43
2ej

VNIVERSIDAD NACIONAL AVPNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

MIGRACION HACIA TECNOLOGIA ATM DE LA RED DE COMPUTO DEL INSTITUTO DE INGENIERIA

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A N :

ESTELA MONROY VARGAS
CESAR SANCHEZ LOPEZ

DIRECTOR: ING. MARCO AMBRIZ MAGUEY

CD. UNIVERSITARIA **1999.**

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

AGRADECIMIENTOS

Quisiera mencionar primero que a nadie a mis padres
por los principios que me inculcaron y el esfuerzo
incomparable que conmigo vivieron a diario
para darme una carrera.
Mil gracias, los quiero.

A mis hermanas que son más que mi familia,
son grandes compañeras, por ustedes, y
para motivarlas a seguir esforzándose
como hasta hoy.

A Mario por enseñarme a valorar las cosas,
gracias también por haberte conocido y
haber concluido juntos la carrera,
y por todo lo que me apoyaste.
A ti y tu familia, gracias.

Al Instituto y la Facultad de Ingeniería, a sus profesores
por todas las enseñanzas que nos comparten, y
en forma especial al Ing. Marco Ambriz por
sus consejos, tiempo y ayuda durante
la dirección de esta tesis.

A mi gran amigo y compañero César Sánchez por
invitarme a participar de este trabajo y por su
gran apoyo y comprensión en todo momento.
Gracias.

A todos los compañeros y amigos que conocí en la
carrera y todos los que participaron en este esfuerzo
culminante, y que considero parte de este logro.

Más que a nadie gracias Dios por permitirme llegar hasta aquí.

MIL GRACIAS

Estela Monroy Vargas

En primer lugar agradezco a Dios por haberme dado la vida, la salud y las circunstancias propicias para llegar a concluir este trabajo.

A mis padres, por haberme inculcado los valores primordiales de la vida y guiarme por el camino del amor, la responsabilidad y la educación.

A mis hermanos, especialmente a Martín, por apoyarme incondicionalmente a lo largo de mis estudios de bachillerato y profesionales.

A mis compañeros y amigos: José, Catalina, Estela, Maité y Verónica por formar el mejor grupo de trabajo en la Facultad de Ingeniería.

Al Instituto de Ingeniería, particularmente al Ing. Marco Ambríz Maguey, por haberme dirigido y apoyado siempre durante el desarrollo del presente trabajo. Así mismo agradezco a mis compañeros, Adán y Claudia, por haber compartido conmigo las responsabilidades diarias en el Instituto y por ser grandes amigos.

De igual manera agradezco a Estela Monroy por haberme ayudado en todos estos meses de trabajo hasta hacer posible la culminación de nuestra tesis de licenciatura y por ser además de gran compañera, excelente amiga.

Por último agradezco a todos aquellos que contribuyeron de una u otra manera a la realización del presente trabajo y que por alguna causa he olvidado mencionar.

A todos ustedes, infinitas gracias.

César Sánchez López

ÍNDICE

INTRODUCCIÓN 1

1. ANTECEDENTES 1

1.1 El Instituto de Ingeniería 1
1.1.1 Finalidad y Orientación *1*
1.1.2 Organización *1*
1.1.3 Antecedentes de la red del Instituto *3*
1.2 Modelo de referencia OSI 3
1.2.1 Introducción al modelo *3*
1.2.2 Descripción de las capas del modelo OSI *4*
1.3 Conceptos y estándares sobre redes de área local 10
1.3.1 Topologías de red *10*
1.3.2 Medios de transmisión para redes *16*
1.3.2.1 Medios terrestres 17
1.3.2.2 Medios aéreos 25
1.3.3 Protocolos de control de acceso al medio *26*
1.3.4 Estándares de redes *32*
1.3.4.1 Estándares del IEEE 32
1.3.4.2 Estándares de cableado estructurado EIA/TIA 568 45
1.3.4.3 Estándares de redes inalámbricas 48

2. TECNOLOGÍAS DE REDES DE ALTA VELOCIDAD EN REDES DE ÁREA LOCAL (LANS) ..54

2.1 Tecnologías de conmutación de redes LAN 54
2.1.1 Relación entre puentes y conmutadores *54*
2.1.2 Redes Token Ring conmutadas *55*
2.1.3 Redes Ethernet conmutadas *55*
2.1.4 Otras funciones disponibles en algunos dispositivos de conmutación *56*
2.2 Interfaz de datos distribuidos por fibra (FDDI) 57
2.2.1 Orígenes de FDDI *57*
2.2.2 Topología de FDDI *57*
2.2.3 Cableado *58*
2.2.4 Codificación *58*
2.2.5 Operación de redes FDDI *59*
2.2.6 Relación entre FDDI y OSI *59*
2.2.7 Las cuatro subcapas principales de FDDI *60*
2.2.8 Capacidad de FDDI *60*
2.2.9 Tipos de FDDI *61*
2.2.10 Comparación entre las versiones de FDDI *61*
2.2.11 Diferencias entre FDDI y FDDI-II *62*
2.3 Fast Ethernet (100 BaseT) 63
2.3.1 El sistema Ethernet *63*
2.3.2 Fast Ethernet *65*
2.3.3 Sistema de medio 100 Mbps TX *67*
2.3.4 Sistema de medio fibra óptica de 100 Mbps *71*
2.3.5 Sistema de medio 100BASE-T4 ..... *73*
2.3.6 La Auto-Negociación *75*
2.3.7 Pulso de enlace rápido *76*

2.4 100VG-AnyLAN 76
2.4.1 Creación de las tramas *77*
2.4.2 La arquitectura de 100VG *77*
2.4.3 Aspectos de cableado *79*
2.4.4 Aspectos del concentrador *79*
2.4.5 Preparativos para cambiar a 100VG-AnyLAN *79*
2.5 Gigabit Ethernet 81
2.5.1 El surgimiento del estándar Gigabit Ethernet IEEE 802.3z *82*
2.5.2 Arquitectura del protocolo Gigabit Ethernet *82*
2.5.3 Productos de Gigabit Ethernet *89*
2.5.4 Ethernet y los servicios de nivel más alto *90*
2.5.5 Distancia máxima en la red de acuerdo a la topología Ethernet utilizada *91*
2.5.6 Ultimos resultados del trabajo 802.3z *91*
2.6 Modo de transferencia asíncrono (ATM) 92
2.6.1 ATM y el modelo OSI *97*
2.6.2 Clases de calidad de servicio ATM (QoS: Quality of service) *99*
2.6.3 Topología de una red ATM *100*
2.6.4 Funcionamiento de ATM *100*
2.6.5 LAN Virtuales *103*
2.6.6 Emulación de LAN *105*
2.6.7 ATM y voz *121*
2.6.8 Aspectos de la migración hacia ATM *121*
2.6.9 Aspectos de integración en WAN *124*
2.6.10 Facilidad de ampliación *126*
2.6.11 Facilidad de administración *126*
2.6.12 Otros aspectos a tener en cuenta *126*
2.7 Red digital de servicios integrados (RDSI) 128
2.7.1 Interfaz de velocidad básica de RDSI *130*
2.7.2 Interfaz de velocidad primara de RDSI *130*
2.7.3 Servicios de RDSI *133*
2.7.4 Implementación de RDSI en una red de área local *135*
2.7.5 El futuro de RDSI en banda ancha *142*

3. ESTADO ACTUAL DE LA RED DEL INSTITUTO DE INGENIERÍA 144

3.1 Descripción de la organización actual de la red 144
3.1.1 Estado del backbone de la red del Instituto *144*
3.1.2 Estado de la red en el edificio 1 ..... *148*
3.1.3 Estado de la red en los edicios 2, 3 y 8 ..... *149*
3.1.4 Estado de la red en el edificio 4 ..... *149*
3.1.5 Estado de la red en el edificio 5 ..... *150*
3.1.6 Estado de la red en los edificios 6 y 12 ..... *151*
3.1.7 Estado de la red en los edificios externos al campo universitario *151*
3.1.8 Observaciones sobre el cableado actual de la red *154*
3.2 Servicios proporcionados actualmente por la red del Instituto de Ingeniería 155
3.2.1 Servicios básicos *156*
3.2.2 Servicios de recursos compartidos *158*
3.2.3 Sistemas de información distribuida *160*
3.2.4 Otros servicios *165*
3.3 Administración, monitoreo y seguridad en la red del Instituto de Ingeniería 166
3.3.1 Administración *166*
3.3.2 Monitoreo *168*
3.3.3 Implantación de herramientas de seguridad en el Instituto de Ingeniería *169*
3.4 Análisis de rendimiento de la red actual 170
3.4.1 Elaboración de pruebas de desempeño *170*
3.4.2 Análisis de resultados y conclusiones *172*

4. ESTUDIO DE LA SOLUCIÓN ATM 177

4.1 METODOLOGÍA DE ANÁLISIS, PLANEACIÓN E IMPLEMENTACIÓN 177
4.2 ANÁLISIS DE LA SOLUCIÓN ATM (ETAPA 2) 178
4.2.1 Revisión de la propuesta ATM *178*
4.2.2 Modificaciones hechas a la propuesta *180*
4.2.3 Relación con el proyecto de la Torre de Ingeniería *183*
4.2.4 Análisis del personal requerido para dar soporte a la red ATM *183*
4.3 INSTALACIÓN DE LA RED ATM (ETAPA 3) 184
4.3.1 Descripción de la nueva estructura del backbone *184*
4.3.2 Descripción de la estructura de red en los edificios 1 y 8 ..... *185*
4.3.3 Descripción de la estructura de red en los edificios 2, 3 y 4 ..... *186*
4.3.4 Descripción de la estructura de red en los edificios 5 y 6 ..... *187*
4.3.5 Descirpción de la estructura de red en el edificio 12 ..... *188*
4.3.6 Descripción de la estructura de red en los edificios externos al campo universitario *189*
4.3.7 Conexión a RedUNAM *189*
4.3.8 Descripción detallada del proceso de instalación *190*

5. EVALUACIÓN DE LA FUNCIONALIDAD DE LA RED ATM 192

5.1 DESEMPEÑO DE LA RED ATM (ETAPA 4) 192
5.1.1 Aspectos importantes de ATM *192*
5.1.2 Rendimiento de la red ATM *211*

CONCLUSIONES 218

GLOSARIO 221

REFERENCIAS 224

INTRODUCCIÓN

Desde el surgimiento de las redes de computadoras, las necesidades por conectar más equipos y compartir sus recursos ha crecido hasta volverse indispensable en prácticamente cualquier ambiente de trabajo donde éstas se empleen. Esta nueva modalidad no sólo es una nueva forma de ver las computadoras compartiendo dispositivos de software y hardware, también representa una forma novedosa de organizar los recursos computacionales para llevar el procesamiento de información de manera eficiente.

Debido a este notorio auge, las organizaciones y comités encargados de la estandarización de las especificaciones de redes, se han preocupado por seguir desarrollando soluciones a las nuevas necesidades y mejorar las que han sido adoptadas como estándar. Paralelamente a esto, están los vendedores y proveedores de dispositivos, quienes con sus diseños buscan cubrir dichas necesidades mejorando su desempeño y rendimiento, agregando nuevas innovaciones y reduciendo sus costos, cumpliendo las especificaciones oficiales y tratando de mantenerse a la vanguardia mundial.

El objetivo de nuestro trabajo, es precisamente la implementación de una de las más recientes tecnologías de redes aplicada a la infraestructura de una dependencia de la UNAM, como lo es el Instituto de Ingeniería.

El Instituto de Ingeniería, desde su creación, se ha enfocado a brindar apoyo a gran número de investigadores y estudiantes que ahí laboran y se encargan de realizar tareas relacionadas con problemas nacionales tanto de solución inmediata como de repercusión futura. Dicho personal requiere constante comunicación dentro y fuera de la institución, así como compartir los recursos de la red. Por la naturaleza de sus funciones, fue necesario evaluar con anterioridad, las condiciones en que se realizan dichas funciones, así como hacer un estudio sobre las opciones con las que se cuenta actualmente en el mercado, para cambiar a una tecnología mejorada que aumente el desempeño y ofrezca un mejor nivel de comunicación en la red del Instituto.

Con la finalidad de llevar una secuencia, se adoptó un método de investigación (de Merise) que permite separar por etapas cada una de las actividades realizadas durante la migración, facilitando el desarrollo y distinguiendo cada etapa de este proceso.

El método cubre cuatro etapas evolutivas en la implementación del proyecto, dichas etapas se encuentran desarrolladas en los capítulos 3, 4 y 5 del presente trabajo.

La etapa 1 correspondiente al estudio preliminar, se cubre en el capítulo 3 con la descripción detallada de la red Ethernet (original) del Instituto de Ingeniería, y el estudio de la propuesta original de su migración.

En el estudio detallado, correspondiente a la etapa 2 y cubierta en el capítulo 4, para la migración del backbone de la red del Instituto de Ingeniería, se consideran los aspectos y resultados contemplados en el trabajo previo de planeación, así como otros nuevos que se requirieron, al realizar la puesta en marcha de la nueva tecnología. Uno de estos aspectos fue el análisis de los sistemas de administración, seguridad y monitoreo sobre ATM, así como la realización e interpretación de diversas pruebas de desempeño con equipo diferente al sugerido.

Esta fase dio pauta a la siguiente etapa en el método de Merise, la cuál abarca la segunda parte del capítulo 4, correspondiente a la distribución y descripción de la instalación de la nueva red ATM.

De esta forma, se llego a la implementación del backbone de alta velocidad (ATM) cubriendo las especificaciones y necesidades planteadas. Por último, se probó la nueva instalación y evaluó su desempeño cubriendo así la última parte del método seguido, correspondiente a la puesta en marcha, que se describe a lo largo del capítulo 5 y que da fin a nuestro plan de migración.

1.- ANTECEDENTES

1.1 EL INSTITUTO DE INGENIERÍA

1.1.1 Finalidad y Orientación.

El Instituto de Ingeniería es parte del subsistema de investigación científica de la Universidad Nacional Autónoma de México. Desde su fundación, en 1956, la política del Instituto ha sido realizar investigación orientada a problemas generales de la ingeniería, así como colaborar con entidades públicas y privadas para mejorar la práctica de la ingeniería en el ámbito nacional, mediante la aplicación de los resultados de las investigaciones a problemas específicos. De igual forma busca promover la más alta calidad en la práctica profesional de los ingenieros que lo conforman tomando en cuenta las necesidades actuales y previsibles de la ingeniería nacional. Las actividades que se llevan a cabo en el Instituto son principalmente: investigación técnica y aplicada, apoyo al desarrollo tecnológico y análisis de los requerimientos sociales a cuya solución puede aportar la ingeniería. En múltiples ocasiones estas actividades se realizan en colaboración con otras instituciones afines, ya sean técnicas, culturales o científicas nacionales y extranjeras.

1.1.2 Organización.

Las actividades del Instituto se agrupan en 14 áreas y líneas de investigación. De esta manera, los programas se forman por conjunto de proyectos específicos dentro de cada una de las áreas.

Las áreas de investigación son:

Automatización. Desarrolla diversos aspectos relacionados a circuitería electrónica, programación y desarrollo de algoritmos para la implantación de esquemas de control y supervisión de procesos industriales.

Estructuras y materiales. Realizar estudios analíticos y experimentales sobre el comportamiento de las estructuras y materiales expuestos a diversas acciones que afectan la vida útil de las construcciones.

Geotecnia. Investiga la estructura y el comportamiento mecánico de suelos naturales y compactados, finos y granulares, e inclusive enrocamientos.

Hidráulica. Realiza investigaciones sobre el comportamiento y diseño de estructuras hidráulicas, hidrología, geohidrología, hidráulica fluvial y marítima, fenómenos transitorios, estabilidad de sistemas hidromecánicos, optimación de aprovechamientos hidráulicos, así como hidráulica fundamental y agrícola.

Ingeniería ambiental. Se orienta a la investigación y desarrollo de sistemas de tratamiento y potabilización de aguas residuales, convencionales y problemáticas.

Ingeniería de sistemas. Investiga metodologías y realiza estudios en planeación urbana y regional, desarrollo rural, desarrollo industrial, innovación tecnológica y planeación sectorial en todas sus especialidades.

Ingeniería mecánica, térmica y de fluidos. Estudia y diseña mecanismos de tipo industrial para la automatización de procesos, dispositivos para la absorción de energía sísmica en edificios, máquinas rotatorias, compresores y bombas. y diversos sistemas de engranes.

Instrumentación. Lleva a cabo investigación y desarrollo relacionado con electrónica e instrumentación aplicada. Proporciona asesoría y apoyo en las labores de selección de equipo de medición especializada y mantenimiento de aparatos de laboratorio.

Mecánica aplicada. Efectúa investigaciones teóricas y aplicadas para analizar la respuesta inelástica de edificios ante solicitaciones sísmicas. Determina el riesgo sísmico en sitios específicos, atendiendo al mecanismo de la fuente y la trayectoria de las ondas sísmicas.

Sismología e instrumentación sísmica. Se encarga de desarrollar e implantar sistemas de medición de alta precisión de temblores, se estudia la actividad sísmica general en el país y en particular la que se genera en las costas del Pacífico.

Vías terrestres. Estudia los sistemas de transporte en aquellos aspectos relacionados con el diseño geométrico y estructural, operación, conservación y reconstrucción de carreteras y aeropistas.

Ingeniería sismológica. Reúne a investigadores especializados tanto en la observación, análisis y modelado de terremotos, así como la evaluación del riesgo sísmico.

Bioprocesos ambientales. Realiza investigación y desarrollo de procesos biotecnológicos ambientales, así como la transferencia de estos al sector privado. Es líder nacional en materia de tratamiento anaerobio de aguas residuales, tanto industriales como domésticas.

Sistemas de Cómputo. Es en general un grupo que hace investigación y planeación de la infraestructura de cómputo del Instituto y se encuentra dividido en 5 áreas que son:

1. *Desarrollo de sistemas de información:* Es aquí donde se desarrollan y mantienen los múltiples sistemas de información del Instituto como son la base de datos académica y la base de datos de la USI de la Secretaría Académica entre otras.

2. *Soporte técnico a computadoras personales y periféricos:* Esta área lleva a cabo el mantenimiento preventivo y correctivo de las computadoras personales y de los periféricos. También se encarga de la instalación de hardware especial y software para las PCs de los usuarios. Por otra parte, presta asesoría al personal académico referente a la compra y uso del tipo de software y hardware a utilizar.

3. *Estaciones de trabajo y servidores Unix:* Este grupo realiza la administración de las estaciones de trabajo que prestan los múltiples servicios de Internet, así como las que se desenvuelven en tareas específicas de ingeniería. También se encarga de brindar asesoría y soporte técnico a los usuarios, además de la constante evaluación de las mejores tecnologías de software y hardware para las estaciones.

4. *Diseño y desarrollo de las páginas del Web:* Este grupo se encarga del diseño gráfico y la implementación de las páginas de Internet que se pondrán a disposición de la comunidad del Instituto, también lleva a cabo la actualización de información de las páginas que actualmente se encuentran disponibles en el servidor local.

5. *Infraestructura de redes y telecomunicaciones:* Se encarga de la planeación, instalación, administración, operación y monitoreo de la red local del Instituto (REDII). Además de mantener la seguridad tanto lógica como física de la red. También brinda asesoría en la compra e instalación de equipo de red nuevo y proporciona el mantenimiento al equipo existente, entre otras actividades.

1.1.3 Antecedentes de la red del Instituto de Ingeniería.

El Instituto de Ingeniería inicialmente tenía una red con tecnología Ethernet de 10 Mbps, a través de un backbone de bus de cable coaxial grueso el cual cumplía con el estándar 10Base5 del IEEE 802.3. En este bus se integraron los edificios 1, 2, 4, 5 y 12, dentro de cada uno de ellos se estableció un cableado basado en el estándar Ethernet 10 BaseT y de cableado estructurado. El backbone se enlazaba a RedUNAM por medio de la cual se conectaba a la red mundial Internet.

Posteriormente REDII sufrió algunos cambios importantes los cuales la convirtieron en la red con que actualmente cuenta el Instituto, dichos cambios se mencionan con detalle en el capítulo correspondiente al estado actual de la red del Instituto de Ingeniería.

1.2 MODELO DE REFERENCIA OSI

1.2.1 Introducción al modelo

Con la proliferación de las redes y la necesidad de establecer e implementar un conjunto de estándares internacionales entre los fabricantes, se definió primeramente una estructura o arquitectura de las tareas de comunicaciones. Estos modelos de comunicación se refieren a las funciones que se deben de realizar (estructuradas en capas) para llevar a cabo la comunicación entre emisor y receptor dentro de una red.

Existen diversos modelos de comunicación, siendo los más importantes:

- OSI (Open System Connection)
- TCP/IP

El modelo de referencia para Interconexión de Sistemas Abiertos (OSI), es el resultado del trabajo hecho en 1983 por la ISO (International Standard Organization) para la definición de estándares que permiten enlazar dispositivos heterogéneos. De esta manera OSI provee las bases para la conexión de sistemas abiertos de red, así como para el procesamiento de aplicaciones distribuidas.

Su estructura consta de 7 capas funcionales, las cuatro inferiores están orientadas al hardware, mientras que las tres superiores sólo al software. Las capas del modelo OSI se muestran en la figura 1.1.

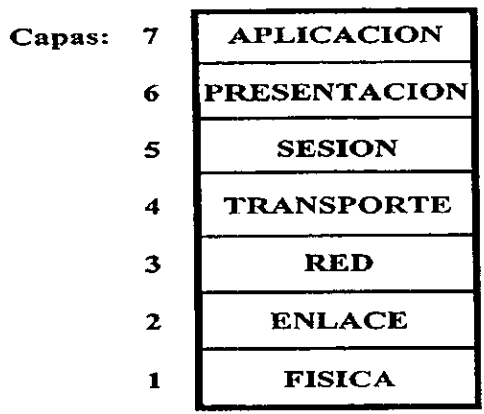


Figura 1.1

Cada capa dialoga con la capa de arriba, y con su par en el otro equipo accesando la capa de abajo. A este diálogo se le llama **protocolo**.

Sus objetivos fundamentales se dividen en dos: primero que los datos del emisor sean dirigidos y lleguen al destino correctamente y en sincronía, y segundo, asegurarse de que los datos que se entregan sean reconocibles y estén en el formato apropiado. Para ello OSI divide los protocolos de los 7 niveles en dos tipos: los que proporcionan el servicio de red y los protocolos de más alto nivel para la segunda parte.

