descubre el tráfico caído y retarda su transmisión. RED esta principalmente diseñado para trabajar con TCP en ambientes de redes IP.

WRED combina el las capacidades del algoritmo RED con la precedencia de IP.

Esta combinación provee tráfico preferencial a los paquetes de mayor prioridad. Puede eliminar selectivamente el tráfico de baja prioridad cuando la interface empieza a congestionarse y mantiene las características de distinción para las diferentes clases de servicio(Fig. 5.4).

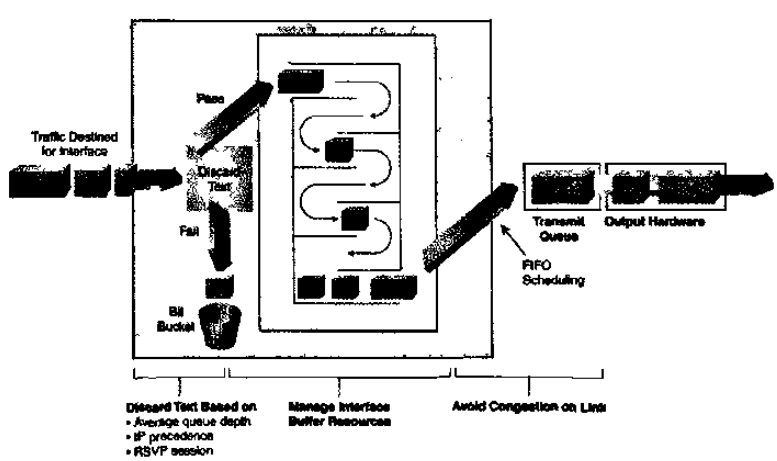


Fig. 5.4 WRED (Weighted Random Early Detection).

D-WRED (Distributed Weighted Random Early Detection).

El software de Cisco proporciona D-WRED, una versión de WRED de alta velocidad que corre sobre procesadores distribuidos VIP. El algoritmo D-WRED proporciona la funcionalidad más allá de lo que WRED proporciona, tales como colas de mínimo y máximo profundidad de borde y capacidades de drop para cada clase de servicio.

Configuración del tráfico y herramientas de monitoreo.

GTS(Generic Traffic Shaping).

GTS proporciona un mecanismo para el control de el flujo de tráfico en una interfaz en particular. Esto reduce el flujo de trafico de salida para evitar la congestión obligando al tráfico especificado a una tasa de bit en particular (también conocido como el token bucket approach), mientras estalla la cola del tráfico especificado. Así, puede formarse tráfico que se adhiere a un perfil particular para reunir los requisitos del contraflujo, eliminando cuellos de botella en topologías con incompatibilidad de tasa de datos. La figura 5.5 ilustara el GTS.

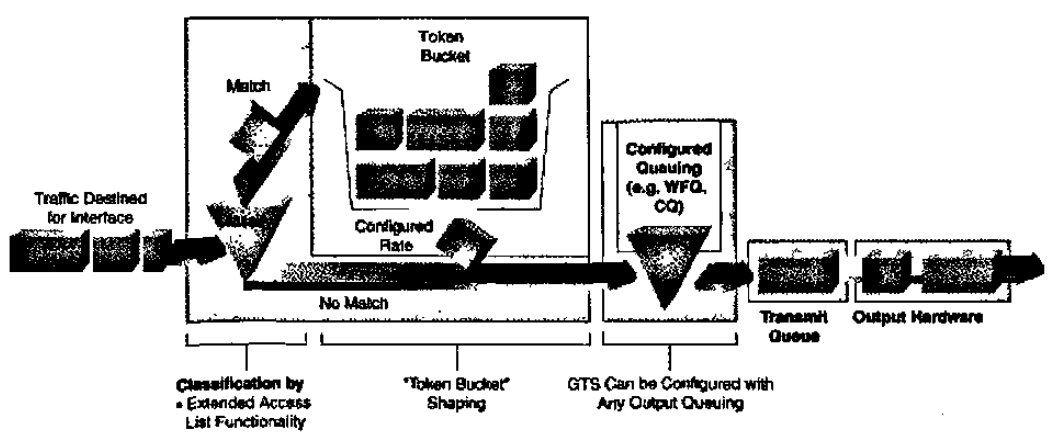


Fig. 5.5 GTS (Generic Traffic Shaping).

GTS se aplica sobre una interfaz básica, puede usar listas de acceso para seleccionar el trafico a configurar y trabaja con una variedad de tecnologías de capa 2, incluyendo Frame Relay, ATM, SMDS (Switched Multimegabit Data Service) y Ethernet.

FRTS (Frame Relay Trafic Shaping).

FRST provee parámetros que son usados para el manejo de las congestiones de tráfico en la red. Estas incluyen tasa de información consignada (CIR.- committed information rate), FECN y BECN y el bit DE.

La característica de FRTS construyen el soporte de Frame Relay con capacidades adicionales que mejoran la escalabilidad y ejecución de una red Frame Relay, incrementando la densidad de circuitos virtuales y mejoras en el tiempo de respuesta. FRTS puede eliminar los cuellos de botella en redes Frame Relay con conexiones de alta velocidad en el sitio central y conexiones de baja velocidad en los sitios ramificados

Mecanismos de eficiencia de enlace.

LFI (Link Fragmentation and Interleaving).

El tráfico interactivo (Telnet, VoIP, etc) es sensible a incrementar la latencia y el jitter cuando la red procesa largos paquetes. Las características de LFI reducen el delay y jitter sobre ligas de baja velocidad, haciendo un rompimiento de datagramas largos e interpolando tráfico de paquetes de bajo delay, obteniendo como resultado paquetes pequeños. La figura 5.6 muestra el proceso.