1.2.2 Descripción de las capas del modelo OSI

Capa física

Esta primera capa se encarga de establecer la conexión eléctrica y aspectos físicos entre nodos a través del medio de transmisión, es decir se encarga de proponer la manera en que la información va hacia y desde los componentes físicos de la red, así mismo establece las reglas para que los bits sean transmitidos.

Entre sus funciones están las siguientes:

- Describe la interfaz a nivel eléctrico, electromagnético o luminoso, tanto en lo mecánico como en lo funcional.

- Temporiza las señales.
- Define los voltajes o niveles de tensión para referirlos a los valores de 0 y 1, así como la duración de estos. También regula las formas de codificación, decodificación, modulación y demodulación de la señal.
- Define características mecánicas de las terminales de conexión (tales como plugs, sockets y pines).
- Define sincronismos y delimitadores a nivel de bit, cuando hay información en el medio.
- Establece y termina un enlace de comunicaciones.
- Implementa físicamente la comunicación dúplex (en su caso).

Los sistemas de redes de área local (LAN) más habituales definidos en la capa física son Ethernet, Token Ring e Interfaz de Datos Distribuidos por Fibra (FDDI: Fiber Distributed Data Interface). Este nivel no controla detalles de conexión y cableado (estos detalles son clasificados en una capa extra llamada **capa 0** ó capa del modelo).

Capa de enlace

La capa de enlace de datos debe proporcionar la transmisión confiable entre dos puntos adyacentes de la red. Con éstos, sus funciones se limitan a las ligas individuales, y solo es responsable del tráfico entre nodos adyacentes (redes WAN) o computadoras sobre la misma línea (redes LAN). De esta manera convierte el medio de transmisión en una línea sin errores para la capa de red (siguiente nivel).

En esta capa la información ya no se procesa como bits de datos individuales, sino como paquetes de información (Data Frames) a los que se agregan encabezados (Headers) y banderas (Flags) para indicar el principio y terminación del mensaje cuando éstos provienen de las capas superiores, las cuales a su vez son removidas cuando los paquetes se reciben de la capa física.

Sus funciones se resumen como sigue:

- Estructura el flujo de bits bajo un formato predefinido (llamado **trama**), ya que todos los equipos no tienen la misma capacidad de procesar información.
- Agrega, para formar una trama, una secuencia especial de bits al principio y al final del flujo inicial de los mismos.
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas). Además para la corrección de errores se debe de incluir mecanismos para recobrar los datos perdidos, duplicados o erróneos (detección de errores por retransmisión).
- Provee control de flujo de datos que cruza el enlace para prevenir que el transmisor envíe los bits de manera rápida y ocasionar que el receptor llegue a saturarse.
- Sincroniza lógicamente (no físicamente) al transmisor y al receptor. Es decir, debido a que la comunicación entre dos extremos de un enlace es, por naturaleza, asincrónica, entonces se requiere que el primer bit de cada bloque esté en sincronía para funciones de reconocimiento de fin de bloque y detección de errores.

- Mantiene conocimiento y control de las condiciones del enlace, como son la fase de conexión, la fase de transmisión de datos y fase de terminación para asegurar que el enlace está hecho y funciona correctamente.
- Para redes tipo LAN, resuelve la competencia por el uso de un canal de comunicaciones compartido por unidades directamente conectadas al mismo.

Para redes WAN es una capa monolítica, para redes LAN y MAN está formada por normas propias; sólo hay nivel físico y nivel de enlace, estando dividido este último en dos subniveles, LLC (control de enlace lógico) y MAC (control de acceso al medio). El resto de niveles pueden ser cualquiera.

El protocolo usado en esta capa se conoce como HDLC (High-Level Data Link Control) o control de enlace de datos de alto nivel. Entre otros protocolos de enlace de datos se incluyen la retransmisión de paquetes y el modo de transferencia asíncrono ATM (Asynchronus Transfer Mode) que se utiliza en los sistemas de áreas extensas. Las normas Ethernet y Token Ring también están definidas en esta capa.

Capa de red

Esta capa se encarga del encaminamiento de los paquetes de datos dentro de la subred. Se pueden utilizar varios algoritmos de encaminamiento o enrutamiento (estáticos o dinámicos).

La unidad de datos en esta capa es el paquete o PDU de la capa 3 (PDU: Protocol Data Unit, es la unidad de información que intercambian las entidades de cada capa). La PDU tiene diferentes denominaciones dependiendo del nivel en que se trate. Los paquetes se forman aquí basándose en los mensajes (PDU de las capas superiores) añadiéndoles direcciones lógicas.

- Físico: Tratamiento a nivel de bit.
- Enlace: Trama.
- Red: Paquete.
- Transporte: T-PDU.
- Sesión: S-PDU.
- Presentación: P-PDU.
- Aplicación: A-PDU.

Esta capa desarrolla cuatro funciones principales: enrutamiento, control de red, control de congestión, interconexión de redes homogéneas y heterogéneas (llevando a cabo los mecanismos de fragmentación y reensamblaje).

Para el *enrutamiento*, la capa de red se auxilia de tablas de enrutamiento en cada nodo a lo largo de la trayectoria (estas tablas determinan las rutas de comunicación entre un transmisor y un receptor, además de tener información del estado de los nodos), y de esta manera escoger la mejor opción de ruta disponible, la cual dependerá de varios factores como son: el congestionamiento, el número de nodos que intervienen en dicha ruta, la velocidad de los enlaces, etc.

En la función de *control de red* cada nodo envía la información de su estado a otros nodos, y de la misma forma recibe información, para que se determine la mejor ruta para los mensajes. Además se asocian prioridades a los mensajes.

El *control de congestión* (que se produce en la red por un exceso de paquetes) reduce los retardos de la transmisión que pueden ocasionarse por sobrecargar algunos circuitos o un nodo en particular de la red. Aunque no todos los sistemas (como el tipo broadcast) pueden adaptarse a estas características cambiantes, la capa de red puede adaptarse a las condiciones de tránsito y así intentar enrutar los mensajes alrededor de estos puntos o nodos de congestión.

Entre otras funciones que competen a esta capa están:

- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final. Esto debido a que cada subred impone un tamaño máximo y formato para los paquetes que pasan a través de esta.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual (cuando se les restringe a los paquetes a seguir una ruta orientada a conexión) o como datagramas (estar moviéndose en modo sin conexión).
- Puede realizar trabajos de contabilidad y establecer tarifas en caso de que sea necesario saber que uso ha realizado cada usuario.
- También compete al nivel de red proporcionar un formato de direcciones, ya que estas son utilizadas por los nodos para calcular el encaminamiento. Estas direcciones deben ser universales, cada ordenador terminal tiene una dirección.

En redes de área local no existen problemas de encaminamiento o congestión, por lo que esta capa no existe.

Éste es el último nivel que se implementa dentro de la subred. Los restantes niveles solo se implementan en los equipos terminales.

Entre los protocolos de la capa de red más utilizados se encuentran el IP (Internet Protocol) y el IPX (Internetwork Packet Exchange) de Novell.

Capa de transporte

Es la primera capa que solo reside en los equipos finales (emisor y receptor). Es el primer nivel en el que se establece un diálogo extremo a extremo (en los niveles anteriores el diálogo es entre máquinas vecinas, ya sea terminal-nodo o nodo-nodo) debido a que la red no soporta este nivel.

Suministra a la capa superior un servicio de transporte de datos que ha de ser fiable (solucionando los problemas que aparezcan en el nivel de red), transparente (ocultando el tipo de red), y con unas primitivas normalizadas independientes del nivel de red.

Sus funciones principales son:

- Garantiza que el conjunto de paquetes que conforman el mensaje (PDU de esta capa) están formados en secuencia sin omisiones ni duplicaciones.
- Si es necesario, realiza una división de las unidades de datos que le llegan del nivel de sesión, en otras más pequeñas y las envía al nivel de red. Esta división solo se puede hacer en esta capa.
- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario (puntos extremos de una conexión).
- Provee la función de difusión de mensajes (broadcast) a múltiples destinos.
- Control de Flujo.

Esta capa también es la responsable de seleccionar entre el servicio *orientado a la conexión* (antes de comenzar a transmitir hay que establecer el circuito virtual por el que van a pasar los datos. Todos los paquetes de datos llevan el mismo camino y no necesitan llevar la dirección. Cuando se termina la transmisión se libera este circuito) o a la *sin conexión* (los paquetes se envían cada uno con su dirección destino y cada uno puede ir por un camino distinto, según el estado de la red. Pueden llegar desordenados. No hay ni conexión ni liberación de la comunicación) para ser usado en la transferencia de datos entre dos nodos y de monitorear dicha comunicación para asegurarse que el nivel de calidad es el adecuado para el tipo de servicio.

En servicios orientados a conexión:

1. Debe encargarse de solicitar una conexión a la red y liberarla cuando termine la transmisión.
2. Puede multiplexar varias conexiones de sesión en una de transporte para reducir gastos.
3. También puede dividir una conexión de sesión en varias conexiones de red para aumentar el caudal de datos.
4. Debe proporcionar una calidad de servicio especificada al establecer la conexión.

En un servicio no orientado a conexión:

1. Como las PDUs pueden llegar desordenadas, el nivel de transporte se encarga de ordenarlas y entregarlas ordenadas al nivel de sesión (para esto dispone del número de secuencia).
2. Este nivel también debe establecer un control de flujo entre los dos terminales (en los niveles de red y enlace, era entre máquinas vecinas), ya que los hosts no tienen porque trabajar a la misma velocidad. Hay diferencia entre el control de flujo entre hosts y nodos de la red o capa de enlace.
3. En la PDU se introduce una cabecera en la cual se identifica, entre otras cosas a qué conexión pertenece de entre todas las que tiene abiertas una máquina (ya que puede estar trabajando con varias conexiones al mismo tiempo).

Algunos de los protocolos de esta capa son TCP (Transmission Control Protocol) de Internet, SPX (Sequenced Packet Exchange) de Novell y Net-BIOS/NetBEUI de Microsoft.

Capa de sesión

Como su nombre lo indica, esta capa se encarga de establecer y terminar "sesiones" de comunicación entre nodos (usuarios de la red) de una forma ordenada, proporcionando los servicios necesarios (que la capa de transporte no aportaba), para organizar, sincronizar y controlar el intercambio de datos entre los mismos y estableciendo los períodos en que éstos pueden transmitir y recibir información.

Este diálogo puede ser dúplex (en forma simultánea) o semi-dúplex (en forma alternada). En las capas inferiores el diálogo puede ser full dúplex. En el caso de diálogo semi-dúplex, el nivel de sesión provee un mecanismo para poder establecer el diálogo por turnos, gestiona los testigos de comunicación.

Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre dos máquinas, etc.

Otras de las funciones que lleva a cabo son:

- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half dúplex o full dúplex).
- Proporciona un servicio de sincronización que permite recuperar la sesión cuando se ha producido una caída de la conexión, sin que se dupliquen ni pierdan datos.
- También es la que mantiene las transmisiones orientadas a la conexión.

El servicio de sincronización se proporciona para sobreponerse a cualquier error que se detecte. Si se llegara a detectar un error, la conexión de la sesión podría restablecerse en un estado definido y los usuarios regresarían a un punto designado en el diálogo, se descartaría una parte de los datos transferidos y después se reiniciará a partir de ese punto.

Capa de presentación

La capa de presentación define el formato de los datos para ser intercambiados entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transmisión de datos.

Permite hacer que sistemas que no utilizan el mismo formato de representación de datos (C-1, C-2) se puedan comunicar. Para ello se ha normalizado una sintaxis abstracta (ASN.1) y todos los sistemas que trabajen en OSI pasarán sus datos a esta sintaxis.

Esta capa también proporciona el cifrado de datos para garantizar la integridad de contenido y evitar que se puedan producir diversos eventos (lecturas de texto en claro, suplantaciones, etc.), para lo que se utilizan algoritmos de cifrado y mecanismos de aplicación de estos algoritmos.

El cifrado sin embargo no es exclusivo del nivel de presentación, también puede ser aplicado en otros niveles.

Esta capa tiene las siguientes funciones principales:

- Establece una sintaxis y semántica de la información transmitida.
- Da formato a los datos para la capa de aplicación.
- Define la estructura de los datos a transmitir (por ejemplo: define los campos de un registro: nombre, dirección, teléfono, etc.).
- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).
- Compresión de datos para aumentar la eficiencia.
- Criptografía. Encripta y desencripta la información que se transmite para evitar que sea utilizada por usuarios no autorizados.

Capa de aplicación

La capa de aplicación proporciona un medio para que los programas de aplicación accesen al ambiente OSI. Esta capa contiene las funciones de administración y generalmente los mecanismos totales para soportar aplicaciones distribuidas.

Algunas aplicaciones de propósito general consideradas para residir en esta capa son:

- Transferencia de archivos (FTP).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail).
- Acceso a bases de datos, etc.

Además servicios como: servicio de directorio, ejecución remota de trabajos y administración de la red.

1.3 CONCEPTOS Y ESTÁNDARES SOBRE REDES DE ÁREA LOCAL

1.3.1 Topologías de red

La forma en que se interconectan los dispositivos de una red determina la topología, o forma lógica de la misma. Las topologías de red son:

- Anillo.
- Estrella.
- Bus.
  - Árbol.
- Malla o Trama
- Semimalla.

- Física vs lógica:
  - Anillo en estrella.
  - Bus en estrella.
  - Estrella jerárquica.

Anillo

Es una de las tres principales topologías de red (figura 1.2). Consiste en un conjunto de estaciones o computadoras unidas una con otra formando un círculo por medio de un cable común (repetidor). Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo, esto es, las ligas son unidireccionales por lo que los datos son transmitidos en una sola dirección y orientados en el mismo camino.

Los repetidores son conectados por ligas punto a punto en este círculo cerrado, por lo que cada repetidor participa en dos ligas. Estos son dispositivos relativamente simples, capaces de recibir datos que viajan a través de una liga y retransmitirlos bit por bit por la otra liga tan rápido como sean recibidos; los repetidores no cuentan con una memoria de almacenamiento o buffer.

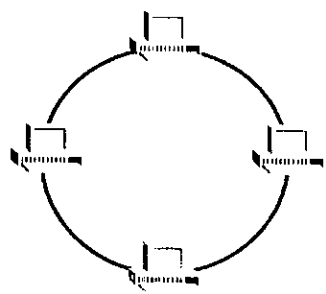


Figura 1.2

La topología de anillo es una solución para los llamados cuellos de botella, además de que la lógica para implementarla es muy simple. Requiere de un mínimo de inteligencia lo que aminora el costo y la hace atractiva, además de que cada elemento de la red es de igual jerarquía en sus facultades de comunicación, lo que resalta su flexibilidad y confiabilidad.

Su principal desventaja es que cuenta con un sólo canal que conecta a cada dos repetidores en el anillo; lo cuál indica que si una liga entre dos repetidores tiene una falla, toda la red se perderá. Otro problema es que conforme va creciendo la red, el paso de los mensajes por cada nodo, disminuye notablemente la velocidad del anillo.

Una variación del anillo que se utiliza principalmente en redes de fibra como FDDI es el doble anillo.

Estrella

En esta topología cada computadora de la red se une en un único nodo (figura 1.3), normalmente con control centralizado, como un concentrador de cableado, mediante dos ligas punto a punto, cada una de transmisión en una sola dirección (una de salida y la otra de entrada al nodo central).

Una transmisión desde cualquier computadora de la estrella, entra al nodo central y es retransmitido por este hacia todas las ligas de salida, pero solamente una computadora a la vez puede transmitir completamente. Por esto, aunque el arreglo es físicamente una estrella, lógicamente se puede decir que es un bus colapsado.

El software de control no es complejo y el flujo de tráfico es simple en esta topología, ya que todo el tráfico emana del nodo central que es el responsable de enrutar el tráfico a través de él, hacia los otros componentes. Además de ser el responsable de aislar fallas, lo cuál es relativamente sencillo ya que las líneas de transmisión pueden ser desactivadas independientemente y de esta manera identificar algún problema. Sin embargo esta topología es vulnerable a los cuellos de botella y fallas en el nodo central de la estrella si el dispositivo utilizado no es seleccionado adecuadamente.

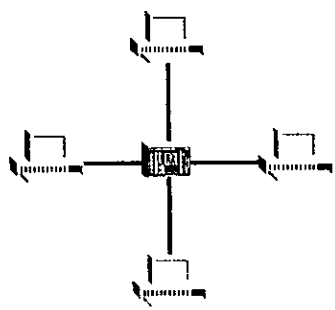


Figura 1.3

Bus

Es la tercera de las topologías principales, en ella las computadoras están conectadas por un único segmento de cable (no se requiere de conmutadores ni de repetidores por cada estación). A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo, esta topología se muestra en la figura 1.4.

Una estación de trabajo o computadora al transmitir, inserta paquetes de información al medio de transmisión, estos paquetes se propagan por toda la longitud del bus y de ésta manera son recibidos por todas las demás estaciones de trabajo (o computadoras) unidas al medio.

La red permite que los mensajes sean transmitidos a todos los nodos que son independientes entre sí, lo que aumenta la confiabilidad y la eficiencia de la red, aunque ello también requiere que cada nodo pueda transmitir, recibir y resolver problemas.

Su principal desventaja es que existe un sólo canal de transmisión para servir a todos los dispositivos sobre la red. Lo que provoca que si se genera una falla en el medio de transmisión se perderá el servicio en toda la red. Otra desventaja es su dificultad de aislar fallas de algún componente en particular que se encuentra conectado al bus. Además la ausencia de puntos centrales hace difícil la solución de problemas.

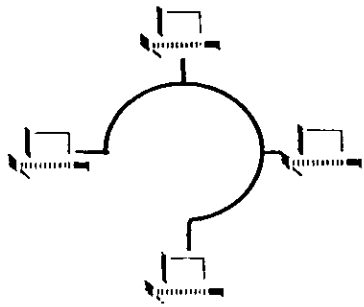


Figura 1.4

Árbol

Una generalización de la topología de bus es la topología de árbol, esta estructura de red se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

El medio de transmisión es una serie de ramificaciones que no cierran los ciclos. Su diseño comienza con un punto conocido como la raíz (headend), de esta manera, uno o más cables empiezan a conectarse o ramificarse. Las ramas a su vez pueden conectar más ramas para permitir realizar diseños más complejos. Al igual que en la de bus, una transmisión desde cualquier punto se propaga a través del medio y puede ser recibido por todas las demás computadoras.

Malla o Trama

Otras topologías menos comunes, son la de malla y semimalla. En la topología de malla, todas las computadoras se conectan entre sí (figura 1.5). A diferencia de otras topologías no hay que "esperar" a que se pueda accesar a la línea común, pues cada máquina tiene su línea directa (tiempo real). Su gran ventaja, por no decir única, es que si se cae una liga hay otras opciones para mandar información. Entre sus desventajas están; que se requiere un ancho de banda muy grande, mucho cable para conectar a todas las estaciones, numerosos dispositivos de interconexión. Por lo anterior su implementación es alta en costos.

Esta topología es típica de las WAN, aunque se puede utilizar en algunas aplicaciones de redes locales. Los nodos están conectados cada uno con todos los demás.

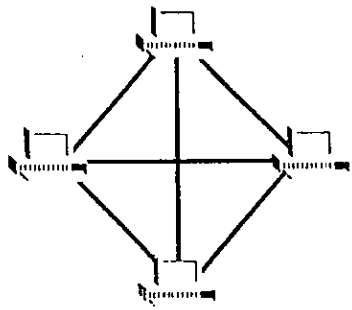


Figura 1.5

Semimalla

No necesariamente todas las estaciones están conectadas entre si, pero si varios de los dispositivos integrados en la red, que son los que necesitan estar en tiempo real. La figura 1.6 muestra esta topología.

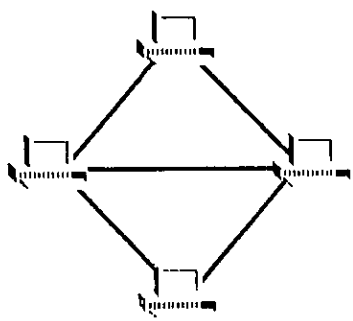


Figura 1.6

Topología física vs topología lógica

Mientras la topología física, estudiada en la parte anterior, se refiere al tendido "físico" de los cables, la topología lógica se refiere a la forma real en que va a operar la red. Cuando se estudia la red desde el punto de vista puramente físico aparecen las siguientes topologías llamadas combinadas, pues soportan físicamente una estructura pero son administradas de otra forma.

- **Anillo en estrella**

Esta topología se utiliza con el fin de facilitar la administración de la red.
Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo, tal como lo muestra la figura 1.7.

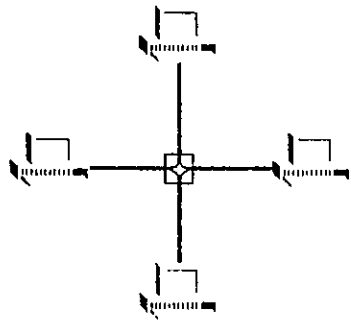


Figura 1.7

- **Bus en estrella**

En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores (figura 1.8).

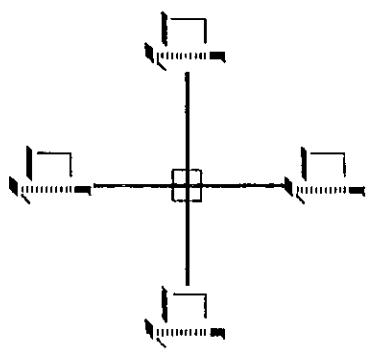


Figura 1.8

- **Estrella jerárquica**

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

- **Malla en estrella**

En este caso se tiene una configuración física tipo estrella (figura 1.9), pero el manejo lógico de la red es simulando una topología malla. Este caso es muy confiable porque todas las computadoras están conectadas al concentrador principal que es el centro de la estrella y a su vez se conectan entre ellas, por lo que si una línea de conexión falla se tienen otras alternativas para llevar a cabo la conexión. Su posible desventaja es que al haber tantos canales de comunicación la red puede alentarse un poco en cuanto a la transferencia de información.