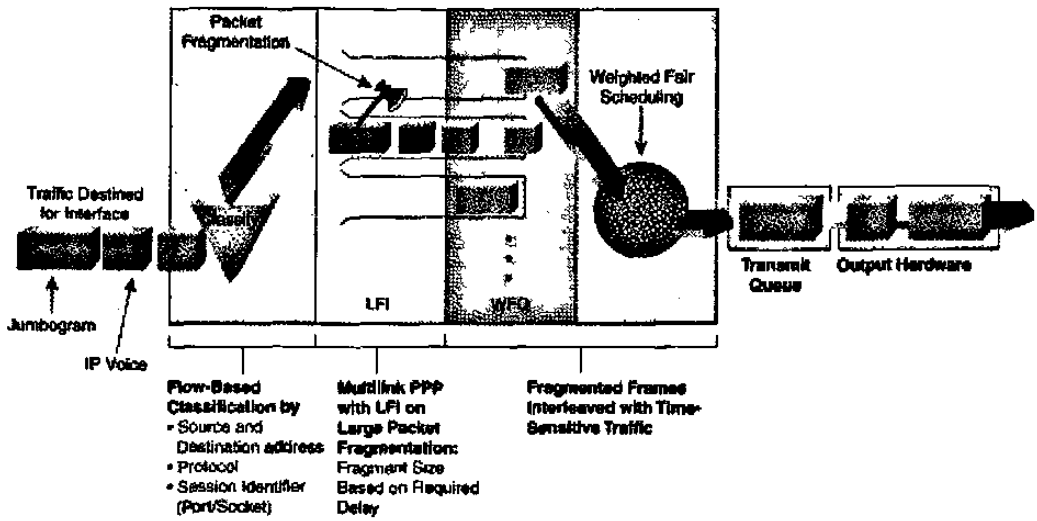


Fig. 5.6 LFI (Link Fragmentation and Interleaving).

RTP Header Compression (Real-Time Protocol Header Compression).

El Real-Time Transport Protocol es un protocolo host-host usado para transportar el nuevo trafico de aplicaciones multimedia, incluyendo audio y video empaquetado, sobre una red de IP. El Real-Time Transport Protocol provee funciones de transporte para redes punto a punto para aplicaciones que requieren transmisiones en tiempo real, como audio, video, o simulaciones de datos sobre servicios multicast o unicast.

El Real-Time Transport Protocol header compression (Fig. 5.7) incrementa la eficiencia de muchas de las nuevas aplicaciones de voz sobre IP o multimedia.

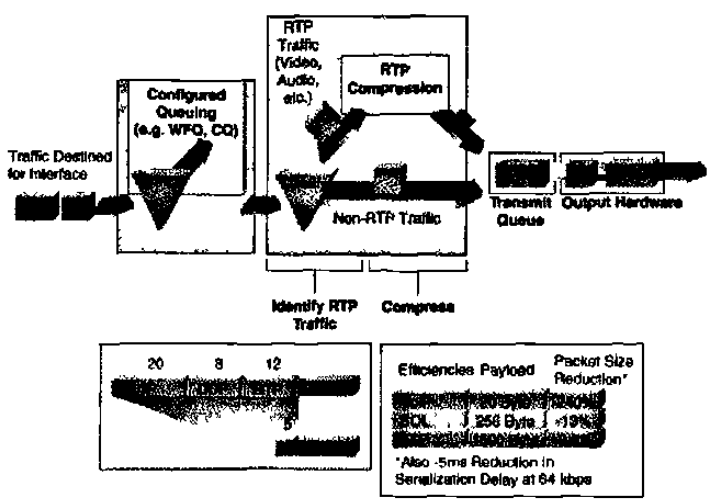


Fig. 5.7 RTP.

La figura 5.7 ilustra el Real-Time Transport Protocol header compression.

5.5 VIDEOCONFERENCIA.

Definición.

Al sistema que nos permite llevar a cabo el encuentro de varias personas ubicadas en sitios distantes, y establecer una conversación como lo harían si todas se encontraran reunidas en una sala de juntas se le llama sistema de "video conferencia".

Como sucede con todas las tecnologías nuevas, los términos que se emplean no se encuentran perfectamente definidos. La palabra "Teleconferencia" esta formada por el prefijo "tele" que significa distancia, y la palabra "conferencia" que se refiere a encuentro, de tal manera que combinadas se refieren a un encuentro a distancia.

La palabra teleconferencia es usada como un término genérico para referirse a cualquier encuentro a distancia por medio de la tecnología de comunicaciones; de tal forma que frecuentemente es adicionada la palabra video a "teleconferencia" o a "conferencia" para especificar exactamente a que tipo de encuentro se esta haciendo mención. De igual forma se suele emplear el término "audio conferencia" para hacer mención de una conferencia realizada mediante señales de audio.

El término "videoconferencia" ha sido utilizado para describir la transmisión de video en una sola dirección usualmente mediante satélites y con una respuesta en audio a través de líneas telefónicas para proveer una liga interactiva con la organización. La palabra "videoconferencia" es usada para describir la comunicación en dos sentidos de audio y video. Esta comunicación en dos sentidos de señales de audio y de video es lo que nosotros llamaremos "videoconferencia".

Existen algunos términos que pueden crear confusión con respecto a videoconferencia, como puede ser el término "televisión interactiva"; esté término a sido empleado para describir la interacción entre una persona y un programa educativo previamente grabado en un disco compacto (Láser disc) pero no requiere de la transmisión de video. Durante el desarrollo de este tema, se habrá de utilizar el término

"videoconferencia" para describir la comunicación en doble sentido ó interactiva entre dos puntos separados geográficamente utilizando audio y video. La baja sustancial registrada en los equipos de videoconferencia, así como también el abaratamiento y disponibilidad de los servicios de comunicación han hecho que la industria de videoconferencia sea la de mayor crecimiento en el mercado de teleconferencias.