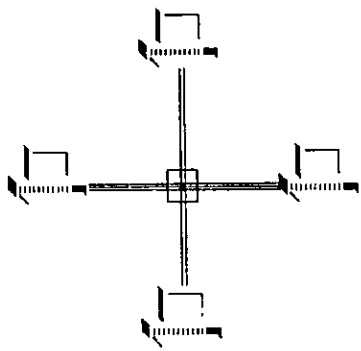


Figura 1.9

- **Estrella en estrella**

No siempre las topologías física y lógica tienen que ser distintas (figura 1.10).

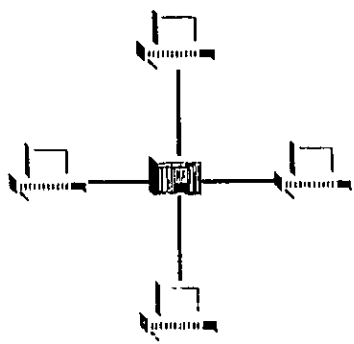


Figura 1.10

En estos casos podemos notar que en redes locales (LAN) el cableado debe tener siempre la topología física de estrella, sin importar la topología lógica, salvo en casos plenamente justificados.

1.3.2 Medios de transmisión para redes

El medio físico es el medio sobre el que se envían las señales eléctricas para realizar la transmisión de la información.

Las personas que tienen que instalar los cables para las redes, tendrán que evaluar detenidamente las necesidades actuales y futuras, así como los requisitos de las aplicaciones multimedia de alto ancho de banda, videoconferencia e imágenes.

El cable y el equipo que utilice el cable deben cumplir con:

- Los requisitos de transmisiones actuales y futuros.
- Las características eléctricas adecuadas.
- Soportar cualquier topología de red.

Cabe aclarar que el medio físico empleado es totalmente independiente del protocolo que se use. Podemos por ejemplo, usar el protocolo TCP/IP sobre cable coaxial, par trenzado, red telefónica o fibra óptica.

1.3.2.1 Medios terrestres

Los medios de transmisión terrestres más comunes, son los conductores de cobre que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable.

A continuación se presentan los tipos de cables más utilizados para la transmisión de datos.

Coaxial

Fue el primer tipo de cable que representó una opción viable para transmisiones seguras, soportando múltiples productos para las redes de área local. Su popularidad comenzó con los orígenes de Ethernet (protocolo que cubre las capas física y de enlace del modelo OSI), que utiliza una topología de tipo bus con el método de acceso CSMA/CD, pero hoy en día se encuentra prácticamente en desuso.

Enseguida se mencionan los tipos de cable coaxial que fueron los más comunes:

- **Coaxial banda base**

Como cable coaxial proporcionó un buen ancho de banda e inmunidad al ruido. Era un alambre de cobre duro en su parte central, rodeado de una capa aislante. Este material aislante estaba rodeado de un conductor cilíndrico que frecuentemente era una malla metálica.

- **Coaxial delgado (10BASE2)**

También se le llamó 'cheapernet' o 'Thin Ethernet'. Su longitud máxima soportada era de 185 metros y no se podían conectar mas de 30 equipos ni haber más de 0.5 metros entre cada uno. Usaba conectares BNC.

- **Coaxial grueso (10BASE5)**

También se le llamó 'Thick Ethernet'. Su longitud máxima fue de 500 metros. Usó conectores tipo vampiro. Era un cable grueso y muy poco manejable.

- **Twinaxial**

Fue una variación del coaxial que disponía de dos conductores centrales, envueltos cada uno en un aislante. Se utilizó en instalaciones de redes de tipo Token Ring

- **Coaxial dual**

Constaba de dos cables coaxiales individuales colocados en una funda común (los cables eran conectados independientemente a las mallas exteriores) para ajustarse o acomodarse a redes que requerían dos conexiones independientes de los cables.

- **Trunk**

Es el nombre general asociado con el Ethernet grueso (thick coaxial) o cable CATV (sistema de televisión por cable).

Sus *aplicaciones* corren a velocidades bajas de pocos Mbps. La clasificación general de las aplicaciones de voz incluye redes locales, sistemas servidores y terminales, CATV, sistemas de seguridad, y sistemas de datos de alta velocidad (T-3).

Algunas *ventajas* fuertes del coaxial incluyeron:

- Inmunidad a las señales de interferencia EMI, por su estructura con el conductor central completamente cubierto por una malla conductora.
- Soporta una amplia variedad de sistemas de redes, por su gran ancho de banda.
- Facilita la unión y terminación pese a lo voluminoso y poco flexible.

Entre las *limitantes* del coaxial se mencionan las siguientes que lo hicieron caer en desuso:

- Los cables previamente instalados no pueden ser reusados en nuevos sistemas.
- Debido a su diámetro más grueso, requiere espacio adicional.
- Tienen gran tamaño y poca flexibilidad.
- Era difícil su mantenimiento y búsqueda de fallas.
- Su costo era alto.

Par trenzado

El cable de par trenzado consta de conductores de núcleo de cobre rodeados por un aislante. Se trenzan dos conductores juntos para formar un par y dicho par forma un circuito por el que se pueden transmitir datos. Un cable consta de uno o más pares trenzados rodeados por un aislante, como se ve en la figura 1.11. Este cable es susceptible a campos magnéticos, por lo que el par de alambres de cobre es encerrado individualmente dentro de un material aislante que los separa para que luego sean trenzados conjuntamente. El material aislante debe cumplir un esquema de codificación de color, el conjunto de colores representa el positivo y el negativo para cada par.

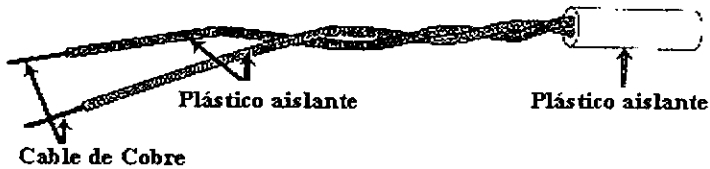


Figura 1.11

Características

Los alambres tienen un diámetro de entre 20AWG (estándar AWG: American Wire Gauge) y 26AWG. Estos son de cobre o acero cubierto por cobre. El cobre provee conductividad y el acero da firmeza. Un par de alambres actúa como una simple liga de comunicación.

Debe mantenerse una proporción de trenzado circular por cada par; de entre 2 a 12 trenzados por cada 2.54 cm, el cuál ayuda a inmunizar al cable contra el ruido y crosstalk (interferencia electromagnética que se genera en cada par).

Las características de impedancia de su alambre oscilan entre 90 y 110 Ohms.

Este tipo de cable se utiliza en Ethernet, red en anillo con paso de testigo y otras topologías de red. Se usa tanto para la transmisión analógica (ejemplo: líneas telefónicas) como para la transmisión digital (ejemplo: redes de datos).

Su ancho de banda depende de la distancia y el calibre del alambre.

Los tipos de par trenzado son:

- **Par trenzado con malla o blindado (STP, Shielded Twisted Pair).**

Este tipo de cable está formado por grupos de dos conductores cada uno con su propio aislante trenzados entre sí y rodeados de una malla de material conductor, recubierta a su vez por un aislante. Cada grupo se trenza con los demás que forman el cable y, el conjunto total se rodea de una malla conductora y una capa de aislante protector. Esta disposición reduce las altas interferencias externas, las interferencias entre pares y la emisión de señales producidas por las corrientes que circulan por el cable.

Comparado con otros tipos de líneas de par trenzado:

- Es más caro que el UTP.
- Puede trabajar a más de 100 Mb/s.
- La longitud puede llegar a 250 metros.

El uso común de este tipo de cables es la conexión de los tranceptores insertados en el coaxial de una red 10BASE5 con la tarjeta de red de una estación.

- **Par trenzado sin malla o sin blindaje (UTP, Unshielded Twisted Pair).**

Es el cable par trenzado típico, esto es, no lleva ningún tipo de blindaje de metal siendo de esta manera más susceptible a interferencias electromagnéticas (EMI) o crosstalks.

En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales. Estos cables se utilizan, sobre todo, para los sistemas de cableado integral, combinando telefonía y redes de transmisión de datos, principalmente 10BASET.

Sus características básicas son:

- Es bastante barato.
- Puede alcanzar hasta los 100 Mb/s de velocidad.
- La longitud máxima son 100 metros.

- **Par trenzado Plenum Rating.**

Es llamado así por su característica de ser un cable aislado por un material que ha sido certificado para no exhalar humo tóxico cuando se quema o se calienta. Por lo que es instalado a través de los ductos de calefacción o aire acondicionado en las oficinas. Los cables tipo plenum decrementan la flexibilidad del cable debido a que incrementa su diámetro, además de que aumenta el costo. Se encuentra en versiones UTP y STP.

Categorías para cables par trenzado:

Categoría 1

Es el cable telefónico de par trenzado sin malla tradicional por el que se puede transmitir voz, pero no datos. La mayoría del cable telefónico instalado antes de 1983 es de esta categoría.

Categoría 2

Es el cable de par trenzado no blindado (sin malla) certificado para la transmisión de datos hasta 4 Mbps y similar al tipo 3 del sistema de cableado de IBM. Este cable tiene cuatro pares trenzados.

Categoría 3

Admite velocidad de transmisión de 10 Mbps y es necesario para las topologías de red en anillo con paso de testigo (4 Mbps) y Ethernet 10 Base-T a 10 Mbps. El cable tiene cuatro pares y tres trenzas por cada pie de longitud.

Categoría 4

Está certificado para velocidades de transmisión de 16 Mbps y es la calidad inferior aceptable para topologías de red en anillo con paso de testigo a 16 Mbps. El cable tiene cuatro pares.

Categoría 5

Es cable de cobre de par trenzado a cuatro hilos de 100 ohms, que puede transmitir datos hasta 100 Mbps para admitir las tecnologías más recientes como Fast Ethernet y ATM. El cable tiene una baja capacidad y presenta una baja diafonía.

Categorías 6 y 7

Aunque los estándares para estas categorías no se han definido, en 1998 han empezado a salir al mercado productos para estas. Este cable es conocido como GigaSPEED y soporta aplicaciones que requieren gran ancho de banda. Se espera que el cable de categoría 6 tenga un ancho de banda entre 200 y 250 MHz, mientras que el de categoría 7 posiblemente opere a 600 MHz.

Aplicaciones

Son los cables que se utilizaron primero y su calidad era muy pobre para transportar información a alta velocidad. Hoy en día ha llegado a ser una parte fundamental en cualquier tipo de construcción de sistema de cableado, ya que es el medio para diferentes tipos de aplicaciones que van desde los sistemas PBX hasta redes locales.

Ventajas

A continuación se mencionan algunas de los puntos que consideramos ventajas del par trenzado:

- Bajo costo, debido al gran número de proveedores que venden y dan servicio para este tipo de cable.
- Simplifica el diseño y configuración, pues involucra una topología tipo estrella con un concentrador central que facilita el aprovechamiento de la configuración y simplifica su instalación.
- Dado a su gran auge en el mercado, existe una gran cantidad de personal calificado, disponible para instalaciones de par trenzado.
- Presenta una fácil instalación en muchas situaciones, incluyendo nuevas construcciones y renovación del cableado en edificios, esto es debido a su pequeño diámetro y extrema flexibilidad.
- Su configuración tipo estrella con un concentrador central, hace que sea fácil predecir los defectos en la instalación y ayuda en su solución (si un cable llega a dañarse, es muy fácil aislarlo y repararlo por separado).

Desventajas

- Mientras que el cable coaxial y la fibra óptica pueden ofrecer proporciones de transmisión arriba de 45 a 600 Mbps el par trenzado está limitado de 16 a 20 Mbps.
- Limitaciones de distancia, todo depende de la construcción del sistema de cableado.
- Es muy susceptible a EMI, dichas señales pueden ser originadas por varias razones incluyendo líneas de poder, maquinaria u otro cable par trenzado. Lo cual puede incrementar errores sobre una señal de comunicaciones.

Fibra óptica

La fibra óptica es una especie de filamento mucho más delgado que un cabello, flexible, generalmente las fibras esta hechas de sílice (combinación de silicio y oxígeno), y algún tipo de vidrio, pero este vidrio es de muy alta calidad, por lo cuál es capaz de transportar rayos de luz en su interior de una manera determinada.

Consta de dos porciones sólidas: el núcleo y el revestimiento, estas dos porciones no pueden ser separadas (figura 1.12). La luz viaja a través del núcleo mientras el revestimiento guarda la luz contenida dentro del núcleo. Esto es realizado para tener índices diferentes de refracción entre éstas porciones.

El núcleo consiste de vidrio o cuarzo, que tiene un índice de refracción más alto que el del revestimiento de vidrio, cuarzo o plástico que lo rodea.

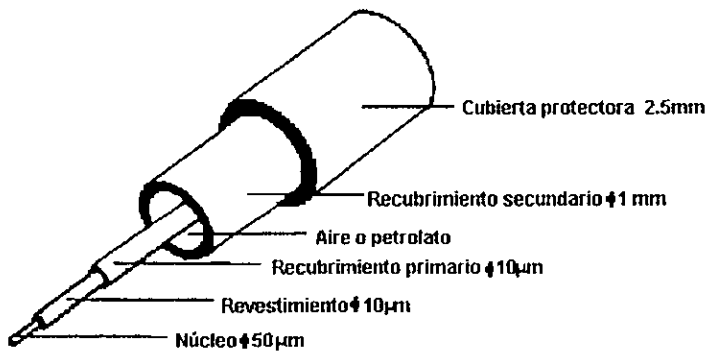


Figura 1.12

A su vez la superficie del revestimiento esta protegida por otras 4 capas más que son: recubrimiento primario, aire o petrolato, recubrimiento secundario y una cubierta protectora.

El recubrimiento primario es típicamente de acrílico y existe sobre todas las fibras. Su propósito es darle más fuerza a la fibra, durante el cableado, el empalme y al poner los conectores. Su diámetro es de aproximadamente 250 micras

El aire o petrolato está entre la cubierta primaria y el recubrimiento secundario y sirve para que el filamento se encuentre libre y manejable. El recubrimiento secundario mide aproximadamente 1 mm.

Por último, la cubierta protectora mide 2.5 mm aproximadamente y es la que protege a la fibra contra esfuerzos mecánicos debidos al cableado, instalación, cambios de temperatura, etc.

El tamaño de la fibra óptica se especifica citando el diámetro del núcleo y del revestimiento en micras. Por ejemplo 62.5/125 micras especifica una fibra con un núcleo de 62.5 micras con un diámetro de revestimiento de 125 micras.

En la fibra óptica en lugar de señales eléctricas se usan señales luminosas (fotones) por un núcleo de dióxido de silicio, tan puro que una ventana de cinco kilómetros de gruesa construida con este material no distorsionaría la vista. Las transmisiones fotónicas no producen emisiones fuera del cable y no se ven afectadas por la radiación externa.

Se recomienda el cable de fibra cuando la seguridad es clave. Las señales de las computadoras se transmiten por el cable de fibra óptica convirtiendo los 1 y los 0 electrónicos en pulsos de luz (un pulso de luz se usa para indicar un bit de valor 1, la ausencia de un pulso indicará la existencia de un bit de valor 0). Un diodo emisor de luz en un extremo emite pulsos de luz por un cable que recogen en el otro extremo con un sencillo fotodetector y se vuelven a convertir en señales eléctricas. Como las señales prácticamente no encuentran resistencia y no hay emisiones, las tasas de transmisión por cable de fibra sólo están limitadas por la pureza del núcleo de cristal, la calidad de los equipos y la velocidad de la luz.

En un sistema de transmisión óptica podemos distinguir tres elementos:

- El medio de transmisión: Es una fibra muy delgada de vidrio o silicio fundido.
- El detector: Es un fotodiodo que percibe los pulsos de luz y los transforma en señales eléctricas.
- La fuente de luz: Puede ser un LED (diodo emisor de luz) o un diodo láser, que convierte las señales eléctricas en pulsos de luz que se pueden transmitir a través de la fibra óptica.

Teniendo en cuenta el modo de propagación, las fibras ópticas se clasifican en:

- **Monomodo**

La anchura del núcleo es igual a la longitud de onda de la luz, por lo que la luz no se propaga refractándose, sino que viaja en línea recta, lo que implica que no existe dispersión modal (hay un solo modo de propagación) y por tanto el ancho de banda es mayor.

- **Multimodo**

Multimodo significa que varios rayos entran con distintos ángulos. Contiene varios modos de propagación y ocurre en consecuencia al efecto de dispersión. Tiene un núcleo muy grande, 50 micras, comparado con la longitud de onda de la luz. En la fibra multimodo la luz se propaga refractándose

A su vez estas últimas se subdividen en:

1. **Índice escalonado.** Tiene dispersión, reducido ancho de banda y son de bajo costo, dado que resultan tecnológicamente sencillas de producir.

2. **Índice gradual**. Más costosas pero de gran ancho de banda. Se puede disminuir la dispersión haciendo variar lentamente el índice de refracción entre el núcleo y el recubrimiento.

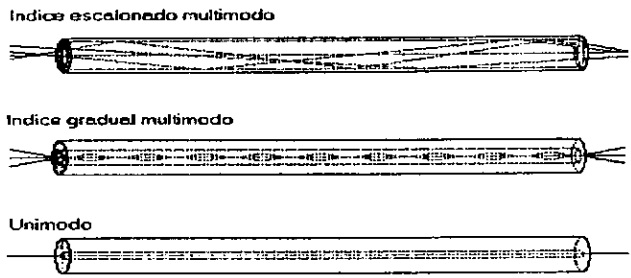


Figura 1.13

Aplicaciones

La fibra óptica puede ser usada para señalización, transmisión de información e incluso en aplicaciones de control.

Sobre la fibra óptica se puede usar otro protocolo que cubra el nivel de enlace, como por ejemplo el Ethernet.

Es muy frecuente el uso de la fibra óptica para construir anillos con el protocolo FDDI. El FDDI consiste en un anillo doble de fibra óptica (monomodo o multimodo) al que se conectan los diferentes equipos. Los dos anillos son usados simultáneamente, uno para recibir y otro para transmitir. En caso de que uno de los anillos caiga, se puede seguir transmitiendo y recibiendo información por el otro. La velocidad alcanzable con FDDI es 100 Mbps.

Ventajas

- Una baja atenuación por kilómetro cuando se transmite por las llamadas ventanas de transmisión, que están ubicadas en torno a los valores siguientes de longitud de onda: 0.8 nm, 1.3 nm y 1.55 nm. Esta última ventana es la que presenta menor atenuación.
- Total inmunidad al ruido y a las interferencias electromagnéticas, lo que constituye un medio especialmente útil en ambientes con alto ruido.
- Uso de potencias del orden de los mW, en comparación con otros medios de comunicaciones que requieren potencias mayores.
- Su pequeño tamaño y poco peso, hacen de ellas medios de comunicaciones fáciles de instalar, especialmente cuando se trata de completar sistemas sobre ductos preexistentes, sobrecargados por otro tipo de medios que no es posible eliminar.
- El índice de refracción de la fibra es de 1.45 aproximadamente, lo que implica que la velocidad de la luz en la fibra es alrededor de 0.7 la velocidad de la luz en el vacío.
- En la fibra óptica la dispersión es menor, por lo que el número de pulsos que se pueden emitir por unidad de tiempo es muy alto.

Líneas telefónicas

Cuando hablamos de líneas telefónicas debemos distinguir entre líneas punto a punto y la red telefónica conmutada (RTC).

- **Red telefónica Conmutada (RTC)**

La RTC son las líneas que se usan para la comunicación telefónica. Estas líneas son analógicas, por lo que se precisa de aparatos conversores analógico-digital y digital-analógico. Estos aparatos son los módems.

Sobre la red telefónica conmutada se puede 'levantar' el protocolo TCP/IP, aunque este es probablemente el medio físico menos adecuado.

El costo de uso de estas líneas es similar al de una llamada telefónica. Además de que permite la comunicación móvil desde cualquier equipo portátil conectado a través de ellas.

Si se va a hacer un uso elevado de estas líneas deberemos pensar en descartar la RTC y pasar a líneas punto a punto porque resultará más económico y la comunicación será más rápida y fiable.

- **Líneas punto a punto**

Es un método bastante usado para unir edificios que se encuentran a varios kilómetros de distancia.

Se trata de un tipo especial de líneas (digitales) que nada tiene que ver con la RTC tradicional. Por estas líneas se paga un alquiler mensual fijo, independientemente del uso que se haga de ellas, por ello son interesantes cuando se va a hacer mucho uso de la línea. Para un uso más esporádico es más barata la conexión por RTC.

1.3.2.2 Medios Aéreos

Los medios aéreos o no guiados representan la nueva técnica que se utiliza para transmitir señales por el aire y el espacio desde el transmisor al receptor, tales como infrarrojos y microondas. Con este medio se pueden cubrir distancias más grandes.

Los medios más comunes en la actualidad son:

Satélite

Los satélites de comunicaciones orbitando sobre un punto fijo de la tierra, reciben las señales de radio de un amplificador en tierra y las transmiten a su destino. La señal del satélite es recibida por una antena parabólica y se distribuye localmente mediante cables. Este medio se utiliza cuando la comunicación cubre millones de kilómetros.

Microondas

Las señales de microondas deben viajar sin obstrucciones, por esto las torres de retransmisión son instaladas en cimas de colinas y montes para enviar las señales sobre terrenos disparejos. También las torres de microondas son instaladas en techos elevados para enlazar oficinas que no están muy distantes.

Radio

Las ondas de radio fueron el primer medio utilizado para transmitir información y, gracias a los avances tecnológicos como la telefonia celular y el auge de los equipos portátiles, se están convirtiendo en uno de los medios de transmisión más utilizados en la actualidad. Las ondas de radio pueden transmitir en distintas frecuencias. También pueden ser utilizadas en una escala geográfica más amplia.

Luz

La luz se utilizó aún antes que la radio para transmitir información, ya los griegos utilizaban espejos para comunicarse con sus barcos en el mar. Pero ha sido necesario mejorar los sistemas de producción de luz láser para permitir transmitir información electrónica con velocidades similares a los cables. Ya existen equipos que pueden establecer enlaces de varios kilómetros a 5-10 Mbps con alto costo.

1.3.3 Protocolos de control de acceso al medio

En todas las redes locales sus dispositivos deben compartir la capacidad de transmisión de la red. Por esta razón es necesario tener un control de acceso al medio de transmisión para que dos dispositivos particulares puedan intercambiar datos cuando sea requerido dentro de un esquema centralizado o distribuido.