Las aplicaciones.

- Reunión de ejecutivos. Educación a distancia.
- Adiestramiento/capacitación.
- Coordinación de proyectos.
- Estudios financieros. Declaraciones ante la corte.
- Actividad en bancos de inversión. Juntas de directorio.
- Control de la manufactura. Servicio al cliente.
- Diagnósticos médicos. Supervisión.
- Compras. Desarrollo de ingeniería.
- Gestión y apoyo de ventas. Contratación/entrevistas.
- Aprobación de préstamos. Manejo de crisis.

Elementos Básicos de un Sistema de Videoconferencia.

Para fines de estudio y de diseño los sistemas de videoconferencia suelen subdividirse en tres elementos básicos que son: la red de comunicaciones, la sala de videoconferencia y el CODEC. A su vez la sala de videoconferencia se subdivide en cuatro componentes esenciales: el ambiente físico, el sistema de video, el sistema de audio y el sistema de control.

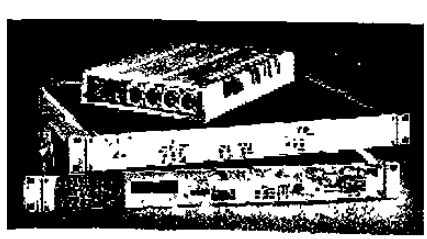
La red de comunicaciones.

Para poder realizar cualquier tipo de comunicación es necesario contar primero con un medio que transporte la información del transmisor al receptor y viceversa o paralelamente. En los sistemas de videoconferencia se requiere que este medio proporcione una conexión digital bidireccional y de alta velocidad entre los dos puntos a conectar.

La Sala de Videoconferencia (Fig. 5.8).

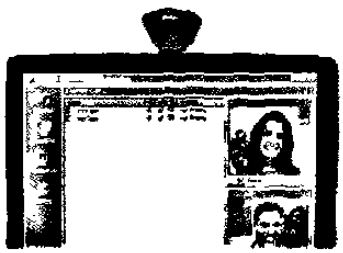
La sala de videoconferencia es el área especialmente acondicionada en la cual se alojarán los participantes de la videoconferencia, así como también, el equipo de control, de audio y de video, que permitirá el capturar y controlar las imágenes y los sonidos que habrán de transmitirse hacia el(los) punto(s) remoto(s). El nivel de confort de la sala determina la calidad de la instalación.

Codec (Fig. 5.9).

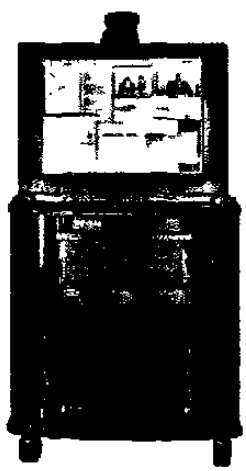


La señales de audio y video que se desean transmitir se encuentran por lo general en forma de señales analógicas, por lo que para poder transmitir esta información a través de una red digital, esta debe de ser transformada mediante algún método a una señal digital, una vez realizado esto se debe de comprimir y multiplexar estas señales para su transmisión. El dispositivo que se encarga de este trabajo es el CODEC (Codificador/Decodificador) que en el otro extremo de la red realiza el trabajo inverso para poder desplegar y reproducir los datos provenientes desde el punto remoto.

Sistemas y Capacidades (Fig. 5.10).



Existen diferentes tipos de sistemas de videoconferencia para diferentes tipos de aplicaciones. Estos sistemas pueden ser desktop (en una computadora), rollabout (sobreruedas) o interconstruidos. En todos estos sistemas, las partes que hacen funcionar el equipo son muy similares.



Los sistemas Desktop son usualmente en Computadoras personales, una cámara, un sistema de audio y software. Se requiere también una conexión a una línea ISDN (u otro tipo de línea digital) para realizar la transmisión. Durante una llamada se puede ver una imagen en movimiento de la persona en el otro extremo de la línea, se puede oír su voz y se pueden compartir los archivos y las aplicaciones. La calidad del video en estos sistemas no es tan buena como en los sistemas más grandes, pero continua mejorando. La mayoría de los sistemas desktop solo trabajan con una velocidad de 128 Kbps, y algunos a 384 Kbps. Están surgiendo nuevos estándares para permitir realizar estas aplicaciones utilizando una línea telefónica conmutada y un modem a 28 Kbps.

Los rollabout son diseñados para alojarse en un gabinete con ruedas. Son utilizados para videoconferencia entre grupos pequeños de personas. Usualmente uno o dos monitores son acomodados, con al menos una cámara montada sobre un monitor, además del sistema de audio, de control y el codec.

El sistema de audio consiste en un cancelador de eco, micrófonos, bocinas y amplificadores.

El sistema de control permite a los participantes manejar todos los dispositivos del sistema.

Los codecs son diseñados para transmitir y recibir dos señales de video: un video en movimiento, y una imagen de video estática.

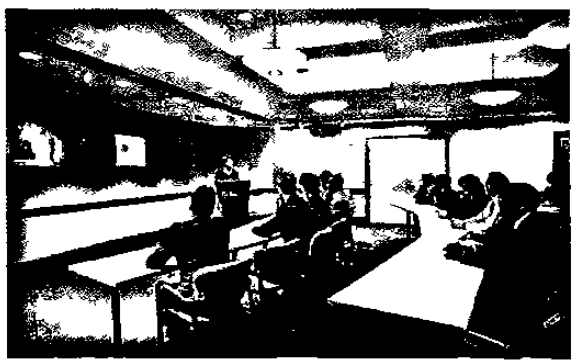


Fig. 5.11 Sistemas interconstruidos.