En un esquema *centralizado*, se designa un controlador con la suficiente autoridad para garantizar el acceso a la red. De esta manera, una estación que desee transmitir deberá esperar a recibir el permiso del controlador. En una red *decentralizada*, las estaciones colectivas desarrollan una función de control de acceso al medio para determinar dinámicamente el orden en el cuál transmitirán las estaciones.

En general se puede clasificar a las técnicas de control de acceso en *síncronas* y *asíncronas*. Con las técnicas síncronas, una capacidad especifica es dedicada para realizar una conexión, se utiliza en redes locales de circuitos conmutados (cabe mencionar que no son muy óptimos para redes LANs y WANs ya que las necesidades de transmisión de las estaciones pueden ser impredecibles). Otra forma más eficaz para redes locales, serían las técnicas asíncronas, las cuales se pueden subdividir en tres categorias: **round robin, reservación y contención**.

Round Robin

Esta técnica está basada en darle a cada quien un turno. A cada estación en turno se le da la oportunidad de transmitir, durante este turno la estación puede declinar la transmisión o puede transmitir sujeto a un cierto límite. El control en esta técnica

puede ser de modo distribuido o centralizado. Este tipo de control de acceso es utilizado en las topologías en bus mediante token bus indicado en el estándar IEEE 802.4 y en topologías anillo mediante token ring basado en IEEE 802.5 y FDDI.

Reservación

En esta técnica, el tiempo sobre el medio de transmisión es dividido en paquetes (frames). Una estación que desea transmitir, reserva paquetes futuros para un período indefinido. La reservación de los paquetes puede llevarse a cabo de una manera distribuida o centralizada. Este tipo de control de acceso es regularmente usado en topologías en bus mediante DQDB, estándar IEEE 802.6 y en anillo mediante FDDI-II, cabe señalarse que tanto como DQDB como FDDI-II por ser protocolos para tráfico de circuitos conmutados no son completamente especificados en los estándares y pueden ser distribuidos o centralizados.

Contención

Con esta técnica no se ejerce el control para determinar que estación tiene derecho a transmitir sino que todas contienden por el tiempo. Es necesariamente distribuida. Para topologías en bus, se establece mediante CSMA/CD del estándar IEEE 802.3, en topologías anillo no es utilizada.

Las técnicas que han sido adoptadas para ser utilizadas en topologías de bus y árbol son:

- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection: Acceso Múltiple con Censado de Portadora / Detección de Colisiones).
- **Token Bus** (control del token).

Mientras que para la topología de anillo son:

- **Token Ring** (control del token).
- **Inserción de Registros.**
- **Anillo Ranurado** (Slotted ring).

A continuación se describen brevemente las técnicas antes mencionadas.

CSMA/CD

El método de acceso al medio CSMA/CD es únicamente utilizado en redes de tipo bus. Con esta topología, todas las máquinas son conectadas directamente al mismo cable o medio de transmisión. El medio, dicho de esta manera, sirve para operar en un modo de acceso múltiple.

Todos los datos son transmitidos por una computadora que primero los encapsula dentro de un paquete de información (frame) con la dirección de la computadora destino en el encabezado de cada paquete; el paquete es entonces transmitido o difundido sobre el medio. Todas las computadoras conectadas al medio, detectan al

momento que un paquete está siendo transmitido de esta forma. Cuando la computadora requerida como destino detecta que el paquete de información que actualmente es transmitido tiene su propia dirección en el encabezado, lee la información contenida dentro de este y responde de acuerdo al protocolo de comunicación definido. La dirección del remitente es incluida como parte del encabezado del paquete, así que el receptor puede dirigir su respuesta a la computadora de origen.

Con este tipo de técnica, es posible que dos o más computadoras transmitan un paquete sobre el medio cuando este se encuentra ocupado por otro paquete, causando de esta manera que los paquetes; de las computadoras transmisoras sean corrompidos al ocurrir una colisión entre ellos. Para reducir la posibilidad de este suceso antes de que un paquete sea transmitido, cada computadora fuente primeramente escucha eléctricamente al medio, lo que es llamado **censo de señal de portadora** (CS: Carrier Sense) para detectar si un paquete esta siendo transmitido actualmente. Si una señal de portadora es censada o detectada, la computadora fuente detiene su intento de transmitir hasta que el paquete que está en el medio haya sido transmitido completamente, solo entonces la computadora fuente tratará de enviar su paquete. De la misma forma, dos computadoras deseosas de transmitir un paquete pueden determinar simultáneamente que no existe actividad de transmisión sobre el medio (paquetes sobre el bus), y de aquí que ambas empiecen a transmitir sus paquetes al mismo tiempo. De esta forma también ocurrirá una colisión. La computadora fuente simultáneamente monitorea la señal del medio a la vez que transmite los datos de un paquete. Si las señales de los datos transmitidos y los monitoreados son diferentes, la computadora asume que ha ocurrido una colisión, esta operación es llamada **detección de colisión** (CD: Collision Detection). De esta manera al detectar la colisión, la computadora cesa la transmisión del paquete de datos y da seguimiento a la colisión transmitiendo un bit patrón aleatorio por un corto período de tiempo, el cuál es conocido como **señal de secuencia de congestión** (Jam Sequence).

Esta señal asegura que todas las computadoras se hallan percatado de que ha ocurrido una colisión. Después de que todas las computadoras involucradas en la colisión conocen el suceso, esperan durante un pequeño intervalo de tiempo aleatorio, antes de intentar retransmitir los paquetes afectados.

Basándose en lo anterior se puede concluir que el protocolo de acceso al medio para bus CSMA/CD, es probabilístico y depende de la carga de la red.

Token Bus y Token Ring

Otra manera de control de acceso para compartir el medio de transmisión es por el uso de un control (permiso) de señal (token). Esta señal (o token) es pasada desde una computadora a otra, de acuerdo a un conjunto de reglas entendidas y apegadas por todas las computadoras conectadas al medio. Una computadora solo puede transmitir su frame cuando tiene posesión de la señal token y después que ha transmitido el paquete de información pasa este token a otra computadora, permitiéndole el acceso al medio de transmisión. Por el desuso de este método solo mencionaremos brevemente su funcionamiento.

La secuencia de operación de la técnica de control token es la siguiente:

1. Se establece una estructura de anillo lógico al cuál se ligan todas las computadoras conectadas al medio físico y se crea una señal única de control de permiso (token).
2. La señal de control token es pasada de una máquina a otra, recorriendo el anillo lógico hasta que llega a una computadora que espera enviar un paquete de información.
3. La computadora que espera para la transmisión cuando es poseedora de la señal de token, envía su paquete o paquetes de información a través del medio físico. Una vez concluida la transmisión pasará la señal de control a la siguiente computadora en el anillo lógico.

Aunque las funciones de monitoreo son normalmente efectuadas entre todas las computadoras sobre el medio, sólo una a la vez acarrea la responsabilidad de recuperación y reinicialización.

El medio físico no necesariamente debe tener una topología de anillo; una señal de token puede ser también utilizada para control de acceso a una red en bus. En esta topología se hace un arreglo de anillo lógico.

Con una topología de anillo físico, la estructura del anillo lógico (token passing ring) es la misma que la del anillo físico, con el orden de la señal token pasando de acuerdo al orden de la estructura física de las computadoras conectadas. Con este control de acceso al medio sobre una estructura de bus física, todas las computadoras no necesariamente deben estar conectadas dentro del anillo lógico. Esto significa que una computadora conectada al bus pero no conectada al anillo lógico, puede operar sólo en estado de recepción, teniendo en cuenta que nunca será propietaria de la señal token; por lo tanto nunca podrá trasmitir, esta situación se muestra en la figura 1.14.

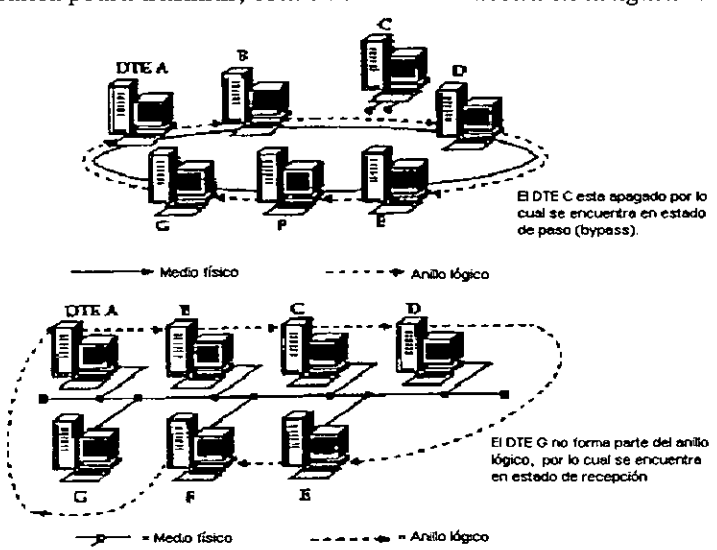


Figura 1.14

Otra caracteristica del método de acceso al medio con señal de token, es la de poder asociar una prioridad con la señal de token, por medio de esto se permite transmitir primero a los paquetes con mayor prioridad.

Inserción de Registros

Esta técnica deriva su nombre del **registro de cambio** asociado con cada nodo conectado al anillo. El registro de cambio, el cuál es igual en tamaño a la longitud máxima del frame, es utilizado temporalmente, manteniendo frames que circulan por el nodo. En adición, cada nodo tiene un buffer para almacenar los frames producidos localmente. En la figura 1.15 se muestra esta estructura:

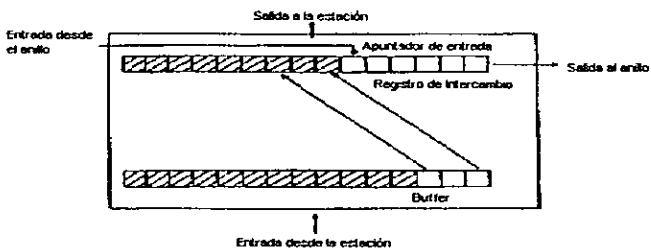


Figura 1.15

A continuación, se explican los dos casos principales que se pueden tener en el anillo de registro de inserción.

El *primer* caso se considera cuando una computadora no tiene datos para enviar, por tal motivo se realiza simplemente el manejo de frames de datos que circulan por su posición. Cuando la posición del apuntador de entrada del registro de cambio se encuentra en la parte más a la derecha de éste registro, indica que el registro está vacío. Cuando los datos llegan provenientes del anillo, estos son insertados bit por bit en el registro de cambio y el apuntador de entrada va cambiando de posición hacia la izquierda. Cada paquete de datos recibido desde el anillo empieza con un campo de encabezado de direccionamiento, tan pronto como este campo se encuentre completamente dentro del registro de cambio, la estación puede determinar si es o no el destinatario del paquete. En caso de que no sea, el paquete será retransmitido al anillo, al intercambiarlo bit por bit hacia la salida del registro de cambio. Si durante este lapso de tiempo no llega un paquete adicional, el apuntador de entrada retornará a su posición inicial (parte más a la derecha); de otra manera, un segundo frame empezará a acumularse en el registro de cambio al mismo tiempo como el primero es enviado fuera hacia el anillo. Cabe notar que más de un frame puede encontrarse sobre el anillo en el mismo instante de tiempo y que se podrían tener una serie de paquetes con huecos entre ellos pasando por el nodo de una computadora, lo que permitiría insertar nuevos paquetes en el anillo.

Si un frame llegase con la dirección de la computadora en cuestión, la computadora tendría dos opciones para elegir: Una puede ser desviar el resto del frame para ella misma y borrar los bits del campo de dirección, de esta manera se purga el frame del anillo. O retransmitir el frame mientras se copian sus datos hacia la computadora local en cuestión.

Ahora considerando el *segundo* caso, en el cuál, la computadora tiene datos para transmitir. Se coloca un frame para ser transmitido en el buffer de salida. Si la linea y el registro de cambio se encuentran vacios, el frame puede ser transferido inmediatamente del buffer hacia el registro de cambio. Si el frame consta de una longitud de *n* bits menor que el tamaño máximo estipulado en el anillo y si al menos *n* bits están vacios en el registro de cambio, los *n* bits son transferidos en paralelo a la porción vacía del registro y al mismo tiempo el apuntador de entrada es ajustado.

Mientras el anillo se encuentre ocioso, una computadora con muchos datos para transmitir puede enviar frame tras frame, utilizando enteramente el ancho de banda del anillo. Sin embargo, si el anillo se encuentra ocupado, la computadora encontrará que, después de enviar un frame, el registro de intercambio no acomodará otro frame. Por lo que deberá esperar hasta que exista un hueco entre mensajes lo suficientemente grande para poder colocar el suyo, teniendo entonces que acumular los frames locales hasta poder enviarlos.

La principal ventaja de esta técnica, es que lleva a cabo la utilización máxima del anillo de entre cualquiera de los otros métodos, permite la utilización de frames de longitud variable y múltiples frames sobre el anillo al mismo tiempo. La principal desventaja que se tiene, es el mecanismo de purgado sobre el anillo, esto es, el permiso de múltiples frames sobre el anillo requiere que el reconocimiento de la dirección se haga antes de que el frame sea removido por el transmisor o por el receptor, esto nos lleva a que si una dirección del frame es alterada, el frame puede circular indefinidamente. Una posible solución a este problema es el uso de un código de detección de errores sobre el campo de direccionamiento.

Anillo ranurado

Es llamado así porque sobre el anillo circulan continuamente varios paquetes (frames) de longitud fija llamados ranuras.

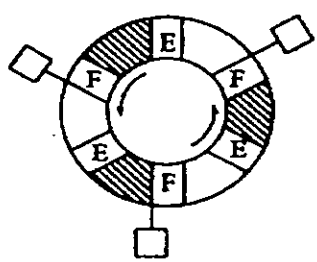


Figura 1.16

Cada ranura contiene un bit en el encabezado el cuál indica si una ranura se encuentra llena o vacía. Inicialmente todas se encuentran vacías. Cuando una computadora desea transmitir deberá repartir los datos en varios frames con una longitud fija y entonces esperará a que llegue una ranura vacía; en este momento marcará la ranura como llena e insertará los datos sobre la ranura. La computadora no podrá transmitir otro paquete hasta que la ranura ocupada regrese. Una ranura

hace un viaje redondo para ser marcada de nuevo como vacía por la computadora transmisora. Cada computadora conoce el número total de ranuras existentes sobre el anillo.

La principal desventaja del anillo ranurado (figura 1.16) es su desperdicio de ancho de banda. Cada paquete de datos debe ser de una longitud lo suficientemente pequeña para poder adaptarse a la ranura, resultando con esto una gran cantidad de sobrecarga. Además, una computadora puede enviar sólo un paquete por viaje redondo a la vez. Si sólo una computadora tiene paquetes por transmitir, varias ranuras circularán vacías. Su principal ventaja es su simplicidad.

Cabe mencionarse que los métodos de acceso al medio antes descritos, sirven para la transferencia de archivos, audio y facsímile.

1.3.4 Estándares de redes.

Como ya se menciono antes, desde el surgimiento y desarrollo de las redes a finales de los años 70's cada compañía fabricante tenía sus propias arquitecturas y protocolos para conectar sus equipos, lo que provocó los llamados sistemas propietarios o sistemas cerrados. Debido a esto y con ayuda de los organismos internacionales de estandarización, se han formulado y aceptado un conjunto de estándares para las redes, con los que se formaron los sistemas abiertos conocidos actualmente. Y aunque los estándares imponen algunas limitaciones para los desarrolladores de los sistemas, son la mejor respuesta para resolver el problema de la intercomunicación de diversos equipos de comunicación y programas de diferentes proveedores.

1.3.4.1 Estándares del IEEE

Uno de los organismos que tuvo un mayor desempeño en esta actividad fue el IEEE el cual desarrolló la serie de estándares conocido como IEEE 802.x para redes de área local (LAN). El 802.x ha sido adoptado por ISO como un estándar internacional.

El estándar 802.x está integrado por varios subcomités, lo que proporciona una mayor flexibilidad para cubrir las diferentes necesidades de los diseñadores de redes. Estos subcomités están organizados de la siguiente manera:

802.1 Interfaces de alto nivel (HLI: High Level Interface) y puentes MAC.
802.2 Control de Enlace Lógico (LLC: Logical Link Control).
802.3 Carrier Sense Multiple Access/Collision Detection (CSMA/CD).
802.4 Token Bus.
802.5 Token Ring.
802.6 Redes de Área Metropolitana (MAN: Metropolitan Area Networks).
802.7 Broadband Technical Advisory Group
802.8 Fiber Optic Technical Advisory Group
802.9 Integrated Data and Voice Networks
802.10 LAN security
802.11 Redes inalámbricas (wireless LANs)
802.12 100VG AnyLAN

Los subcomités del IEEE abarcan las 2 capas inferiores del modelo de referencia OSI: la capa física y la capa de enlace de datos. Enseguida se describen los subcomités antes mencionados.

Interfaz de redes de alto nivel (IEEE 802.1)

Este subcomité trata asuntos comunes entre todos los subcomités 802 de redes LAN, en los que se incluyen: el sistema de direcciones, la administración de las redes y los puentes (bridges); además de la relación entre las normas 802.x del IEEE y el modelo de referencia OSI.

Sistema de direcciones del IEEE 802

Las redes locales, al ser de tipo multipunto, hacen que cada computadora conectada a la red examine uno a uno los paquetes que se transmiten por la misma, por lo que es necesario que cada paquete contenga dos campos de dirección: un campo con la dirección de la computadora destino y otro, con la dirección de la computadora origen. Para prevenir que cada computadora interrumpa sus actividades por cada paquete que examina, es necesario, que las interfaces de red filtren los paquetes que no contienen su dirección en el campo destino.

Por lo anterior el subcomité 802.1 llevó a cabo la estandarización del sistema de direcciones para redes locales; estableciendo una longitud de 48 bits (El rango de una dirección entera por lo tanto es de 6 octetos) para cada dirección. Este argumento es suficiente para proveer un identificador global único para cada dispositivo de red. Por tanto cada dispositivo tiene una dirección física única, la cuál es asignada por el fabricante en el momento de su fabricación (esta dirección es referida también como dirección de hardware o MAC).

Actualmente la organización IEEE es la autoridad administrativa universal para la asignación y manejo de bloques o rangos de direcciones. Cuando un fabricante desea construir equipo que se enlazará en red, primeramente debe contactar a la autoridad global para obtener un bloque de direcciones.

Al fabricante se le asignan tres octetos de valor fijo (24 bits), esta porción de valor fijo de direcciones es referido también dentro de la industria como código del vendedor u OUI (Organizationally Unique Identifier). Los otros tres octetos o 24 bits identificadores son asignados por el fabricante para cada uno de sus productos.

Actualmente los 24 bits de valor fijo (OUI) tienen una estructura adicional (2 bits de control). El primer bit puede representar un grupo/individual. Si el bit es 0, la dirección se refiere a una computadora particular o individual, y si el bit es 1, la dirección se refiere a que el resto del campo de la dirección pertenece a un grupo lógico de computadoras que necesita mayor resolución. El segundo bit es el bit Universal/Local. Si es 0, quiere decir que la dirección fue establecida por la autoridad administrativa universal (significa que los siguientes 22 bits fueron asignados por el IEEE). Si el segundo bit tiene valor de 1, el campo OUI fue asignado en forma local.

Cabe señalarse que el tipo de asignación local del OUI puede causar problemas de direccionamiento, si se descifra como si se tratara de una dirección asignada por el IEEE.

En la figura 1.17, se muestra el esquema del direccionamiento IEEE 802 antes mencionado:

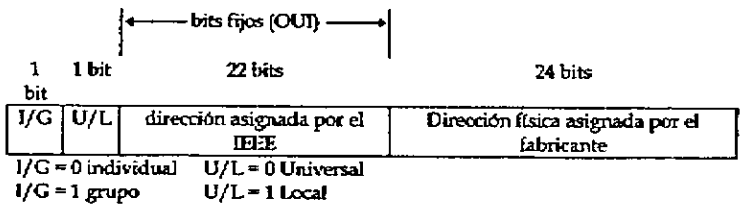


Figura 1.17

Si un fabricante se quedará sin direcciones físicas, el IEEE tiene capacidad de asignarle un segundo OUI identificador. Cabe hacer notar que si sigue la tasa actual de crecimiento es posible que en un futuro se lleguen a agotar los OUIs.

Direcciones multicast y broadcast

Una dirección *multicast* permite a un solo frame ser recibido por un grupo seleccionado de computadoras. Esto hace posible que para un conjunto de computadoras, se les asigne un grupo multicast al cual se le ha dado una dirección multicast específica. Un solo paquete enviado a la dirección multicast asignada a ese grupo será entonces recibido por todas las computadoras incluidas en el mismo.

También existe un caso especial de dirección multicast conocida como dirección *broadcast* o de difusión, la cuál es una dirección donde los 48 bits de dirección son establecidos en valor de 1. Todas las interfaces Ethernet que observen un frame con esta dirección destino leerán el frame recibido y lo entregarán al software de la capa de red de la computadora, lo que en otras palabras quiere decir que en esta ocasión todas las computadoras conectadas a la red local de donde se envió el broadcast recibirán el paquete no importando el grupo al que pertenezcan.

- **802.1 A**

Es responsable de proveer una arquitectura con manejo en red, consistente con el modelo OSI.

- **802.1 B**

Desarrolla protocolos de manejo y administración de redes LAN-MAN. Estos estándares tienen por objeto ser un complemento para los estándares de administración de sistemas OSI. Tales como el CMIP (Common Management Information Protocol) y SMNP (Simple Management Network Protocol) entre otros.

- **802.1 D**

Define el estándar para encaminamiento por medio de puentes (encontrándose bajo consideración por el IEEE), distribuido sobre múltiples redes LAN conectadas a través de estos dispositivos. Este estándar ha adoptado el algoritmo de enrutamiento **Spanning tree,** el cuál es utilizado por puentes para redes locales tipo Ethernet. Se pretende incorporar al estándar algo de encaminamiento del protocolo de IBM para redes tipo anillo llamado **source routing** el cuál forma parte del protocolo 802.5

- **802.1 G**

Ha estado trabajando para desarrollar un estándar para encaminamiento de puentes remotos (remote bridges) en redes de área amplia WANs. El comité ha adoptado para los puentes remotos la utilización del algoritmo de encaminamiento **Spanning tree.**

IEEE y la capa de enlace de datos (data link level)

Los protocolos en el nivel de enlace de datos llevan a cabo la tarea de transmisión eficaz de frames o bloques de datos entre dos nodos adyacentes (sin nodos de conmutación intermedios). Las funciones principales de la capa de enlace de datos son:

- Sincronización lógica del transmisor y receptor.
- Control de flujo de datos.
- Control y detección de errores.
- Secuenciamiento de los paquetes de datos para garantizar una entrega ordenada.