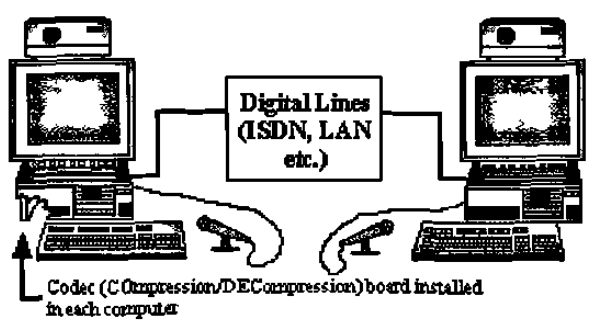
Los sistemas interconstruidos (Fig. 5.11) incluye a todos los equipos tiene un sistema rollabout, pero en lugar de residir en un gabinete con ruedas, estos sistemas se ubican en un lugar especialmente diseñando para ellos, pueden estar empotrados en una pared o en un rack. Esto crea una vista permanente de la sala que es conveniente para algunas aplicaciones especiales.

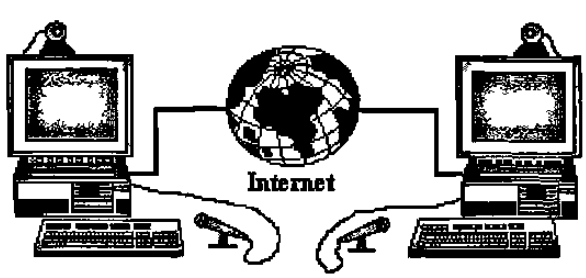
Las características de los dos tipos de sistemas son similares; aunque los sistemas interconstruidos frecuentemente tienen mas periféricos conectados y se utilizan para aplicaciones más especificas (ver fig. 5.12 y 5.13).

Fig. 5.12 Tipos de enlaces en redes.

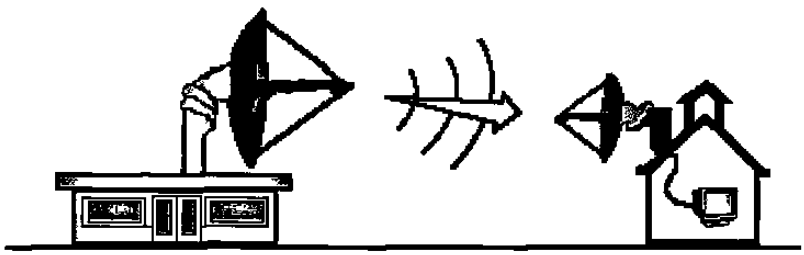
A través de líneas de ISDN.

En redes LAN.

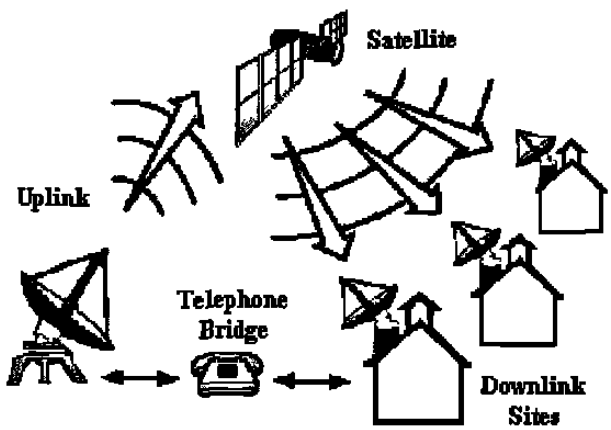




En redes WAN



Enlace corto de micro-ondas bidireccio-nal.(siempre y cuando exista línea de vista entre los lugares).



Un enlace a un codec digital que comprime la señal a 384KBps y subir al satélite a través de un sistema TDMA, se utiliza un solo transponder y llegar al extremo remoto.

Subir la señal a un transponder completo con señal de video y audio analógico, ocupando un transponder diferente para lograr ser bidireccional.

Fig. 5.13 Tipos de enlaces.

5.6 VOZ POR IP

Introducción.

Voz sobre IP se refiere al soporte de comunicaciones de voz mediante el uso del Protocolo de Internet o IP. Este tipo de comunicaciones son especialmente atractivas debido al bajo costo del acceso a Internet.

VoIP puede ser definida como la capacidad de hacer llamadas telefónicas, y todo lo que se puede hacer dentro de una red de Telefonía Pública, sobre redes basadas en IP con una adecuada calidad de Servicio (QoS) y un alto costo - beneficio.

VoIP presenta una gran oportunidad para los desarrolladores, proveedores de Internet, etc., pero sobre todo para las instituciones que desean lograr una mayor eficiencia y menor costo en sus comunicaciones.

Aplicaciones y Beneficios.

Las redes de Telefonía Publica no pueden ser remplazadas o cambiadas dramáticamente en el corto plazo, por lo que VoIP debe igualar las capacidades que estas tienen y presentar una alternativa.

El primer beneficio que trae VoIP es el ahorro en las llamadas de larga distancia. La persona que hace la llamada puede hacerlo desde su PC o un teléfono especial conectado a Internet, por lo que el costo que se aplica es el del acceso a Internet, la persona que recibe la llamada lo hace como cualquier llamada en su teléfono o por el mismo Internet. Otros beneficios son la consolidación y simplificación de las infraestructura de comunicaciones.