El estándar IEEE divide el nivel de la capa de enlace de datos en dos subniveles: El nivel Control de Acceso al Medio MAC (subcomités 802.3,802.4,802.5 y 802.12) y el nivel Control Lógico de Enlace LLC (subcomité 802.2).

Las funciones asociadas en el nivel de enlace de datos para realizar la transmisión y recepción entre computadoras conectadas a una red local son las siguientes:

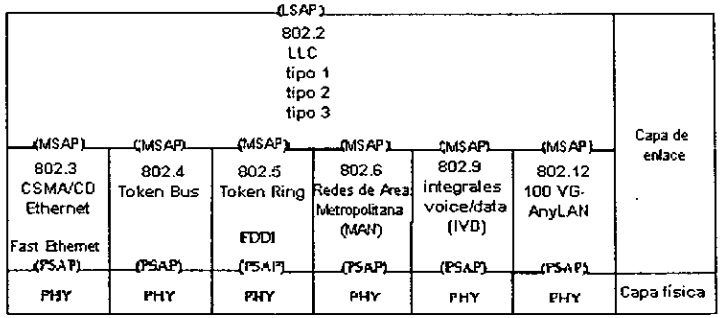
- Proveer uno o más puntos de acceso a servicio SAPs (interfaz lógica entre dos niveles o capas adyacentes) para soportar la característica multiacceso del enlace.
- Deberá realizar algunas funciones del nivel 3 (capa de red) del modelo OSI.
- En la transmisión, lleva a cabo el ensamblado de datos dentro de un frame con los campos correspondientes a las direcciones y el método CRC (para detección de errores).
- En la recepción, lleva a cabo el desensamblaje del paquete desarrollando el reconocimiento de las direcciones y la validación con el método CRC.
- Administración del acceso al medio compartido de las redes locales para llevar a cabo la transmisión.

Las dos primeras funciones son desarrolladas por el subnivel LLC, las últimas tres por el subnivel de control de acceso al medio (MAC).

Cabe señalarse que dentro de los estándares definidos por el IEEE también se han definido las características para el nivel físico como son:

- Tipo de medio para las respectivas topologías que soportan las diferentes opciones de subnivel de MAC.
- Codificación/decodificación de señales.
- Transmisión/recepción de bits.
- Preámbulo de generación/remoción (para la sincronización).

Los protocolos de IEEE para redes LAN para los niveles inferiores del modelo OSI, se conforman de la siguiente manera:



LLC: Control de Enlace Lógico
MAC: Control de Acceso al Medio
LSAP: LLC Punto de Acceso al Servicio
MSAP: MAC Punto de Acceso al Servicio
PSAP: Punto de Acceso Físico
PHY: Medio Físico
Tipo1 servicio sin-conexión-sin-reconocimiento
Tipo2 servicio orientado a conexión
Tipo3 servicio sin-conexión-con-reconocimiento

Como se puede observar en la tabla anterior, la división MAC/LLC del nivel de enlace de datos provee varias ventajas esenciales. Primero, controla el acceso al canal compartido entre los dispositivos (subcapa MAC). Segundo, provee un esquema descentralizado que reduce la susceptibilidad de errores en la red. Tercero, brinda una interfaz más compatible con las redes de área amplia (WAN), partiendo de la idea de que el LLC es un subconjunto del protocolo HDLC. Además el LLC es independiente de un método de acceso al medio, mientras que el MAC es un protocolo específico dependiente del diseño. El resultado de ésta división hace más fácil el diseño de las redes, al proveer una interfaz con mayor flexibilidad para redes locales.

Control de Enlace Lógico LLC (IEEE 802.2)

El control de enlace lógico (LLC) está basado en el protocolo Control de Enlace de Datos de Alto Nivel (HDLC: High-level Data Link Control). LLC define los campos que permiten a múltiples protocolos de niveles superiores compartir el uso del enlace de datos. Este se comunica con la capa de red por medio de las interfaces llamadas LSAPs (Link Service Access Points), las cuales son direcciones de enlace de datos lógicos en puntos de acceso. Una sola dirección MAC puede tener múltiples direcciones LSAPs, las cuales habilitan múltiples conexiones punto-final entre dos nodos de una red local.

De acuerdo a este estándar se definen dos categorías generales de operación en el control de enlace de datos. La primera es una operación **sin-conexión** que provee un servicio suficiente con un mínimo de complejidad de protocolo. Esto es muy útil y eficiente cuando los protocolos de las capas superiores (de red, de transporte etc.) proveen el control de error, control de flujo y funciones de secuencia. También es muy útil cuando no se requiere garantizar la entrega de datos. La segunda categoría es la operación **orientada-a-conexión,** ésta provee las funciones similares al protocolo HDLC. Estos dos tipos de operaciones son reflejadas en las especificaciones tanto de los servicios LLC como del protocolo LLC.

Por lo anterior, la subcapa LLC provee tres tipos servicios:

Tipo 1: Servicio **sin-conexión-sin-reconocimiento** (Unacknowledge connectionless service). Este es un servicio de datagrama que simplemente permite el envío y recepción de frames LLC, sin ninguna forma de reconocimiento (acknowledge) para asegurar la entrega, ya que en éste servicio los paquetes (frames) llevan la información completa de la dirección fuente y dirección destino, sin garantizar que los paquetes lleguen intactos o en el orden adecuado. Este tipo de servicio, soporta transmisiones punto-a-punto, multipunto y broadcast. Se puede utilizar en casos donde los protocolos de niveles superiores (usualmente el de transporte) proveen un control de error y control de flujo punto-a-punto, de manera que este servicio mínimo es todo lo que se necesita.

Tipo 2: El servicio **orientado a conexión** provee un estilo de conexión de circuito virtual entre LSAPs (puntos de acceso a servicio de capa de enlace LSAPs). Con esto provee una medida por la cuál un usuario puede hacer una petición o ser notificado del establecimiento o terminación de una conexión lógica. Este servicio también provee control de flujo, funciones de secuencia y control de errores. Soporta direccionamiento punto-a-punto.

Tipo 3: Servicio **sin-conexión-con-reconocimiento** (Acknowledge connectionless service): este es también un servicio sin conexión, pero con reconocimiento (acknowledge). Con él se provee un mecanismo por el cuál cada usuario puede enviar una unidad de datos y recibir un reconocimiento (acknowledgment) que indica que los datos fueron entregados sin la necesidad de establecer una conexión lógica. Además lleva a cabo la corrección de datos erróneos por medio de la retransmisión de paquetes que contienen los datos erróneos, esto libera a los niveles superiores de ésta tarea. Soporta transferencias punto-a-punto. Puede ser muy útil en algunos ambientes de tiempo real (como son las redes locales en empresas e industrias donde las funciones de tiempo son críticas).

CSMA/CD (IEEE 802.3)

La red de bus CSMA/CD es mejor conocida como tecnología Ethernet. El método de control acceso al medio CSMA/CD y el formato del frame Ethernet es idéntico para todas las variedades de velocidad en la que ellos operan y los medios soportados por Ethernet. Sin embargo, las velocidades 10Mbps y 100Mbps individualmente tienen diferentes tipos de medios los cuales pueden usar diferentes componentes de conexión, y por tanto tienen diferentes guías de configuración.

Cada computadora equipada con Ethernet, opera de forma independiente de todas las demás sobre la red (no existe un controlador central). Todas las estaciones unidas en un sistema Ethernet son conectadas a un sistema de señal compartido, también llamado *medio compartido o bus* (backbone). Las señales Ethernet son transmitidas serialmente es decir, un bit a la vez, sobre el canal de señal compartido, el cuál es recibido por cada computadora conectada al bus. Para transmitir datos una computadora primero escucha el canal, y si esta desocupado o vacío transmite sus datos en forma de un frame Ethernet.

Después de cada transmisión, todas las computadoras sobre la red deberán contender de igual forma para obtener la oportunidad de transmitir el siguiente frame. Esto asegura que el acceso al canal de transmisión compartido sea claro, y que ninguna computadora pueda bloquear a las demás. El acceso al canal compartido es determinado por un método de control de acceso (MAC) llevado a cabo en cada interfaz Ethernet localizado en cada máquina. Ethernet ocupa el mecanismo de control de acceso al medio llamado CSMA/CD.

A continuación se presenta una tabla con las posibles opciones de medios para la capa física de Ethernet:

Parámetros	10Base5	10Base2	10BaseT	10Base36	10BaseF
Medio de transmisión	Coaxial	coaxial	UTP	coaxial	Fibra
Diámetro de cable (mm)	10	5	0.4-0.6	0.4-1.0	
Tasa de transmisión de datos (Mbps)	10	10	10	10	10
Longitud máx. del segmento (m)	500	200	100	100	1800
Técnica de señal utilizada	Baseband manchest	Baseband manchest	Baseband manchest	Broadband (DSPK)	Baseband manchest
Extensión máx. de la red (m)	2500	925	500	3600	2000
Nodos por segmento	100	100	No. de puertos del hub	No. de puertos del hub	No. de puertos del hub
Número máx. de nodos	1024	1024	No. de puertos del hub	No. de puertos del hub	No. de puertos del hub
Topología	Bus	bus	estrella	bus	estrella

A continuación detallaremos solo los medios más utilizados actualmente.

- **10BASET**

En este sistema, todos los repetidores multipuertos funcionan como un repetidor ordinario de los sistemas 10BASE5 o 10BASE2. Una ventaja de utilizar repetidores y el uso de la tasa de transmisión de datos a 10Mbps es que el sistema 10BASET puede ser mezclado con los sistemas 10BASE2 y 10BASE5. Para más de un concentrador, las reglas de configuración son; un máximo de cuatro concentradores en la ruta de datos entre dos computadoras cualquiera, y que los segmentos de cable UTP no sean mayores de 100 metros.

La ruta de transmisión máxima permitida entre dos computadoras cualquiera es de cinco segmentos y un conjunto de cuatro repetidores. Un segmento deberá ser uno de los dos siguientes: segmento de enlace punto-a-punto o un segmento coaxial 10BASE2 o 10BASE5. El número máximo de segmentos de cable coaxial en una ruta es de tres segmentos. En la siguiente tabla se resumen las conexiones permisibles para un repetidor multipuertos 10BASET:

Medios de transmisión	No. de dispositivos conectados	Longitud máxima (m)
Dos cables de par trenzado	2	100
Dos cables de fibra óptica	2	500
Cable coaxial (10BASE)	30	185
Cable coaxial (10Base2)	100	500

- **10BaseF**

El sistema 10BASE-F es el estándar de medio de fibra óptica para redes Ethernet, es el más usado actualmente para cubrir largas distancias (hasta 2 km. entre repetidores). Es también usado para inter e intra backbone de edificios (por costumbre no es instalado para la conexión directa a las computadoras por el alto costo del cableado de la fibra óptica). Ethernet utiliza pulsos de luz en lugar de corriente eléctrica para el envío de las señales, lo que provee un mejor aislamiento eléctrico para los equipos con terminación de enlace con fibra óptica. Mientras que el equipo Ethernet usado en segmentos de medio metálico tiene solamente protección de circuitos diseñado para riesgos eléctricos internos, el medio de fibra óptica es totalmente no-conductivo. Este completo aislamiento eléctrico provee inmunidad para un mayor número de riesgos eléctricos incluyendo el efecto llamado "lighting strikes", de los diferentes niveles de corriente de tierra eléctrica que pueden ser encontrados en la conexión de instalaciones separadas. Además de que este completo aislamiento eléctrico es esencial cuando los segmentos Ethernet viajan a la intemperie a través de la parte exterior de las instalaciones para enlazar dos edificios separados.

La mejor ventaja que da un segmento de enlace de fibra óptica 10BaseF es la gran distancia a la que este puede extenderse. Además de que puede soportar velocidades de transmisión mucho más altas que 10Mbps. Así, cuando se diseña una red con el enlace de bus backbone basado con medio de fibra óptica con enlace a concentradores de 10Mbps, o cuando se lleve a cabo una actualización en el futuro se pueden cambiar los concentradores de 10Mbps por otros a 100Mbps sin modificar el esquema de cableado de fibra óptica.

- **Los estándares FOIRL y 10BaseFL**

El uso más común para el tipo de medio de fibra óptica es el enlace entre segmentos. Existen dos tipos de enlace entre segmentos con fibra óptica en uso, el segmento original **Fiber Optic Inter-Repeater Link (FOIRL)** y el nuevo segmento **10BaseFL**.

La especificación original FOIRL del estándar Ethernet de principios de 1980 provee un segmento de hasta 1000 metros entre dos repetidores únicamente. Cuando se hizo costeable realizar enlaces individuales entre las computadoras y los puertos de un concentrador repetidor por medio de fibra óptica, los vendedores crearon salidas de interfaz FOIRL MAUs para permitir que se hiciera la conexión, aunque una conexión repetidor-a-DTE no fue específicamente descrita en el estándar FOIRL.

El conjunto de estándares llamados 10BaseF para medios de fibra óptica, fue desarrollado para cubrir aspectos de la conexión Ethernet con fibra óptica. Este conjunto de estándares incluye especificaciones para un segmento de enlace de fibra óptica que permitiera conectar directamente a las computadoras. El conjunto completo de especificaciones 10BaseF incluye tres tipos de segmentos:

1. 10Base-FL: Reemplaza las anteriores especificaciones FOIRL, y es diseñado para interoperar con el equipo basado en FOIRL existente. 10Base-FL provee un segmento de enlace de fibra de hasta 2000 metros de longitud, previendo que solamente equipo 10Base-FL sea usado en el segmento. Si equipo de 10BASE-FL es combinado con equipo basado en FOIRL, entonces la longitud máxima de segmento puede ser de 1000 metros. Un segmento 10Base-FL puede ser conectado entre dos computadoras, dos repetidores o entre una computadora y un puerto del repetidor. Este tipo es el más ampliamente usado de las especificaciones de fibra óptica 10Base-F, y el equipo esta disponible a través de un gran número de distribuidores.

2. 10Base-FB: Describen un segmento backbone (espina dorsal) de señal síncrona que permite que el límite de repetidores usados en un sistema Ethernet a 10Mbps pueda ser excedido. Los enlaces 10Base-FB son usados para enlazar concentradores repetidores de señal síncrona 10Base-FB especiales juntos en un sistema backbone repetido que puede expandirse largas distancias. Un enlace individual de 10Base-FB puede ser de hasta 2000 metros de longitud. Este sistema tiene una limitación en el mercado ya que el equipo está disponible solo con pocos vendedores.

3. 10Base-FP: El sistema de fibra pasiva provee un conjunto de especificaciones para un segmento combinado de fibra óptica que enlaza múltiples computadoras sin el uso de repetidores. Los segmentos 10Base-FP pueden ser de hasta 500 metros de longitud. El uso de un solo empalme en estrella pasiva de 10Base-FP puede enlazar hasta 33 computadoras. Este sistema no ha sido ampliamente adoptado y el equipo no está disponible.

Nuevas especificaciones del 802.3

Por ultimo se hace notar que la velocidad de transmisión original del estándar 802.3 Ethernet es de 10 Mbits/seg pero las nuevas implantaciones como el 100BaseT, transmiten hasta 100 Mbits/seg en cable de par trenzado para tipos de datos.

Token Bus (IEEE 802.4)

El estándar token bus se caracteriza por tener un control de acceso al medio del tipo determinístico por estar basado en el tipo de control de acceso al medio con token, además de la habilidad de poder poner prioridades a la transmisión de paquetes. Bajo condiciones normales, la operación de este tipo de red es muy parecido a las redes

token ring. Sin embargo existen diferencias en los métodos de control de acceso al medio (broadcast para el bus y secuencial para el anillo), los procedimientos que utiliza para el manejo y administración del anillo lógico, tales como inicialización y pérdida del token, son manejados de manera diferente en ambos tipos de redes.

Las redes tipo token bus normalmente utilizan cable coaxial como medio de transmisión, operando en modo Broadband o un modo de Baseband modificado llamado **Carrierband.**

El modo carrierband es el mismo baseband en el aspecto de que cada transmisión ocupa el ancho de banda completo del cable, la diferencia radica en que en el modo carrierband todos los datos son primeramente modulados antes de que se transmitan. Además el formato del frame utilizado por este estándar es muy parecido al utilizado por los frames de tipo Token Ring.

La topología utilizada para este estándar es de bus físico o tipo árbol, mientras las computadoras son organizadas en forma de un anillo lógico. El estándar token bus especifica tres tipos de opciones para la capa física. El primero es un sistema broadband, el cual soporta canales de datos a 1, 5 y 10 Mbps con anchos de banda de 1.5, 6 y 12 MHz respectivamente. El estándar recomienda el uso de un sistema dividido el cuál conste de un solo cable con un traductor de frecuencia principal (la configuración de cable dual o doble también es permitida).

El segundo esquema es conocido como **carrierband** o **broadband de un solo canal (single-channel broadband)**. La señal carrierband significa que el espectro entero del cable es dedicado a una sola ruta de transmisión para señales analógicas. El esquema carrierband especifica las tasas de transmisión en 1, 5 y 10 Mbps.

La más reciente adición al nivel físico del estándar 802.4 es una especificación de fibra óptica, en la que se especifican tres tasas de transmisión: 5, 10 y 20 Mbps.

La especificación de fibra óptica del estándar 802.4 puede ser utilizada con cualquier topología que sea lógicamente un bus. Esto es, una transmisión desde una computadora cualquiera será recibida por todas las demás computadoras, y si dos computadoras transmiten al mismo tiempo, ocurrirá una colisión. El estándar recomienda el uso de estrellas (activas o pasivas).

Cabe mencionar que esta norma no se implementa frecuentemente en el entorno de redes LAN. Siendo su mayor aplicación en las industrias de manufactura (fábricas automatizadas) y otras relacionadas con las industrias de control de procesos.

Token Ring (IEEE 802.5)

También llamada 802.1 de ANSI 1985, define los protocolos de acceso, cableado e interfaces para las LANs en anillo con testigo. IBM popularizó esta norma, que utiliza un método de acceso con testigo o token y se cablea físicamente en una topología de tipo estrella pero formando un anillo lógico. Los nodos se cablean a una unidad de acceso múltiple central (concentrador MAU) que repite las señales de una computadora

a la siguiente. Las unidades de acceso múltiple (MAUs) se cablean conjuntamente para extender la red, lo cuál implica el anillo lógico.

Este tipo de red es una concatenación de enlaces punto a punto (no broadcast, aunque pueden realizar un broadcast de red local de manera secuencial con los enlaces punto a punto formando un circulo). La tecnología de redes en anillo es digital a diferencia de las redes Ethernet donde el método de acceso al medio CSMA/CD puede ser analógico. Otra característica de estas redes es su tiempo de respuesta ya que es determinístico aún bajo condiciones donde existe mayor carga.

Como se mencionó, las redes locales Token Ring son concatenaciones de enlaces punto a punto donde cada computadora actúa como un repetidor, proveyendo a la señal la amplificación necesaria y la corrección necesaria de la misma. Los enlaces pueden ser realizados con cualquier tipo de medio, cable coaxial, par trenzado blindado y fibra óptica. El tamaño mínimo de un anillo deberá ser de un kilómetro. Este tamaño es muy extenso sobre todo cuando se desean conectar pocas estaciones de trabajo o computadoras dentro de un solo cuarto, por esta razón, se instala una estación especial designada como "monitor activo", el cuál adiciona un retraso de almacenamiento de 24 bits para el anillo. Este almacenamiento también compensa cualquier **fase jitter** acumulada sobre el anillo. El monitor activo es indispensable para el buen funcionamiento del anillo y no es una estación con dispositivos de red especial, de hecho cualquier estación sobre el anillo puede ser monitor activo ya que las otras estaciones del anillo son designadas estaciones pasivas. La selección de qué estación debe ser activa, se lleva a cabo mediante el procedimiento de inicialización.

El estándar 802.5 especifica tres opciones de tasa de transmisión: 1 Mbps, 4 Mbps y 16 Mbps. La configuración a 1 Mbps utiliza cable par trenzado UTP. Inicialmente, las configuraciones de 4 y 16 Mbps utilizaban cable STP. La demanda en el mercado hizo que estas configuraciones soportaran también cable UTP. Varios dispositivos soportan el uso de cable UTP para anillos de 4 y 16 Mbps (IBM en un principio no soportaba los 16Mbps sobre UTP más tarde junto con Synoptics Communications propuso el estándar a IEEE 802.5). Las estaciones a 16Mbps no esperan el regreso del frame de datos para poner la señal de token otra vez sobre la red. Con este mecanismo, llamado el **"early token release mechanism"**, dos frames pueden ser transmitidos simultáneamente sobre la red token ring.

Aunque el número máximo de estaciones o computadoras permitidas; con cable tipo 1 y tipo 2 son 260, el número recomendado es de 100. El límite máximo de estaciones sobre el anillo es debido a la acumulación del **clock jitter**. La distancia máxima entre estación y el MAU es de 300 metros. Cabe aclararse que el MAU es la unidad de acceso multiestación y no el dispositivo MAU para Ethernet. En este caso se trata de un centro de cableado donde pueden ser conectadas varias estaciones. Contienen dos puertos finales llamados ring in y ring out, estos sirven para interconectar múltiples MAUs juntos.

Tamaño del anillo

Una red token ring que utiliza cable STP, tal como los cables de IBM tipo 1 y tipo 2, tiene un número máximo de computadoras que pueden ser conectadas en un solo anillo limitado a 260 (aumentar el número de estaciones por encima de éste número

causa problemas en el clock jitter haciendo fallar al anillo) para tener el mínimo anillo utilizable, el número mínimo de estaciones es dos. En éste estándar solo se especifica el tipo de medio par trenzado blindado (STP) con tasas de transmisión de 4 y 16 Mbps utilizando el método Manchester diferencial de codificación de señal.