La figura 5.14 ilustra la infraestructura necesaria para hacer posible lo anterior:

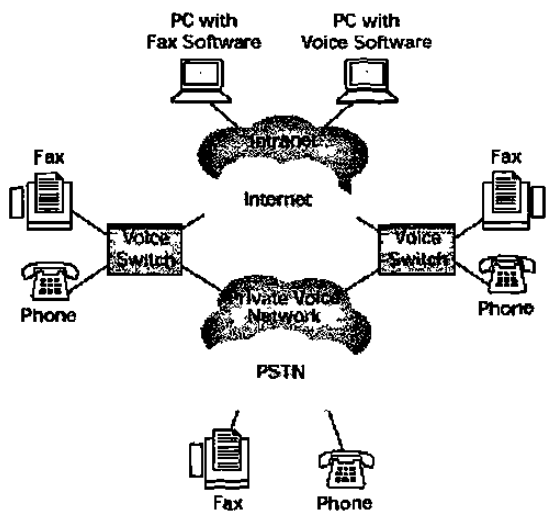


Fig. 5.14 Infraestructura VoIP.

Algunos ejemplos de aplicaciones de VoIP son los siguientes:

- Gateways.
  Interacción entre el Internet y la red de Telefonía Pública.
- Teléfonos Internet.
  Teléfonos normales con acceso a Internet.
- Acceso Remoto.
  Integración a la red telefónica corporativa desde puntos remotos

5.7 MPLS.

El MPLS CUDI es un grupo de trabajo identificado para la adopción de Multi Protocol Label Switching (MPLS) y sus tecnologías asociadas en la red de CUDI.

Nuestro compromiso es ser abierto a todos los operadores, fabricantes y usuarios que tengan deseos de producir una visión global para un completo servicio de Internet en la red de CUDI con tecnología MPLS, además de poder actuar como un canal que sirva como complemento de los grupos de trabajo existentes y a sus iniciativas, tales como QoS, Multicast, H.323, etc.

Por todo esto, no esta de mas mencionar que buscamos la neutralidad y la homogenuidad de la tecnología y NO inclinar preferencias hacia cualquier norma en particular, es así que nuestros objetivos estan identificados en dos rubros, que son:

Desde el punto de vista Técnico...

Servir como centro de referencia para las compañías que crean y desarrollan productos o servicios que dependan de las capacidades introducidas por MPLS y sus tecnologías asociadas.

- Promover la compatibilidad e interoperabilidad entre las diferentes plataformas
- Facilitar la comprobación de interoperabilidad
- Facilitar el soporte a la amplia gama de aplicaciones que hacen uso de esta tecnología
- Identificar, seleccionar y publicar acuerdos de implementación de MPLS, establecidos por los organismos de las normas nacionales e internacionales.

Desde el punto de vista educativo...

- Proveer información en normas e implementaciones de MPLS.
- Ayudar a los usuarios a desarrollar estrategias y criterios de evaluación para implementar MPLS en sus redes IP.
- Incrementar el conocimiento del usuario de los beneficios de implementar soluciones basadas en MPLS.
- Actuar como un centro de referencia de recursos didácticos con un interés en MPLS.

Proyectos...

- Propuesta de Implementación de MPLS en Backbone de CUDI (27-oct-00).
- Pruebas de interoperabilidad entre las diferentes marcas.
- Desarrollar documentación técnica de MPLS.
- Administración de MPLS.
- Voz sobre MPLS.
- Circuit emulation sobre MPLS.

5.8 CUDI.

CUDI es el acrónimo utilizado para nombrar a la Corporación Universitaria para el Desarrollo de Internet.

Este organismo es una asociación civil, cuyo principal objetivo es promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México.

¿Quiénes integran CUDI?

El 8 de abril de 1999 se oficializó en Los Pinos la constitución de CUDI, la cual se encuentra integrada por diversas instituciones educativas y centros de investigación científica de todo el país, además de empresas patrocinadoras.

Como Asociados fundadores, se encuentran las siguientes instituciones:

- Instituto Politécnico Nacional.
- Instituto Tecnológico de Estudios Superiores de Monterrey.
- Universidad Autónoma de Nuevo León.
- Universidad Autónoma Metropolitana.
- Universidad de Guadalajara.
- Universidad de Las Américas-Puebla.
- Universidad Nacional Autónoma de México.

CAPÍTULO 6

RED DE TELECOMUNICACIONES DE FIME

6.1 INTRODUCCIÓN

La red de la Facultad de Ingeniería Mecánica y Eléctrica de la Universidad Autónoma de Nuevo León, la respuesta a las grandes y diversas necesidades que plantea la enseñanza, la investigación y la administración.

Las universidades del país se preocupan día a día en brindar las mayores facilidades para una mejor preparación de sus estudiantes y de su personal docente, a fin de que sus futuros ingenieros estén cada día mejor capacitados técnicamente, dado a los grandes cambios tecnológicos que se dan en la industria.

La gran demanda de información, obliga a la industria de la computación a ofrecer mejores soluciones a. corto, mediano y largo plazo.

A fin de poder contar con una infraestructura de computo que esté adecuada a estos cambios y ofrezca una versatilidad de opciones de comunicación, la Facultad de Ingeniería Mecánica y Eléctrica evaluó la mejor opción de computo para ofrecer a sus catedráticos y alumnos la tecnología que este a la vanguardia y deje la ventana abierta para los futuros cambios tecnológicos del siglo XXI.

Fue entonces cuando la Facultad de Ingeniería Mecánica y Eléctrica invitó a : IBM, HP y DIGITAL a participar en un proyecto el cual ofreciera una solución de computo a todas las áreas académicas de la propia Facultad, así como el diseño de una red de área local (LAN), para unir los laboratorios de computo en la FIME.

La empresa DIGITAL presentó la mejor solución de equipo de computo y el diseño de una red local con tecnología en base al estándar IEEE 802.3/ETHERNET,

con una velocidad de transferencia de información de 10 Mbps. Sin embargo por ser la Facultad de Ingeniería la que debe de llevar la pauta en el desarrollo y la investigación tanto de computo como de comunicaciones dentro de la Universidad Autónoma de Nuevo León, y por ser una de las más grandes en población estudiantil, solicitó debido a nuevos anuncios en productos de tecnología más avanzada un nuevo esquema de red basado sobre una plataforma de tecnología de FDDI.

Bajo esta premisa se consideró la factibilidad y rentabilidad de tener un cambio de tecnología en el esquema de red, esta vez DIGITAL puso a consideración de la FIME una red de comunicaciones en base al estándar FDDI (Fiber Distributed Data Interfase),para transferencia de información con una velocidad de 100 Mbps.

Los equipos seleccionados cuentan con una versatilidad tecnológica que tiene la funcionalidad de interconectar redes Token Ring, Ethernet, y FDDI. Además su tecnología tiene preparación para las futuras redes públicas y privadas de ATM (Asynchronus Transfer Mode), con transferencia de datos de 155 Mbps.

6.2 CARACTERISTICAS PRINCIPALES.

- Anillo de fibra óptica de 2 Km. o 10 nodos FDDI.
- 12 Servidores Alpha.
- 500 computadoras en red.
- 4 Graficadores.
- 10 Impresores de inyección.

6.3 TOPOLOGIA DE RED

Los sitios seleccionados por la Facultad de Ingeniería Mecánica y Eléctrica fueron los siguientes:

El ler. sitio de inicio o punto de partida del anillo está en el edificio de la Dirección de la escuela, en el segundo piso del Departamento de Control Escolar, donde se remata

la fibra óptica del Backbone de la Cd. Universitaria. Se inició la red en este punto, logrando enlazar la Red d FINE al Backbone de Cd. Universitaria sin ningún problema de distancias y así poder realizar la conmutación de servicios que ofrece hoy y en un futuro la Dirección de Sistemas de la Universidad.

El segundo punto es la sala de Informática: (antigua Biblioteca) en donde actualmente está la Micro Vax, para dar servicio a las microcomputadoras de este punto y del auditorio en el tercer piso. El cableado que se utilizó es cable .UTP para las nuevas PC's y coaxial delgado (Thin Wire) para las computadoras anteriores, dentro de la sala como las del auditorio. También se instaló un Backplane Digital para alimentar a los servidores DECAlpha que en esta sala se localizan, los cuales son cinco servidores alpha, esta sala cuenta además.,con un módulo de impresión que consta de 6 impresoras láser, 2 plotters (graficadotes) y un total de 144 PC's .

El tercer punto de enlace en el anillo de FDDI, es el segundo piso del edificio de aulas 9, donde actualmente se cuenta con una sala de microcomputadoras. En este punto se instaló el equipo de comunicaciones de Digital DEChub 900, y los módulos 900 MX y 900 TM necesarios para los servicios a los equipos DECApha y PC's. El cableado también es coaxial delgado para los equipos anteriores y UTP para los nuevos equipos. Este punto está formado por dos aulas, en este punto también se cuenta con un servidor DEC Alpha.

El cuarto punto de enlaces es el primer piso del edificio de la Coordinación de Administración y Sistemas (a un costado de aulas 3) en una de las aulas de microcomputadoras, a fin de enlazar estas al anillo de FDDI e instalar uno de los equipos DECAlpha. Las redes actuales de micros se enlazan al anillo de FDDI vía los DECrepeaters 90 C, y las nuevas computadoras se conectan a los módulos DECrepeater 900 TM, para cableado coaxial delgado.

Este cuarto punto está formado por dos aulas, además está integrado por un equipo de comunicaciones (Backplane DEChub 900), módulos 900 MX y 900 TM indispensables para los equipos DEC Alpha y PC's, 2 servidores DEC Alpha y 1 00 computadoras.

El quinto punto de enlace es el segundo piso de la Biblioteca, en este punto también se tendrán los equipos de comunicaciones para el acceso al anillo de FDDI, y

adicionalmente se dejarán 4 hilos de fibra óptica, para los futuros enlaces ya sean de videoconferencias o de voz para enlace al conmutador central de la Facultad de Ingeniería Mecánica y Eléctrica.

El sexto punto es el edificio de Ciencias ' en este punto también tendremos un enlace a la red de datos de FDDI , y se dejarán 4 hilos de fibra óptica adicionales para el uso de transmisión de señales de video o voz. Las microcomputadoras en esta área se enlazaran con módulos DEC repeater 90T, para cableado de par torcido.

El séptimo punto en el edificio de POST-GRADO, se instalaron los equipos de comunicaciones, en un lugar cercano a la sala de conferencias, punto suroeste del edificio, donde dejamos hilos adicionales de fibra óptica para los enlaces de video o bien voz . El enlace será desde la Coordinación de Control y computación.

Los equipos Alpha que se instalarán en esta área, estarán conectados a los módulos DECrepeater 90 T o 900 TM, según la cantidad de servicios requeridos.

El siguiente punto es la sala de comunicaciones, segundo piso lado norte del edificio de Coordinación de Electrónica, en este piso se dejo infraestructura de hilos de fibra óptica, para usos futuros (Laboratorio de Conectividad).