Por último, se puede mencionar que el estándar X3T9 referente a la Interfaz de Datos Distribuido por Fibra (FDDI) y CDDI se basa en el protocolo de anillo con testigo 802.5 token ring. Pero éste estándar X3T9 fue desarrollado por el Comité de Normas Acreditadas (ASC: Accredited Standards Commitee). Además el estándar X3T9 es compatible con el estándar 802.2 control de enlace lógico (LLC) y así con otras normas 802.x referentes a la conexión de red.

Red de Área Metropolitana (IEEE 802.6)

La norma 802.6 del IEEE para redes de área metropolitana define un protocolo de alta velocidad en el cuál las estaciones enlazadas comparten un bus doble de fibra óptica que utiliza un método de acceso llamado **bus dual de cola distribuida** (DQDB: Distributed Queue Dual Bus). Este bus ofrece tolerancia a fallos para mantener activas las conexiones en caso de que falle o llegue a romperse el bus. La norma MAN se designa para proporcionar servicios de datos, voz y video en una área metropolitana de aproximadamente 50 kilómetros, con una velocidad de transmisión de datos de 1.5, 45 y 155 Mbps. El DQDB es el protocolo subyacente de acceso para el Servicio de Conmutación de Datos Multimegabit (SMDS: Switched Multimegabit Data Service), que ofrecen la mayoría de las compañías de telecomunicaciones públicas como una forma de construcción de redes privadas en áreas metropolitanas. DQDB es una red de transmisión de celdas conmutadas con una longitud fija de 53 bytes, por lo tanto, es compatible con la ISDN (ISDN: Integrated Services Digital Network) de banda ancha (ISDN-B) y el modo de transferencia asíncrono (ATM: Asynchronous Transfer Mode). La conmutación de celdas tiene lugar en el nivel de control de enlace lógico 802.2.

Los servicios MAN son tanto orientados como no orientados a la conexión, y/o isócronos (video en tiempo real). El bus tiene una serie de ranuras de longitud fija donde la computadora sitúa los datos para su transmisión sobre el bus. No obstante, para acomodar datos isócronos sensibles al tiempo, se reservan unas ranuras a intervalos regulares para garantizar que los datos lleguen a tiempo y en orden (secuencial).

Grupo asesor para técnicas de banda ancha (IEEE 802.7)

Este comité proporciona consejos técnicos a otros subcomités en técnicas de conexión de redes de banda ancha.

Grupo asesor para técnicas de fibra óptica (IEEE 802.8)

Ofrece consejo a otros subcomités de redes que utilizan fibra óptica como una alternativa a las redes actuales basadas en cables de cobre.

Redes integradas por voz/video (IEEE 802.9)

Este grupo trabaja en la integración de tráfico de voz, datos y vídeo en LAN 802.x y en redes digitales de servicios integrados (ISDN). Los nodos definidos en las especificaciones incluyen teléfonos, computadoras, además de codec's de video. Las especificaciones se han llamado Integración de datos y voz, o IVD (Integrated Voice and Data). El servicio proporciona un flujo multiplexado que puede llevar información de datos y voz por los canales que conectan las dos estaciones sobre cables de par trenzado de cobre. Se definen varios tipos distintos de canales entre los que se incluyen los canales dúplex no conmutados a 64 Kbits/seg., de conmutación de circuitos o de conmutación de paquetes.

Seguridad de red (IEEE 802.10)

Este grupo trabaja en la definición de un modelo normalizado de seguridad que interopera sobre distintas redes e incorpora métodos de autentificación y cifrado.

Redes inalámbricas (IEEE 802.11)

Este comité define las normas para redes inalámbricas. Trabaja en la normalización de diversos medios como: la radio de espectro expandido, radio de banda estrecha, rayos infrarrojos y transmisiones sobre líneas de potencia. También trabaja en la normalización de interfaces inalámbricas para redes informáticas, donde los usuarios se conectan a sistemas que usan computadoras basadas en lápices, asistentes digitales personales (PDS: Personal Digital Assistant) y otros dispositivos portátiles.

Se han planeado dos enfoques para las redes inalámbricas: el planteamiento distribuido y el planteamiento de punto de coordinación. En el planteamiento distribuido, cada computadora de trabajo controla su acceso a la red. En cambio, en el planteamiento de punto de coordinación, un concentrador central perteneciente a una red cableada controla las transmisiones de las computadoras de trabajo inalámbricas. El comité 802.11 favorece las redes con planteamiento distribuido.

IEEE 802.12: LAN de Acceso de prioridad por demanda (100VG-AnyLAN)

Este comité define una de las normas de Ethernet a 100 Mbits/seg con el Método de Acceso de Prioridad por Demanda propuesto por Hewlett-Packard y otros fabricantes. Este método de acceso al medio utiliza un concentrador central para controlar el acceso al canal compartido de comunicación. El cable especificado es de par trenzado de cuatro hilos de cobre. Las prioridades están disponibles para soportar la distribución de la información multimedia en tiempo real.

1.3.4.2 Estándar de cableado estructurado EIA/TIA 568

Un sistema de cableado estructurado consiste en una infraestructura de cableado flexible que puede soportar múltiples computadoras y sistemas de telefonía de un modo independiente de su fabricante. En el cableado estructurado cada computadora es alambrada hacia un punto central utilizando una topología en estrella facilitando el sistema de interconexión y administración. Este aprovechamiento permite la comunicación virtualmente con cualquier dispositivo, donde sea y en cualquier momento. Un plan de alambrado bien diseñado puede incluir varias soluciones de cableado independientes con diferentes tipos de medios instalados para cada estación de trabajo o computadora para soportar y satisfacer sus requerimientos.

La especificación actual ANSI/EIA/TIA-568 es el estándar de cableado estructurado de telecomunicaciones comerciales. Las siglas significan lo siguiente: ANSI, American National Standars Institute; EIA, Electronic Industry Association y TIA, Telecommunications Industry Association.

El propósito del estándar EIA/TIA 568 es:

- Establecer un estándar de cableado de telecomunicaciones para que soporte un ambiente no propietario (multiproveedor o sistema abierto).

- Facilitar la planeación e instalación de un sistema de cableado estructurado en organizaciones comerciales.

- Establecer el desempeño y los criterios técnicos para diferentes sistemas de cableado.

El estándar EIA/TIA 568 especifica los siguientes puntos:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente corporativo.
- Recomendaciones de topologías y distancias.
- Parámetros de los medios, los cuales determinan el desempeño.
- Asignaciones de pines para conectores para asegurar la interconectividad.
- El tiempo de vida de un sistema de cableado para telecomunicaciones (10 años).

El EIA/TIA 568, describe seis subsistemas de un sistema de cableado estructurado:

1. Entrada a la estructura (building entrance facilities).
2. Habitación de equipo (equipment room).
3. Cableado de backbone (backbone cabling).
4. Armario de telecomunicaciones (telecommunications closet).
5. Cableado horizontal (Horizontal Cabling).
6. Área de trabajo (work area).

1. Entrada a la estructura:

Es la parte donde los servicios externos de telecomunicaciones entran al edificio interconectándose con los sistemas de telecomunicaciones internos del edificio o estructura. En un ambiente de campus o multi-edificios, puede contener las interconexiones del backbone entre edificios. Los requerimientos se definen en el estándar EIA/TIA-569.

2. La habitación del equipo:

Es el área en un edificio donde está localizado el equipo de telecomunicaciones. Partes de o todo el sistema de cableado de telecomunicaciones termina en esta área. Esta área es generalmente de mayor complejidad que los armarios de telecomunicaciones. Algunas o todas las funciones de un armario de telecomunicaciones pueden ser provistas por la habitación del equipo.

3. Cableado del backbone (backbone cabling):

Este aspecto provee la interconexión entre los closets de telecomunicaciones, las habitaciones del equipo y la entrada al edificio. Este cableado consiste en el backbone como tal, en las conexiones cruzadas (cross-connect) principales e intermedias, en las terminaciones mecánicas y en los patch cords o jumpers utilizados para conexiones backbone-backbone, dentro de este punto se incluyen:

- La conexión vertical entre pisos (risers).
- Los cables entre habitaciones de equipo y entradas a la estructura.
- Los cables entre edificios (interconexión de edificios o interbuilding).

En este estándar se definen algunas distancias máximas permisibles dependiendo del tipo de cable utilizado, dichas distancias se muestran en la siguiente tabla:

Tipo de Cable	Distancia
100 ohms UTP(24 o 22 AWG)	800 metros (voz)
150 ohms STP	90 metros (datos)
Fibra óptica multimodo 62.5/125 mm	2000 metros
Fibra óptica monomodo 8.3/125 mm	3000 metros

Las distancias del cableado son dependientes de la aplicación. Las máximas distancias especificadas en la tabla están basadas en aplicaciones de transmisión de voz para UTP, transmisión de datos para STP y fibra. La distancia de 90 metros para aplicaciones STP con un espectro de ancho de banda entre 20MHz y 300MHz. Una distancia de 90 metros también se aplica al cable UTP con un espectro de ancho de banda de 5MHz-16MHz usando categoría 3, 10MHz para categoría 4 y de 20MHz-100MHz para categoría 5.

Las distancias actuales dependen del tipo de sistema, velocidad de datos y especificaciones del proveedor para los sistemas electrónicos y los componentes asociados. En la actualidad el estado de las facilidades de distribución usualmente incluyen una combinación de cables de cobre y fibra óptica para el backbone.

Otros requerimientos del diseño son:

- El backbone debe ser una topología en estrella.
- No más de dos niveles de jerarquía de cross-connects.
- No son permitidos los derivadores de puente (Bridges taps).
- El cableado de interconexión en paneles de parcheo principales e intermedios no deberán exceder la longitud de 20 metros.
- Evitar la instalación en áreas donde puedan existir equipos que generen altos niveles de interferencia (EMI/RFI).
- El nivel de tierra eléctrica deberá soportar los requerimientos definidos en el estándar EIA/TIA 607.

4. Armario de telecomunicaciones:

Es un área dentro del edificio, en la que se localiza el equipo del sistema de cableado de telecomunicaciones. Las funciones que toman lugar en el armario incluyen los terminadores mecánicos y/o cross-connects para interconexión de los puntos de cableado horizontales y backbone.

5. Cableado horizontal

Es la porción del sistema de cableado que se extiende desde la caja de contactos del área de trabajo (outlets) hasta el armario de telecomunicaciones. Su topología es en estrella, y además consta de los contactos de telecomunicación en el área de trabajo (outlets), cable terminador y conexión cruzada (cross-connection).

Se reconocen tres tipos de medios como opciones para el cableado horizontal, cada una tiene una extensión de distancia máxima de 90 metros. Aunque se permiten 10 metros más para el área de trabajo, el panel de parcheo del closet de telecomunicaciones y los cables jumper. Cada área de trabajo permitirá tener un mínimo de dos contactos de telecomunicación (enchufes u outlets), uno para voz y otro para datos.

El subsistema horizontal permite el uso de:

- 4 pares de 100 ohms de cable UTP para voz (24AWG).
- 4 pares de 100 ohms UTP/STP.
- 2 pares de 150 ohms STP.
- Cable coaxial de 50 ohms (10Base2). No recomendado para nuevas instalaciones.
- Cable de fibra óptica 62.5/125 micras para datos.

6. Área de Trabajo

Interconecta al cableado horizontal que llega a los contactos de telecomunicaciones en la pared con los dispositivos de los usuarios. El cableado del área de trabajo esta diseñado para ser relativamente simple en su conexión. La máxima distancia permisible para los cables de parcheo es de 3 metros, y están hechos del mismo tipo de cable que se utiliza para el cableado horizontal.

Los componentes son:

- Equipo terminal (estaciones de trabajo, computadoras, teléfonos, impresoras, etc.).
- Cables de parcheo, cordones modulares, cables adaptadores para PC's, jumpers para fibra, etc.
- Adaptadores. Deberán ser externos al conector de telecomunicaciones

Por último, ISO actualmente esta desarrollando un estándar internacional de sistema de cableado con el título **Generic Cabling for Customers premises Cabling ISO/ IEC 11801**.

1.3.4.3 Estándares de redes inalámbricas

Las redes inalámbricas son una nueva herramienta para los diseñadores de redes. Los segmentos de redes locales inalámbricas pueden aplicarse totalmente en ambientes donde el sistema de cableado es difícil de implementar (depósitos aislados, áreas de recepción o departamentos donde los grupos de trabajo se mueven frecuentemente). Esta tecnología aún está en sus primeros desarrollos y contiene un número de limitaciones en las que se incluyen el ancho de banda, aunque se esta desarrollando de manera rápida y se piensa que llegará a ser más popular cuando los precios de los dispositivos utilizados para su implantación bajen.

Actualmente las redes locales inalámbricas usan una de tres tecnologías siguientes: rayos infrarrojos, espectro disperso (spread spectrum), o radio de banda angosta (narrowband radio).

Redes locales inalámbricas por medio de rayos infrarrojos

Estas redes pueden igualar las velocidades de redes locales que utiliza un sistema de cableado (incluyendo la velocidad de 16Mbps que ofrece token ring). Su precio y nivel de desarrollo son mucho más favorables que el de las redes locales basadas en la tecnología de espectro disperso. Un tercer beneficio es que las señales de rayos infrarrojos ofrecen una mayor seguridad que las señales de espectro disperso.

Una limitante de esta tecnología es que requiere una línea de vista limpia para la señal entre los transmisores y los receptores. Cuando las redes locales inalámbricas basadas en rayos infrarrojos son utilizadas para llevar a cabo conexiones extramuros (como cruzar un jardín por ejemplo), sus señales son susceptibles a interrupciones durante condiciones ambientales adversas. Otra limitante, es que se puede transmitir solo a distancias limitadas de aproximadamente 100 pies.

A principios de 1994 la Asociación de datos por Infrarrojo (Infrared Data Association) introdujo un estándar de codificación y decodificación por medio de rayos infrarrojos. Este conjunto de especificaciones aseguraba que en 1995 existiría interoperabilidad entre productos basados en infrarrojos desarrollados para computadoras móviles (actualmente Apple ha anunciado que tendrá soporte para este estándar).

- **Línea de vista (Line-of-sight):** La gran variedad de tecnología de infrarrojos con línea de vista está limitada a lugares como oficinas, donde no existan obstrucciones físicas para la señal entre las estaciones de usuarios. Aunque su naturaleza punto a punto restringe la distancia alrededor de 100 pies, la velocidad de transmisión puede igualarse a las redes basadas en el sistema de cableado que se encuentre en dicha instalación.

- **Infrarrojos por diseminación (Scatter infrared):** La tecnología de redes locales de infrarrojos por diseminación rebota las señales en las paredes y techos para iluminar un área de aproximadamente 100 pies cuadrados. Esta característica produce una señal con una velocidad relativamente baja.

- **Rayos infrarrojos reflejados (Reflective infrared):** En sistemas reflejados, los dispositivos de acoplamiento (transceivers) óptico son montados cerca de las estaciones o PC's y son dirigidos hacia un spot común sobre el techo de la oficina. Esta propuesta trabaja bien en un ambiente con techos altos.

De esta manera podemos decir que la ventaja principal de una red local inalámbrica es que iguala las velocidades de redes basadas en un sistema de cableado, sin ocupar cableado. Aunque existen las limitantes antes mencionadas.

Redes locales inalámbricas por medio de propagación de ondas de radio de espectro disperso.

Desarrollada por los militares para brindar una transmisión eficaz y segura, la tecnología de espectro disperso utiliza la técnica de **secuencia directa de acceso múltiple por división de código** para "propagar" datos sobre varias frecuencias. Esta técnica (secuencia directa CDMA) representa cada bit con un bit patrón llamado "chip". Unos y ceros son representados por chips que son inversos uno del otro. Cada bit, cuando es transmitido, es propagado sobre un espectro de frecuencia amplia. El receptor colapsa cada chip transmitido dentro de un solo bit. Todas las señales que no son iguales son eliminadas, dando como resultado una señal libre de interferencias.

En EEUU, un canal de 83MHz de amplitud esta disponible, desde 2.4 a 2.483 GHz para operaciones sin licencia. Esta banda de frecuencia es dividida dentro de canales (referidos también como hops) de 82.1 MHz. Los adaptadores se sintonizan en un canal específico durante un corto periodo de tiempo y entonces se mueven a un diferente canal. Los canales son visitados en un orden predefinido, especificado por la secuencia de canalización, la cual es diseñada para que canales sucesivos se encuentren separados por varios MHz. Todas las estaciones participantes de la misma red usan la misma secuencia de canalización y sincronizan sus temporizadores de canal. Cuando la interferencia esta presente, afecta solo a pocos canales.

El FCC (Frecuency Comunication Comite) autorizó que tres bandas de frecuencia separadas se establecieran para redes locales basadas en radio comercial: 902 a 928 MHz, 2.4 a 2.5 GHz, y 5.8 a 5.9 GHz. Muchos de los primeros productos para redes inalámbricas fueron diseñados para trabajar en el rango de banda industrial, científico y médico (ISM) sin licencia de 902 a 928 MHz. En 1993, la tendencia cambió. Cabe hacer notar que mientras más alta sea la frecuencia seleccionada, más altos son los costos de los dispositivos. Además de que no importa que banda de frecuencias se utilice el resultado es el mismo.

Esta tecnología de propagación puede transmitir sus señales de baja frecuencia a través de materiales de construcción comunes y de esta manera cubrir una mayor área que otras alternativas inalámbricas. Mientras que la inmunidad virtual a señales de interferencia y la seguridad significativa que provee, complementan al espectro disperso, su mayor limitante ha sido su considerable consumo de ancho de banda que da como resultado una relativa baja velocidad de transmisión comparada con otras tecnologías de redes inalámbricas.

Las posibles ventajas de instalar una red que use el espectro de radio como medio de propagación son:

- No se requiere una licencia para la utilización de las bandas de frecuencia.
- No se requiere de una línea de vista para la señal.
- Proporciona alta inmunidad a la interferencia.

En contraparte, las posibles desventajas son:

- La distancia de alcance de la señal es limitada ya que 1 watt de potencia tiene un límite de cobertura de alrededor de 800 pies.

- Pueden presentarse conflictos de frecuencia con múltiples redes locales al estar trabajando todas ellas en ambiente de alta demanda (high-rise). Esto se presenta cuando los equipos de espectro disperso son instalados uno al lado del otro o por cercanía a otras formas de emisión electromagnética y maquinaria pesada que afecten el rendimiento.

Redes inalámbricas de radio de banda angosta

El uso dedicado de redes locales de radio de banda angosta, tiene una licencia de uso de ancho de banda de 18 a 19 GHz, el cual es asignado por el FCC. Debido a que el ancho de banda utilizado por la tecnología de radio de banda angosta es mayor que el rango de espectro disperso, la tasa de transmisión es generalmente mayor. Esta tecnología no puede atravesar muros de metal o muros de concreto dentro de una estructura, pero su alta frecuencia permite cubrir un volumen de 5000 pies cúbicos.

Especificaciones del comité 802.11 para redes inalámbricas

El comité 802.11 ha sido el desarrollador de las especificaciones para redes inalámbricas que soportarán punto-a-punto y la infraestructura de redes inalámbricas locales interconectadas vía un punto de acceso a una red existente con sistema de cableado. Los protocolos desarrollados permiten al usuario móvil moverse con toda libertad por toda una área manteniendo la misma conexión, asi como el poder de conversación. Además están disponibles dentro de pequeños dispositivos de computadoras móviles para comunicarse por largos periodos de tiempo con una sola carga de batería.

El comité está definiendo los protocolos para redes inalámbricas del rango de 900 MHz, 2.4 GHz, y bandas de frecuencia infrarroja. Además de diferentes especificaciones físicas (PHY) para protocolos que dependen del medio. Existen diferentes especificaciones PHY para cada banda de frecuencia soportada por el estándar 802.11. Un solo protocolo MAC independiente del medio provee una interfaz de red unificada entre diferentes PHY inalámbricas y redes con sistema de cableado.

Los requerimientos de usuario para redes locales inalámbricas establecidos en marzo de 1992, incluyen el soporte para anchos de banda de 1 Mbps o más en las siguientes áreas de aplicación:

- Transferencia de archivos y control remoto.
- Carga de programas (program loading).
- Paginación de programas (program paging).
- Procesos de transacciones.
- Multimedia.
- Control y monitoreo de manufactura.
- Manejo de material.

Concentradores o puntos de acceso

En el caso de redes inalámbricas, los concentradores o puntos de acceso llevan a cabo dos tareas adicionales a la de conectar múltiples estaciones a los servidores o a otras máquinas. Estas tareas son: proveer una conexión a un backbone para las unidades inalámbricas, y por medio de un número de ellos localizados estratégicamente, puede extender el rango para cada computadora con acceso a la red.

A diferencia de redes alambradas como 10BaseT, algunas redes inalámbricas pueden establecerse sin utilizar concentradores del todo. En la figura 1.18 se presenta un esquema de una pequeña red con topología bus, utilizando concentradores inalámbricos.

Antecedentes

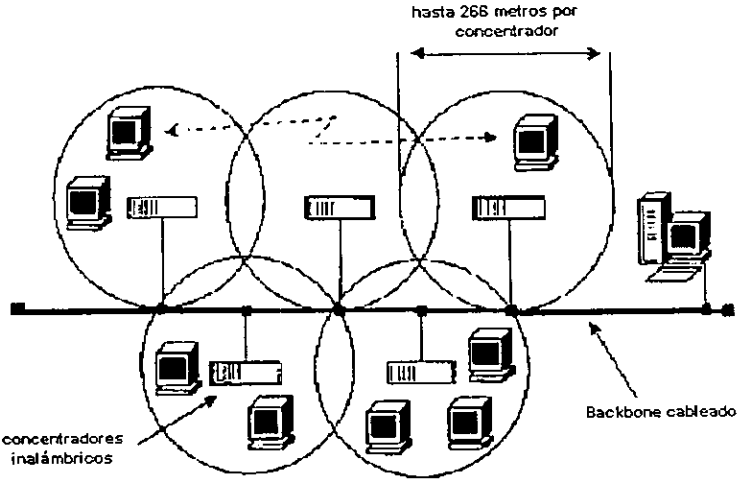


Figura 1.18

Puentes entre edificios para la interconexión de redes locales inalámbricas

Existen varios puentes de espectro disperso los cuales pueden conectar edificios con una distancia de separación de hasta 3 millas a una velocidad de hasta 2 Mbps. Un ejemplo de esta tecnología es la desarrollada por AirLAN/puentes, en la cuál se transmite sobre la banda 902 a 928 MHz, este dispositivo soporta tanto redes Ethernet como Token Ring, además de ser compatible con muchos sistemas operativos en red. A una tasa de transmisión de 2 Mbps este dispositivo puede transmitir correo electrónico entre los edificios, pero tiene limitantes al transmitir archivos de datos de gran longitud.

Para enviar y recibir señales de datos, los puentes inalámbricos requieren de antenas espaciales. Variando el tipo, de acuerdo a los requerimientos de distancia y las demandas físicas del sitio.

El costo alto del equipo aunado con la rápida declinación de los precios de los dispositivos Ethernet basados en cableado, es una razón por la cual las redes inalámbricas no son tan populares. Una segunda razón es que el estándar ha sido desarrollado de manera lenta. El IEEE 802.11 ha tomado mucho tiempo en llevar a cabo la finalización de especificaciones, y las corporaciones han llegado a estar poco dispuestas a investigar productos que puedan resultar ser propietarios.

Redes híbridas: inalámbricas y cableadas.

Hace pocos años la compañía AT&T introdujo una red inalámbrica basada en espectro disperso, WaveLAN, como un reemplazo inalámbrico para redes locales con sistema de cableado, el cual falló. La diferencia de precios entre los dos sistemas (inalámbrico y

cableado) fue y es aún muy grande para justificar grandes redes locales inalámbricas, excepto donde las condiciones hacen imposible llevar a cabo un sistema de cableado convencional. Actualmente, el mercado de productos AT&T cuenta con una solución híbrida para ambientes difíciles que necesitan ser conectados a una red local con sistema de cableado.

Cuando las compañías se muevan con tendencias a integrar todas las partes que las componen, la tecnología de redes inalámbricas tendrá una tarea más importante y significativa. Mientras tanto, durante los próximos años la tarea se mantendrá dentro de las redes híbridas, proveyendo segmentos de red inalámbricos donde el sistema de cableado convencional no es fácil de implantar.

La tecnología inalámbrica está ligada a jugar un papel mucho más significativo, sobre redes de área amplia antes de que tome ventaja en redes locales.

La tecnología infrarrojos ofrece velocidades de transmisión compatibles con los sistemas de redes cableadas; desafortunadamente, las distancias de transmisión son limitadas y los usuarios de la red frecuentemente deben contar con una línea de vista de señal para que el funcionamiento de este tipo de red sea apropiado. La tecnología de espectro disperso ofrece menos velocidad de transmisión (alrededor de 2 Mbps), pero brinda grandes distancias, y más soporte por parte de los vendedores.

2.- TECNOLOGÍAS DE REDES DE ALTA VELOCIDAD EN REDES DE ÁREA LOCAL (LANs)

2.1 TECNOLOGÍAS DE CONMUTACIÓN DE REDES LAN

Fundamentalmente las redes Ethernet y Token Ring están basadas en el concepto de ancho de banda compartido entre los usuarios conectados a la red.

Este esquema de ancho de banda compartido fue muy efectivo cuando las redes locales consistían de un pequeño número de dispositivos (generalmente 50) que solo necesitaban transferir sus archivos e imprimir sus documentos. Actualmente las redes han crecido en complejidad y tamaño (a cientos de dispositivos). La conmutación de redes locales es una tecnología de interconexión que le da un nuevo respiro a las redes locales con ancho de banda compartido. Esto se lleva a cabo al poder dividir toda la red compartida, en pequeños segmentos de red con un ancho de banda compartido dedicado a cada segmento.

2.1.1 Relación entre los puentes y los conmutadores

El término puenteo se refiere a una tecnología en la cuál un dispositivo (referido como puente) conecta dos o más segmentos de red LAN. La función característica de un puente es transmitir datagramas de un segmento a su destino en otro segmento. Cuando un puente es conectado por primera vez en una red, este empieza a operar examinando la dirección MAC (dirección de Control de Acceso al Medio) del datagrama que fluye a través de él, y de ésta manera construye una tabla de destinos conocidos.

Si el puente conoce que la dirección destino de ese datagrama se encuentra en el mismo segmento del que provino, lo desecha por que no tiene la necesidad de retransmitirlo. Si el puente conoce que la dirección destino se encuentra en otro segmento, retransmite el datagrama sobre ese segmento solamente. Si el puente no conoce el segmento destino del datagrama, retransmite el datagrama sobre todos los segmentos excepto el segmento origen, esto se lleva acabo, por medio de una técnica llamada inundación (flooding), es decir, por broadcast. Por lo tanto, se puede decir que el principal beneficio del puenteo, es que limita el tráfico a ciertos segmentos de la red.

De manera similar a los puentes, los conmutadores conectan varios segmentos de redes LAN, utilizando una tabla de direcciones MAC para determinar el segmento destino de un datagrama y así reducir el tráfico en los demás segmentos. Pero a velocidades mucho mayores, debido a que mueven los datos principalmente por medio de hardware (circuitos ASICs: Application Specific Integrated Circuit) en lugar de software (procesadores RISC). De esta manera, son mucho más rápidos y proveen un mayor rendimiento a un menor costo. La mayoría de los conmutadores, soportan tanto tecnologías de velocidades bajas como Ethernet o Token Ring, así como tecnologías de alto rendimiento como 100BaseT, FDDI y ATM. Esta habilidad de los conmutadores de

soportar varias tecnologías inmediatamente incrementa el rendimiento de la red sin la necesidad de una actualización masiva de infraestructura de la red, además de que algunos conmutadores pueden soportar nuevas funcionalidades, tales como las redes virtuales (VLANs), que brindan una configuración flexible al administrador de red, por permitirle distribuir los grupos de trabajo de una manera lógica y no estar sujeto a la localización física.

Por tal motivo, se dice que la conmutación es una tecnología que ayuda a aliviar los problemas de congestión en redes al reducir el tráfico e incrementar el ancho de banda. Estos conmutadores, están diseñados para trabajar con infraestructura de cable existente. Frecuentemente reemplazan a los concentradores compartidos.

2.1.2 Redes Token Ring conmutadas

Como ya se ha mencionado, la transmisión en las redes Token Ring está basada en una señal referida como señal token, la cuál es pasada alrededor de las computadoras conectadas al anillo, por el método ya descrito en el capítulo pasado. Aunque las redes pequeñas (anillos con un menor número de usuarios) tienen menores retrasos en el paso de la señal token, grandes redes, aún garantizan que cada computadora eventualmente, tendrá acceso a la señal token en una modalidad round robin. La segmentación de un gran anillo por medio de un conmutador reduce el número de usuarios por anillo, con lo que la congestión y el retraso entre oportunidades de las computadoras de tener la señal token también disminuye. Además, los conmutadores de redes Token Ring brindan una mejor tolerancia a fallas en la red.

2.1.3 Redes Ethernet conmutadas

Las redes Ethernet tienen un máximo de ancho de banda de 10 Mbps y es una tecnología half dúplex. Cada dispositivo Ethernet verifica la red para ver si no existe transmisión de datos sobre el medio y pueda empezar a transmitir sus datos, o en caso contrario, esperar un tiempo para volver a verificar y poder transmitirlos (mientras un dispositivo envía sus datos, todos los demás están obligados a esperar para transmitir). En el caso de que dos computadoras comiencen su transmisión al mismo tiempo, se origina una colisión y entonces, los dispositivos entran en un estado pasivo durante un tiempo aleatorio para realizar un nuevo intento posteriormente.

Como cada vez más anfitriones son conectados a estas redes compartidas, deberán esperar con más frecuencia para poder empezar a transmitir, igualmente, ocurrirán más colisiones (ya que más anfitriones trataran de transmitir al mismo tiempo).

Es por esto que un conmutador de red LAN Ethernet brinda un mayor ancho de banda, al separar la red en varios dominios de colisión con un menor número de estaciones y reenviar el tráfico de una manera selectiva hacia el segmento apropiado ya que cada segmento de red Ethernet es conectado a un puerto del conmutador LAN. Al hacer esta división se puede reducir el número de colisiones en cada segmento y por tanto, el desempeño aumenta. De esta manera, en lugar de compartir el limitado ancho de banda de Ethernet entre muchas computadoras, cada estación o cada pequeño grupo de estaciones, puede tener un segmento de 10 Mbps dedicados.

Otra ventaja es que su desempeño no requiere de grandes cambios al sistema de cableado, adaptadores de red ni reconfiguración de software en las estaciones.

Tipos de redes Ethernet conmutadas

Es importante balancear el número de usuarios por segmento, ya que se tienen diferentes necesidades por usuario o por grupo de usuarios. Existen dos opciones de incrementar el desempeño del grupo de trabajo en Ethernet, dependiendo del tipo de segmento Ethernet conmutado, éstos pueden ser:

- **Ethernet conmutado compartido (múltiples estaciones)**

En un grupo de trabajo todos los usuarios y servidores locales en el grupo, compiten por 10 Mbps de ancho de banda. Al adicionar un conmutador Ethernet y conectar el repetidor(es) de 10 Mbps a los puertos del conmutador, cada segmento (cada puerto del conmutador) tiene 10 Mbps. La figura 2.1 presenta un esquema ilustrativo.

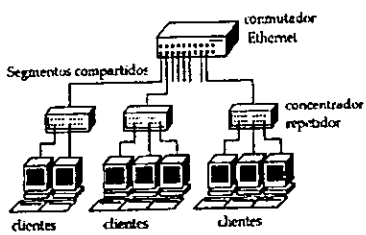


Figura 2.1

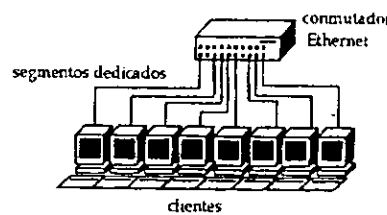


Figura 2.2

- **Ethernet conmutado dedicado (una sola estación)**

En este esquema de la figura 2.2, se conecta cada dispositivo final a un puerto del conmutador, de esta manera se dedican 10Mbps de ancho de banda a cada dispositivo final. Esta solución es especialmente deseable para los diferentes servidores de la red o para clientes que requieran altos anchos de banda para sus necesidades.

2.1.4 Otras funciones disponibles en algunos dispositivos de conmutación

Redes Virtuales

Las redes virtuales referidas como VLANs (Virtual LAN), son grupos de usuarios que son definidos basándose en su función lógica en lugar de su locación física. De esta manera, ayudan al desempeño y facilitan la administración de las redes en ambientes grandes de redes conmutadas. Por lo tanto, se puede decir, que una red LAN virtual (VLAN) es un grupo de anfitriones o dispositivos de red que forman un solo dominio de puenteo.

En conclusión, los conmutadores son ideales para ayudar al desempeño de las redes al poder expandir las capacidades del ancho de banda existente. Además de que preservan la protección de inversión al no requerir de grandes cambios en las redes actuales. Además, cabe mencionar que los conmutadores de redes LAN son tecnologías propietarias que trabajan por igual.

2.2 INTERFAZ DE DATOS DISTRIBUIDOS POR FIBRA (FDDI)

2.2.1 Orígenes de FDDI

FDDI (Fiber Distributed Data Interface) fue diseñado por la ANSI como respuesta a la necesidad de una red LAN troncal de alta velocidad. Para permitir mayor interoperabilidad con las redes locales existentes (Ethernet y Token Ring), el comité X3T9 de la ANSI siguió el estándar definido por los comités 802 de la IEEE.

En 1982 el estándar propuesto comenzó inicialmente como una Interfaz de Datos Distribuidos Localmente (LDDI: Locally Distributed Data Interface), pensada en un principio como un sistema de banda ancha (broadband) con un alcance de un kilómetro y siete nodos conectados. En 1986, ANSI publicó una propuesta que finalmente sería el FDDI como se conoce actualmente.

La arquitectura FDDI constituyó un excelente medio para construir redes de campus o backbone. Esta arquitectura beneficia principalmente a redes extensas, que poseen numerosos segmentos LAN, generadoras de una cantidad importante de tráfico.

2.2.2 Topología de FDDI

La arquitectura FDDI especifica una topología que tiene dos anillos de fibra óptica independientes y de sentido inverso, que proporciona una velocidad global de 200 Mbps, es decir, 100 Mbps para cada uno de los canales.

El anillo, que en realidad son dos anillos paralelos; primario (A) y secundario (B) pueden utilizarse para enviar datos por cada uno de ellos (usualmente solo se utiliza el primario), pero se puede utilizar para formar un solo anillo en caso de que haya una interrupción en la continuidad del medio físico (el anillo B es una ruta de respaldo y solo es usada cuando hay problemas en la ruta A).

Su topología incluye árboles, cada árbol se inicia de un concentrador conectado al doble anillo al cual se le pueden conectar estaciones y tantos niveles de concentradores como sea necesario.

Algunas estaciones, las denominadas estaciones de acoplamiento doble (DAS: Dual-Attached Station) se conectan a los dos anillos. De otro modo, las estaciones de acoplamiento único (SAS: Single-Attached Station) se conectan a través de un concentrador el cual, proporciona las conexiones oportunas a muchas SASs.

Una de las ventajas de esta configuración es que si una estación SAS falla no puede interrumpir el funcionamiento del anillo.

2.2.3 Cableado

Es importante mencionar que FDDI fue la primer red local diseñada para trabajar a 100 Mbps y que tomó como medio físico cables de fibra óptica multimodo 62.5/125. Posteriormente se definió la operación con fibra óptica unimodo 9/125, con otros tipos de fibra óptica (50/125, 85/125, 100/140 y 200/230) y con cable par trenzado UTP categoría 5 y STP IBM tipo 1. FDDI no exige necesariamente que todos los canales sean de fibra óptica. El concentrador (que permite conectar estaciones y reconfigurar el sistema así como de aislar los nodos problemáticos mediante el punto de concentración) puede incluir una interfaz en el que el usuario instalará fibra óptica para una parte de la red, y par trenzado o coaxial para otra parte de la red.

2.2.4 Codificación

El mejor código que puede emplearse en una red es aquel que proporciona cambios de señal frecuentemente. Estas variaciones permiten ajustar constantemente el receptor con los datos recibidos, garantizando de esta forma una perfecta sincronización entre el nodo emisor y el receptor.

Debido a esto, ANSI ideó el código llamado 4bits/5bits, en el que se usa un código de cuatro bits para crear otro de cinco bits.

DATOS DE USUARIO		CÓDIGO 4Bits/5Bits	
Binario	Hexadecimal	Código	Símbolos
0000	0	11110	0
0001	1	01001	1
0010	2	10100	2
0011	3	10101	3
0100	4	01010	4
0101	5	01011	5
0110	6	01110	6
0111	7	01111	7
1000	8	10010	8
1001	9	10011	9
1010	A	10110	A
1011	B	10111	B
1100	C	11010	C
1101	D	11011	D
1110	E	11100	E
1111	F	11101	F

Esto es, por cada cuatro bits que envía el transmisor, FDDI crea cinco. Estos cinco bits proporcionan la autosincronización buscada. De este modo, FDDI solo exige un ancho de banda de 125 MHz.

La ventaja de esta configuración es que ahorra ancho de banda, pero su desventaja es la pérdida de la autosincronización. Para compensar esta pérdida, se utiliza un largo preámbulo con objeto de sincronizar el receptor con el reloj del transmisor.

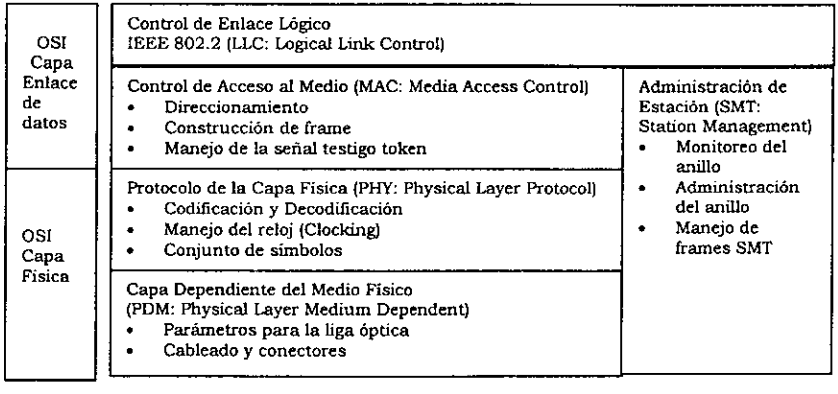
2.2.5 Operación de redes FDDI

El método de acceso de las redes FDDI es análogo al método de Token Ring denominado Token Passing with Early Token Release.

La red FDDI emplea un método de temporización de la trama (o testigo). Donde cada nodo mide el tiempo que tarda el testigo en regresar a él (TRT), y lo compara con el Tiempo Previsto de Llegada (PTT). Si la trama regresa antes de lo estimado según el PTT, ello indica, casi con seguridad, que la red no esta congestionada y que el nodo puede enviar todo el flujo de datos que requiera, siempre que no supere el tiempo marcado por PTT. Si, por el contrario, la trama llega después del plazo PTT, lo más probable es que la red este bastante congestionada y el nodo solo deberá transmitir el tráfico de alta prioridad.

2.2.6 Relación entre FDDI y OSI

La relación entre FDDI y el Modelo de Interconexión de Sistemas Abiertos (OSI), se muestra en la siguiente figura.



El nivel superior de FDDI encaja en el subnivel de acceso al medio (MAC) del nivel de enlace de datos. Por encima se encuentra el nivel de Control Enlace Lógico (LLC), que puede actuar como un puente y transferir los paquetes entre las redes Token Ring y Ethernet representadas. Los paquetes destinados a una estación de trabajo local se envían a los protocolos de niveles superiores en vez de reenviarlos.

2.2.7 Las cuatro subcapas principales de FDDI

Las cuatro áreas funcionales de las cuales se compone FDDI son:

1. Capa dependiente del medio físico (PMD: Physical Media Dependent).
2. Protocolo de la capa física (PHY: Physical Layer Protocol).
3. Control del acceso al medio (MAC: Media Access Control).
4. Administración de estación (SMT: Station Management).

PMD. Corresponde a la capa física del modelo OSI, en ella se especifican las señales ópticas y la forma de las ondas sobre el cable de fibra, además de su instalación (incluyendo los conectores). Con fibra óptica 62.3/125 de un mínimo de 500MHz, se especifica una distancia máxima de 2 km entre estaciones FDDI. La atenuación máxima del anillo FDDI es de 11 dB entre terminal y terminal. También existe la subcapa PMD que utiliza fibra monomodo referida como *SMF-PMD*, para cubrir una distancia de 60 km en lugar de 2 km entre estaciones.

PHY. Ésta corresponde a la mitad superior de la capa física del modelo OSI. Su función principal es codificar y decodificar las señales y del reloj, además de especificarse el tamaño máximo del frame. El proyecto de mejora llamado *PHY-2*, fue aprobado por ANSI en 1990.

MAC. Corresponde a la mitad más baja de la capa 2 (Enlace de datos) del modelo OSI. Planea y transfiere datos dentro y fuera del anillo FDDI, además de construir los paquetes, reconoce las direcciones de las estaciones, la señal testigo (token passing) y la generación y verificación de la Secuencia de Verificación del Frame (FCS: Frame Check Sequences). El proyecto de mejora fue referido como *MAC-2* aprobado en 1990.

SMT. Cubre las subcapas anteriores. Se encarga principalmente de la configuración inicial del anillo FDDI y el monitoreo del bit de error. Incluye la administración de la conexión y del anillo, así como sus funciones y servicios basados en frames.

2.2.8 Capacidad de FDDI

El estándar de FDDI especifica arriba de 500 estaciones (sea un concentrador, puente, brouter, enrutador o una estación final) conectadas directamente al anillo. Esto significa que el número máximo de estaciones no está limitado por el ancho de banda.

Utilizando fibra multimodo de 50/125 se llega a cubrir una menor distancia, ya que al utilizar monomodo de 9μm se puede extender la distancia entre estaciones por arriba de los 60 km dependiendo del equipo usado, aunque la distancia del anillo sigue siendo de hasta 100 km. Es por ello, que el anillo FDDI deberá ser segmentado en anillos por medio de compuertas, enrutadores o puentes para superar este límite.

Especificación	Tipo de cable	Distancia
PMD	Fibra Óptica 62.5/125	2km
TP-PMD	UTP Categoría 5 o STP IBM tipo 1	100m
SMF-PMD	Fibra Óptica 9/125	60km
LCF-PMD	Fibra Óptica 50/125, 85/125, 100/140, 200/230	500m

2.2.9 Tipos de FDDI

FDDI dispone de 3 modos de transmisión. Los dos primeros asíncrono y síncrono, ya aparecen en la norma FDDI original, mientras que el tercero, basado en circuitos, puede proporcionar circuitos dedicados. Este último modo se encuentra disponible en la nueva norma *FDDI-II.*

SERVICIOS ASÍNCRONOS. El modo de anillo asíncrono se basa en el uso de un testigo mediante el cual cualquier estación puede acceder a la red. Este modo implica que no se establece prioridad sobre algún tipo de tráfico, lo que perjudica el tránsito sensible al tiempo. Un método de resolución de tráfico consiste en almacenar los paquetes recibidos hasta completar el conjunto y ordenarlos. Esto involucra un retraso inaceptable en videoconferencias interactivas, aunque es aceptable si se trata de una visualización final de video almacenada.

SERVICIOS SÍNCRONOS. El modo de anillo síncrono con testigo permite realizar una priorización de trafico sensible al tiempo, de modo que los paquetes lleguen dentro de unos márgenes de tiempo. Las capacidades síncronas deben añadirse a través de actualizaciones de software en la mayoría de tarjetas FDDI existentes.

SERVICIO BASADO EN CIRCUITOS. Este modo utilizado únicamente en FDDI-II, puede crear una línea de comunicación dedicada entre dos estaciones de trabajo con un ancho de banda garantizado. Estos servicios de FDDI-II se proveen mediante la asignación de intervalos de tiempo regulares y repetidos durante la transmisión con objeto de crear un canal de comunicación dedicado entre dos estaciones. A este método se le denomina transmisión *isócrona.*

2.2.10 Comparación entre las versiones de FDDI

A continuación anexamos una tabla comparativa entre las versiones de FDDI conocidas.