Otro punto de conexión es también en el edificio de Electrónica en el cual se encuentra el laboratorio de Técnicas Computacionales en Ingeniería,- Este laboratorio cuenta con su DEC hub 900 y sus respectivos módulos, además -aloja dos servidores DEC Alpha.

6.4 INFRAESTRUCTURA.

La red de Fibra óptica para la FIME cuenta con la tecnología FDDI, para la transmisión de información de datos a alta velocidad (100 Mbps) y además deja instalada una infraestructura de cableado para la transmisión de señales de video y/o voz, en las áreas académicas y administrativas de la facultad. Esta red se integra al Backbone de Ciudad Universitaria a través de los equipos DECbridge 900 MX (puentes entre FDDI y Ethernet), a fin de tener acceso a los servicios que actualmente ofrece la Dirección de Sistemas de la Universidad, que son entre otros:

a) Acceso a la red universitaria.
b) Acceso a la red internacional de video conferencias.
c) Enlace de conferencia.
d) Enlace de conmutadores telefónicos (PBX, Private Branch Exchange) de Cd. Universitaria.
e) Acceso a Internet .
f) Acceso a la red de bibliotecas de UANL.

Dada la gran cantidad de aulas edificios de laboratorios, salas de conferencias y oficinas administrativas dentro de la facultad, se decidió integrar una comisión en la propia facultad con el fin de definir los puntos de mayor necesidad para la instalación de equipos de comunicaciones.

Se definió integrar en la red los puntos donde actualmente se cuenta con salas de microcomputadoras, laboratorios, 3 salas de conferencias y un punto adicional el cual tendrá la posibilidad de realizar un enlace de voz con el conmutador telefónico central de la Facultad y este a su vez con la red de conmutadores de Cd. Universitaria, o bien este punto se puede integrar a la red de video conferencia interna de la Facultad como también de Cd. Universitaria.

La red esta diseñada en una topología de anillo, con cable de fibra óptica de 12 hilos multimodo de 62,51125 micras para la transmisión de señales de datos, voz o video a velocidades de hasta 100 Mbps. Como se visualiza en el diagrama esquemático podemos observar la distribución de los hilos de cable de fibra óptica, para los enlaces de datos, video y voz, además de un enlace adicional de datos con tecnología Ethernet.

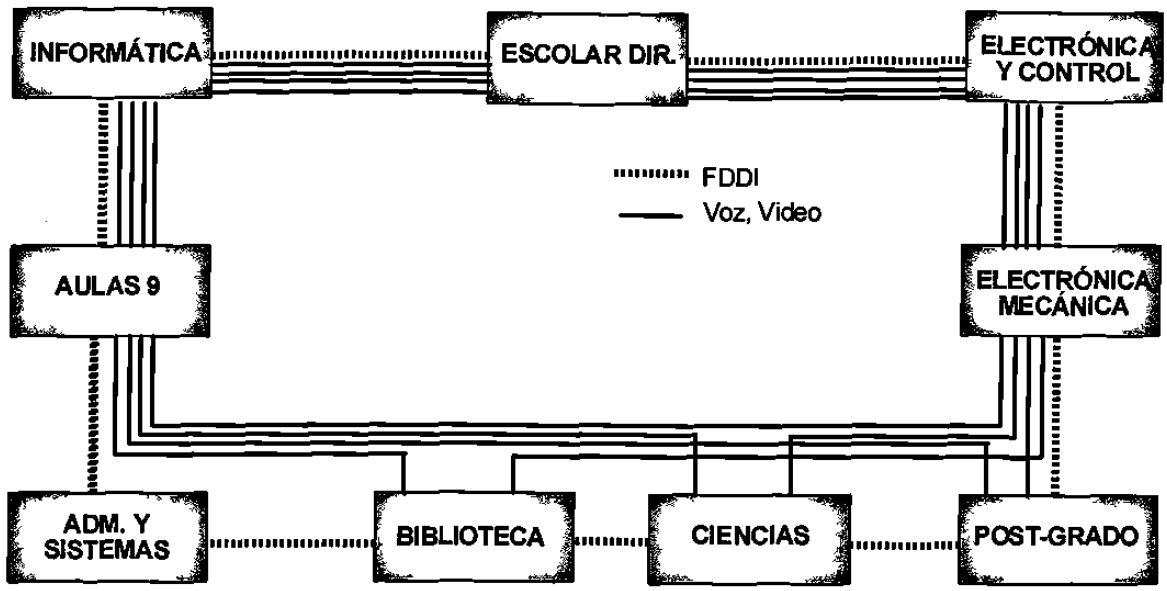


Fig. 6.1 BACKBONE DE FIBRA ÓPTICA DE FIME

En cada uno de los sitios seleccionados, los hilos de fibra óptica quedaron terminados con conectores ST en cajas de distribución de 12 fibras para la instalación de los "jumpers" a cada uno de los equipos de comunicaciones. Por lo que se refiere a los hilos que no se conecterizaron en cada sitio(porque no forman parte de la red de Datos, por ser hilos de la red de video o Voz), se realizaron empalmes de fusión y continuaron hasta el siguiente punto seleccionado para el enlace de video o voz.

6.5 DESCRIPCIÓN DEL ANILLO FDI

El equipo de comunicaciones que se instaló en los sitios seleccionados es el que a continuación se enumera:

- DEChub 900 (Concentrador para redes Ethernet, Token Ring, FDDI y ATM DECconcentrator 900 MX (Modulo FDDI).
- DECbridge 900 MX (Modulo para puente entre Ethernet y FDDI).
- DECrepeater 900 TM (Modulo repetidor de 32 puertos Ethernet para cable UTP).

- DEChub 90 (Concentrador para redes Ethernet).
- DECrepeater 90 C (Repetidor de 6 puertos Ethernet para cable coaxial delgado "Thin wire").
- DECrepeater 90 T (Repetidor de 8 puertos Ethernet para cable UTP).

Para comprender mejor la funcionalidad de estos equipos es necesario conocer los principios básicos en los cuales se basa su tecnología.

HUB: En forma genérica, término que describe un dispositivo que sirve como centro de una red con topología estrella. En la terminología Ethernet/IEEE 802.3 se refiere a un repetidor multipuerto, que a veces se conoce como concentrador. El término también se usa para el dispositivo de hardware/software que contiene múltiples módulos independientes, aunque conectados, de equipo de redes e interconexión entre redes.

Es un concentrador de alta escala. Se utiliza para extender las redes y hacer las conexiones con diferentes emulándolas sobre un mismo equipo.

REPETIDOR: Estos dispositivos operan en la capa física del modelo OSI, regeneran las señales físicas. Son usados principalmente para extender físicamente el alcance de una red local, pero no filtran el tráfico.

BRIDGE: Operan en la capa de enlace a nivel MAC, estos dispositivos operan en el modo Store-and-Forward y son independientes del protocolo de red utilizado. Son utilizados para la extensión de redes, dando mejor rendimiento y seguridad.

Para formar el anillo de FDDI, se instaló un cableado de, 12 hilos de-fibra óptica que circunda la facultad, en los puntos seleccionados se dejaron conectados solamente 4 hilos en un sentido y 4 en el sentido opuesto, a fin de que quede conformado el anillo doble.

Los hilos restantes servirán para los futuros enlaces de video y/o Voz, según lo determine la propia facultad (estos quedaron conecterizados en 4 sitios).

El anillo de FDDI, esta integrado por los módulos 900 MX, estos equipos se instalan al Concentrador DEChub 900, para enlazar la red FDDI con los equipos de computo DECAlpha. En cada sitio está rematada la fibra óptica y se utilizó dos pares de hilos para conectar el Módulo Concentrador 900 MX al anillo FDDI.

Los Módulos Bridge 900 MX realizaran la función dc puente entre la red de FDDI de alta velocidad (100 Mbps) y las redes locales Ethernet de 10 Mbps internas en cada edificio o sala de computación.

Los Módulos 900 TM, son repetidores de red Ethernet de 32 puertos, para cable de par torcido " Twisted Pair " (UTP) a distancias no mayores a 100 metros (punto a punto) donde concentremos cada uno de los equipos PC's, en las salas de computación.

Los Módulos 90 C, son módulos que cumplen con el estándar 10base2, para la transmisión de datos en formato de Ethernet a 10 Mbps,. con cable coaxial delgado (Thin Wire), a distancias no mayores de 185 metros (conectando no mas de 29 puntos) estos módulos los utilizaremos para integrar a la red los equipos de cómputo anteriores, que se encuentran, en las salas de computación con este tipo de cableado.

6.6 SERVICIOS

Servicio a alumnos.

Informática.

- 1 Sala con 144 computadoras.
- 5 Servidores ALFA.
- 6 Impresores Laser.
- 2 Graficadores.

Servicios Académicos.

Área Básica.

- 2 Aulas.
- 70 Computadoras.
- 1 Servidor alpha.
- Servicio 18 horas diarias.
- 2,200 Alumnos por semana.

Coordinación Administración y Sistemas.

- 3 Aulas.
- 100 Computadoras Personales.
- 2 Servidores alpha.
- Servicio 1 8 horas diarias.
- 3,000 Alumnos por semana.
- Carreras : Ingeniero Administrador de Sistemas y Mecánico Administrador.

Laboratorio de Conectividad.

Objetivo:

- Desarrollar, experimentar y comprobar.
- Programas para la comunicación.
- Aplicaciones de red.
- Protocolos de comunicación.
- Topologías de red.
- Carreras: Ingeniero Electrónica y Comunicaciones, Control y Computación.
- 8 Computadoras 486/50.
- 1 DEC Hub 900 Multiswitch.
- 1 FDDI Multimode (62.51125).
- 1 DEC Repetear 90 C y 90 T.
- 1 FDDI TP-UTP Modular.
- 1 DEC Bridge 900 MX.
- 1 Wave Llano PC NetWare Interface.
- 1 DEC Repeater 900-02. e 1 DEC Brouter 90 TI.
- 1 Back Plane Rack.

Áreas Adicionales beneficiadas.

- Técnicas Computacionales de Ing. Eléctrica.
- Técnicas Computacionales de Ing. Mecánica.
- Laboratorio de Control.
- Laboratorio de Máquinas Eléctricas.
- Aulas de Dibujo Técnico.
- Laboratorio de Circuitos Eléctricos.
- Laboratorio de Ciencias Básicas.
- Laboratorio de Potencia Eléctrica.
- Laboratorio de Electrónica.
- Laboratorio de Mecánica.
- Centro de Manufactura Integrada.
- Robótica y FMS.
- CADICAM Simulación.
- Máquinas y Herramientas.

Investigación.

- Doctorado.
- Servicio a estudiantes y profesores de Post- Grado.

Servicio a maestros.

Sala de Apoyo Académico y Capacitación.

- Cursos continuos de actualización.
- 32 Computadoras conectadas a la red FW.
- Auto-Aprendizaje.
- Biblioteca de manuales y software.

- Multimedia.
- Digitalización de imágenes.
- Impresión de alta calidad.

Servicios Administrativos.

- Dirección.
- Secretaría Académica.
- Tesorería.
- Recursos Humanos.
- Servicios Escolares.

Internet.

Red Mundial de Comunicación e Información.

- FTP.
- GOPBER.
- TRC.
- ARCHE.
- MAIL.