Características	**FDDI**	**FDDI-II**	**FFOL**
Estado	Disponible	Por salir	Futuro
Madurez	Adulto	Prenatal	En proyecto
Complejidad	Media	Alta	Alta
Tasa de transmisión	100 Mbps	16 circuitos de 96 canales de 64 Kbps c/u	155Mbps - 2.48 Gbps
Medio de transmisión	Fibra Óptica, UTP, STP	Fibra Óptica	Fibra Óptica
Tipo de transmisión	Asíncrona y síncrona	Asíncrona, síncrona e isócrona	Asíncrona, síncrona, isócrona y ATM
Tipo de información	Datos, algo de multimedia	Datos, imágenes, voz, audio y video	Datos, imágenes, voz, audio y video

FFOL (FDDI Follow-On LAN) es el nombre propuesto al estándar que reemplazará algún día a FDDI para operar arriba de 2.4 Gbits/s.

2.2.11 Diferencias entre FDDI y FDDI-II

Ambos FDDI y FDDI-II corren a 100 Mbits/s en fibra. FDDI puede transportar ambos tipos de frames asíncrono y síncrono. FDDI-II tiene un nuevo modo de operación llamado *Modo Híbrido* (HRC: Hybrid Ring Control), este modo usa una estructura de ciclo de 125μs para modo isócrono, en adición a los frames síncrono/asíncrono. FDDI-II soporta integradas capacidades de voz, video y datos, y por lo tanto expande el rango de aplicaciones de FDDI. Las estaciones FDDI y FDDI-II pueden ser operadas en el mismo anillo solo en modo básico.

Estándar FDDI-II

FDDI-II es un conjunto de estándares desarrollados por el Instituto de Estándares Nacionales Americanos (ANSI), el Comité de Estándares Acreditados (ASC) y el Grupo de Trabajo X3T9.5. Sus componentes se conocen como MAC-2, PHY-2 y SMT-2.

Es compatible hacia abajo con FDDI a partir, de que FDDI-II puede interpretar la parte de datos de FDDI. FDDI no es compatible hacia arriba con FDDI-II porque no puede interpretar la parte de voz y video. Los servicios básicos de FDDI pueden estar disponibles desde una estación FDDI-II además, esta estación deberá soportar el Control de Anillo Híbrido (HRC) para las funciones del anillo FDDI-II.

La norma FDDI-II se ha diseñado para redes que necesitan transportar video en tiempo real u otro tipo de información que no puede tolerar retrasos de tiempo. La arquitectura, requiere que todos los nodos de la red utilicen FDDI-II; de otro modo, la red se convierte en una FDDI.

FDDI-II utiliza técnicas de multiplexaje que dividen el ancho de banda en circuitos dedicados, y de esta forma garantizan la distribución del tráfico multimedia. Puede crear hasta 16 circuitos separados que trabajen dentro de unos márgenes de velocidad establecidos (entre 6.144 Mbps hasta 99.072 Mbps cada uno). Además estos canales pueden subdividirse para producir un total de 96 circuitos separados a 64 Kbps.

Además de la capacidad de conmutación de paquetes que soporta el protocolo FDDI, incluye la capacidad de conmutación de circuitos, la cual provee soporte para determinar el tiempo usado para la transmisión de video y voz, entre otros.

El anillo FDDI-II sólo opera en el modo en el que fue inicializado, es decir; básico o híbrido. El tamaño del frame en el modo híbrido no esta limitado a 4500 bytes como es para el modo básico.

Subcapa HRC

Es la principal diferencia entre FDDI-II y FDDI. HRC es la subcapa más baja de la capa de liga de datos, tomando su lugar entre la subcapa MAC y la PHY.

El HRC esta compuesto de los protocolos Multiplexor Híbrido (H-MUX: Hybrid Multiplexor) y el Control de Acceso al Medio Isócrono (I-MAC: Isochronous Media

Access Control). El H-MUX integra paquetes de datos isócronos en ciclos que se transmiten y reciben del medio utilizando los servicios de la capa física del modelo OSI.

El I-MAC provee canales de transmisión separados para la transferencia de información isócrona de los usuarios. El anillo HRC puede operar hasta 100 Mbps.

Especificaciones del SMT para FDDI-II

El estándar SMT-2 se construyó sobre el actual SMT (Administración de Estación) y está conformado por tres documentos que son: Servicios Comunes de Administración de Estación para FDDI-II (SMT-2-CS), Servicios Propios de Administración de Estación para FDDI-II (SMT-2-PS) y los Servicios Isócronos de Administración de Estación para FDDI-II (SMT-2-IS).

Productos de FDDI-II

Aunque FDDI-II todavía no está disponible, la compañía Alfa, Inc. Ha introducido un sistema llamado FDDI-Sync el cual es esencialmente una implementación FDDI-II pre-estándar.

2.3 FAST ETHERNET

En esta sección incluimos un breve tutorial del sistema Ethernet. Trataremos solo los orígenes y los estándares de Ethernet dada su similitud con Fast Ethernet. Después describiremos las características esenciales de la operación de Fast Ethernet.

2.3.1 El sistema Ethernet

Ethernet es una tecnología de redes de área local (LAN) que transmite información entre computadoras a velocidades de 10 y 100 Mbps.

Actualmente la versión más usada de esta tecnología es la variedad de par trenzado de 10 Mbps. El estándar más reciente de Ethernet define el nuevo sistema de Fast Ethernet a 100 Mbps el cual opera sobre medio par trenzado y fibra óptica.

Una razón por la cual Ethernet es tan comúnmente implementada en la industria de la computación es que, sus especificaciones y los derechos para construirla han estado disponibles para cualquiera, combinadas con la facilidad de usarse y la fuerza del sistema Ethernet.

Como el estándar 100 Mbps se convirtió en el más adoptado, las computadoras están siendo equipadas con una interfaz Ethernet que opera a ambos 10 y 100 Mbps. La habilidad para ligar un rango amplio de computadoras usando una tecnología de red neutral es una característica esencial para los administradores de LANs de hoy.

Desarrollo de Estándares de Ethernet

Ethernet fue inventado en el Centro de Investigaciones de Palo Alto Xerox en los '70s por el Dr. Robert M. Metcalfe. El primer sistema Ethernet corrió aproximadamente a 3 Mbps y fue conocido como "Ethernet experimental".

Las especificaciones formales para Ethernet fueron publicadas en 1980, fue entonces cuando esta tecnología fue adoptada para estandarización por el Comité de Estándares LAN del Instituto de Ingenieros Electricistas y Electrónicos (Institute of Electrical and Electronics Engineers) como IEEE 802.

El estándar de IEEE fue publicado por primera vez en 1985, con el título formal de "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications". El estándar de IEEE ha sido adoptado por la Organización Internacional para la Estandarización (ISO), lo cual lo hace un estándar de red mundial mejor conocido por su nombre original de Ethernet.

Elementos del Sistema Ethernet

El sistema Ethernet consta de tres elementos básicos:

1. El medio físico usado para transportar las señales Ethernet entre computadoras,
2. Un conjunto de reglas de control de acceso al medio fijadas en cada interfaz, y
3. Una trama Ethernet que consta de un conjunto estandarizado de bits usado para transportar datos sobre el sistema.

Operación de Ethernet

Cada computadora equipada con Ethernet (conocida como estación), opera independientemente de todas las otras estaciones en la red: no hay un controlador central. Todas las estaciones son conectadas a un sistema de señalización compartido, llamado el medio. Las señales de Ethernet se transmiten serialmente, un bit a la vez, sobre el canal de señales compartido para cualquier estación conectada. Para enviar datos a una estación primero escucha el canal, y cuando el canal está desocupado la estación transmite sus datos en forma de una trama Ethernet o paquete.

Después de cada transmisión de trama, todas las estaciones de la red deben competir por igual por la siguiente oportunidad de transmisión de trama. El acceso al canal compartido se determina por el mecanismo de control de acceso al medio (MAC) fijado en la interfaz Ethernet localizada en cada estación. El mecanismo de control de acceso al medio esta basado en el sistema CSMA/CD.

El Protocolo CSMA/CD

El protocolo CSMA/CD funciona un poco como una fiesta en un cuarto oscuro. Todo mundo alrededor de la mesa debe escuchar por un período de quietud antes de hablar (Carrier Sense). Una vez que ocurre un espacio cada cual tiene una oportunidad igual para decir algo (Multiple Access). Si dos personas empiezan a hablar al mismo instante ellas detectan lo ocurrido, y paran de hablar (Collision Detection).

Para traducir esto en términos de Ethernet, cada interfaz debe esperar hasta que no exista señal en el canal, entonces este puede empezar a transmitir. Si alguna otra interfaz esta transmitiendo allí se dará una señal en el canal, la cual se llama portadora (Carrier). Todas las otras interfaces deben esperar hasta que la portadora cese antes de tratar de transmitir, y este proceso se llama Detección de Portadora (Carrier Sense).

Para mejor compresión del método, así como sus características y las colisiones ver el capítulo anterior en la sección 1.3.3.

2.3.2 Fast Ethernet

A continuación describiremos el sistema 802.3 y los segmentos Fast Ethernet 100BASE-T que son parte de este sistema.

Cuando el comité de estandarización IEEE comenzó a trabajar en un sistema más rápido que Ethernet, presentó dos propuestas. Una de ellas fue acelerar el sistema Ethernet original a 100 Mbps, conservando el mecanismo de control de acceso al medio CSMA/CD. Esta propuesta se conoce como Fast Ethernet 100BASE-T. La otra propuesta presentada por el comité fue crear un mecanismo completamente nuevo de control de acceso al medio, basado en hubs que controlaran este acceso usando un mecanismo de "prioridad de petición". Este sistema fue extendido para permitir transportar también frames Token Ring. Como conclusión, esta propuesta es llama ahora 100VG-AnyLAN.

El IEEE decidió crear estándares para ambas propuestas. El estándar Fast Ethernet 100BASE-T descrito aquí es parte del estándar original 802.3. El sistema 100VG-AnyLAN está estandarizado bajo un número nuevo: IEEE 802.12, que se describirá en la siguiente sección.

Sistemas 100 Mbps

Comparado a las especificaciones de 10 Mbps, el sistema 100 Mbps incrementa diez veces la velocidad de los paquetes sobre el medio. Sin embargo, otros aspectos importantes del sistema Ethernet como es el formato de trama, la cantidad de datos que una trama puede llevar y el mecanismo de control de acceso al medio, son iguales.

Las especificaciones de Fast Ethernet incluyen mecanismos para Auto-Negociación de la velocidad. Esto hace posible la distribución de interfaces Ethernet dual-speed que pueden instalarse y correr a 10 ó 100 Mbps automáticamente.

Existen 3 variedades de medio especificados para transmitir sobre este sistema.

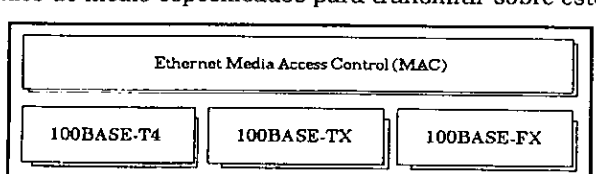


Figura 2.3

Los 3 tipos de medio mostrados, se presentan con sus identificadores IEEE. Los identificadores IEEE incluyen 3 partes de información. El primer número, "100", establece la velocidad media de 100 Mbps. La "BASE" establece la "banda base," la cual es un tipo de señalización que significa que las señales Ethernet son las únicas soportadas en el sistema. La tercera parte del identificador provee una indicación del tipo de segmento. El tipo de segmento "T4" es un segmento par trenzado que usa cuatro pares de hilos par trenzado grado telefónico. El tipo de segmento "TX" se refiere a par trenzado que usa dos pares de hilos y se basa en el estándar de medio físico con grado de datos desarrollado por ANSI. El segmento tipo "FX" es un segmento de enlace de fibra óptica basado en el estándar de medio físico desarrollado por ANSI y que usa dos hilos de cable de fibra.

Los estándares del medio TX y FX son colectivamente conocidos como 100BASE-X. El estándar T4 también fue provisto para hacer posible el uso de cable par trenzado de baja calidad para señales Ethernet a 100 Mbps.

Componentes usados para la conexión 100 Mbps

La figura 2.4 es un diagrama de bloques de los componentes definidos en el estándar IEEE, que pueden usarse para hacer una conexión al sistema 100 Mbps. Estos componentes difieren un poco de los usados en un sistema a 10 Mbps.

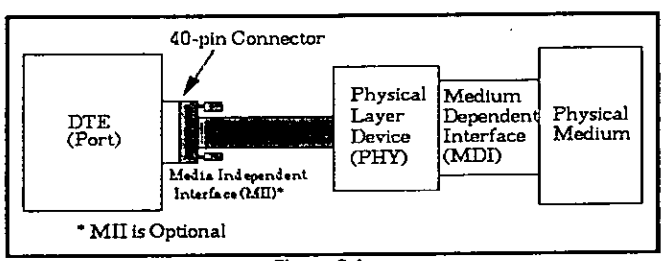


Figura 2.4

- **Medio físico**

Comenzando del lado derecho del diagrama de bloques, encontramos el medio físico usado para transportar señales Ethernet entre computadoras. Éste puede ser cualquiera de los 3 tipos de medio 100 Mbps. Se puede hacer una conexión al medio con la **interfaz dependiente al medio**, o **MDI**. Éste es un conector par trenzado de 8 pines o conector de fibra óptica en el sistema 100BASE-T.

- **Dispositivo de capa física**

El dispositivo siguiente del diagrama se llama Dispositivo de la Capa Física (PHY). Puede ser un conjunto de circuitos integrados en lugar del puerto Ethernet de un dispositivo de red (invisible al usuario), o puede ser una pequeña caja equipada con un cable MII, como el transceiver exterior y cable transceiver usado en Ethernet 10 Mbps.

- **Interfaz independiente al medio**

El MII es un conjunto opcional de electrónicos que provee un camino para unir las funciones de control de acceso al medio Ethernet en el dispositivo de red con el dispositivo de la capa física (PHY) que envía señales al medio de red. Un MII permite soportar opcionalmente ambas operaciones 10 y 100 Mbps, admitiendo cómodamente dispositivos de red para conectar a ambos segmentos de medio.

El MII convierte las señales de línea recibidas de los diversos segmentos por el transceiver (PHY) en señales digitales que son entonces provistas a los chips Ethernet en el dispositivo de red. La electrónica opcional MII, y el conector hembra de 40 pines asociado y el cable MII, hacen posible conectar un dispositivo de red a cualquier de los tipos del medio, proveyendo máxima flexibilidad.

El cable MII para uso con transceivers externos 100 Mbps, esta especificado como un cable de 40 pines con un enchufe de 40 pines al final, equipado con tornillos jack machos. El cable puede ser máximo de 0.5 metros en longitud (casi 19.6 pulgadas).

- **Equipo terminal de datos o Computadora**

El dispositivo conectado a la red por si mismo se define como **equipo terminal de datos (DTE)** en el estándar IEEE. Cada DTE anexado es equipado con una interfaz Ethernet que provee una conexión al medio, y contiene los dispositivos electrónicos y software necesarios para desarrollar las funciones de control requeridas para enviar (después de formar) las tramas sobre el canal Ethernet. Esta interfaz, está unida al medio usando equipo que puede incluir, un cable MII externo y un transceiver PHY con su asociado MDI (par trenzado RJ45 estilo jack o conector de fibra óptica).

Un puerto de repetidor conectado al sistema de medio Fast Ethernet usa la misma PHY y equipo MDI. Sin embargo, los puertos de los repetidores operan en el nivel de bit individual para señales Ethernet, moviendo las señales directamente de segmento a segmento. Por lo tanto, cabe hacer notar que los puertos del repetidor no contienen interfaces Ethernet ya que no operan a nivel de tramas Ethernet.

Por otro lado, un hub repetidor puede estar equipado con una interfaz Ethernet para proveer un camino de comunicación con el hub sobre la red. Esto permite proveer una interfaz manejable en el hub que puede interactuar con una estación remota, usando el Protocolo de Administración de Red Simple (SNMP: Simple Network Management Protocol).

Existen dos clases de repetidores en el sistema 100BASE-T: I y II. Siguiendo el estándar, los repetidores Fast Ethernet deben ser etiquetados con el número romano "I" o "II" encerrado en un círculo.

2.3.3 Sistema de medio 100 Mbps TX

La interfaz 100BASE TX se muestra en la figura 2.5 conectada directamente a un puerto del hub (Clase II) 100BASE-TX. También pueden usarse transceivers unidos a un conector MII de 40 pines en la interfaz para hacer esta conexión.

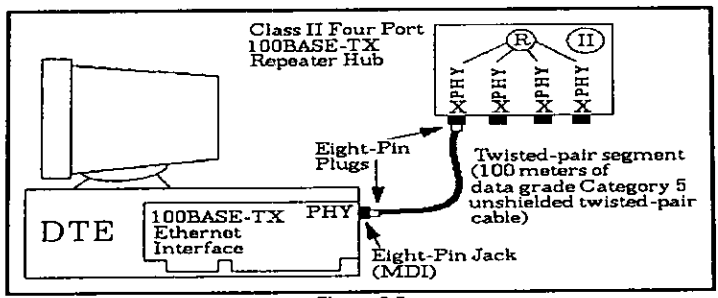


Figura 2.5

El sistema de medio 100BASE-TX esta basado en especificaciones publicadas en el estándar de medio físico ANSI TP-PMD. Este sistema opera sobre dos pares de cables, un par para recibir las señales de datos y el otro par para su transmisión, ya que la especificación ANSI TP-PMD provee el uso de cables par trenzado blindado o sin blindaje.

El cableado más popular usado es el cable par trenzado sin blindar. Los dos hilos de cada par del cable deben ser trenzados juntos, y guardar el trenzado entre ½ pulgada aproximadamente de cualquier conector o punto terminal de cable. Ésta es una técnica del estándar usada para mejorar las características de la señal enviada a través de un par de cables no blindados.

Componentes de 100BASE-TX

El siguiente conjunto de componentes se usa para construir un segmento par trenzado 100BASE-TX y hacerle conexiones:

- Medio de red
- Repetidores 100BASE-TX
- Instalación de paso (crossover) 100BASE-TX
- Prueba de integridad de enlace 100BASE-TX

- **Medio de red**

El sistema de medio 100BASE-TX esta diseñado para permitir segmentos arriba de los 100 metros usando cable par trenzado sin blindar (con impedancia característica de 100 ohms y especificaciones de cable EIA/TIA categoría 5). Los segmentos limitados a un máximo de 100 metros son para asegurar que las especificaciones de coordinación de transporte sean cumplidas. Esto está en contraste con el sistema de medio 10BASE-T, donde la longitud máxima de segmento para 10 Mbps está generalmente limitada por la fuerza de la señal.

El estándar de cableado EIA/TIA recomienda una longitud de segmento de 90 metros entre el equipo de terminación, en el closet de instalación y la pared en la oficina. Esto provee 10 metros de cable para acomodar cables de parcheo al final de cada liga, señalar perdidas en terminaciones de cable intermedio en la liga, etc.

Existen probadores de cable Ethernet par trenzado disponibles que permiten checar las características eléctricas del cable usado, para estar seguro que satisface las especificaciones eléctricas importantes del estándar. Estas especificaciones incluyen crosstalk de señal (cruce de línea o interferencia), la cual se refiere a la cantidad de señal que cruza entre el par receptor y el transmisor, y atenuación de señal, la cual es la cantidad de señal pérdida encontrada en el segmento.

El sistema de medio 100BASE-TX usa dos pares de hilos, lo cual significa que cuatro de ocho pines del conector MDI (estilo RJ-45) se usan para transportar señales Ethernet.

Número del pin	Señal
1	Transmite +
2	Transmite -
3	Recibe +
4	No se usa
5	No se usa
6	Recibe -
7	No se usa
8	No se usa

Las señales de transmisión y recepción de datos en cada par de un segmento 100BASE-TX son polarizadas, con un par de hilos enviando la señal positiva (+), y el otro enviando la señal negativa(-).

El número de pines usados en el conector de 8 pines para 100BASE-TX se cambió a unos definidos en el estándar TP-PMD de ANSI, en orden para ajustarse al esquema de cableado ya usado en el estándar 10BASE-T. El estándar ANSI usa el pin 7 y 8 para recibir datos, mientras que 100BASE-TX usa los mismos pines que el sistema 10BASE-T: 3 y 6. De esa manera, una tarjeta 100BASE-TX puede remplazar una 10BASE-T, y ser conectada en el mismo sistema eléctrico categoría 5 sin hacer ningún cambio de instalación.

El estándar 100BASE-TX también adapta cableado par trenzado blindado (sistemas ya construidos) con una impedancia característica de 150 ohms. Si se usa el cable par trenzado brindado con conectores "tipo D" de 9 pines, el conector es alambrado de acuerdo a las especificaciones TP-PMD de ANSI: pin 1 recibe (+), pin 5 transmite (+), pin 6 recibe (-), pin 9 transmite (-).

- **Repetidores 100BASE-TX**

De acuerdo al estándar Fast Ethernet se definen dos tipos de repetidores: clase I y clase II. Un repetidor Clase I esta asignado para tener largos retrasos y operar por traslado de señales de línea en un puerto entrante a la forma digital, y después retransmitirlas a señales de línea cuando las envía fuera en otros puertos. Esto hace posible repetir señales entre segmentos que usan diferentes técnicas de señalización, como segmentos 100BASE-TX/FX y 100BASE-T4, permitiendo mezclarlos dentro de un simple hub repetidor. El proceso de translación en repetidores Clase I usa un número de momentos de bit, pero sólo un repetidor Clase I puede usarse en un dominio de colisión dado, cuando se usan las longitudes de cable máximas.

Un repetidor Clase II es restringido a retrasos más pequeños, e inmediatamente repetir la señal entrante a todos los otros puertos sin un proceso de translación. Para ello se conecta solo a tipos de segmento que usan la misma técnica de señalización, como segmentos 100BASE-TX y 100BASE-FX. Pueden usarse un máximo de dos repetidores clase II entre un dominio de colisión cuando se usan las longitudes máximas de cable. Tipos de segmentos con diferentes técnicas de señalización (como son; 100BASE-TX/FX con 100BASE-T4) comúnmente no pueden combinarse juntos en un hub repetidor clase II.

- **Instalación de paso (crossover) 100BASE-TX**

Cuando se conectan dos estaciones juntas sobre un segmento, los pines de transmisión de datos de un MDI deben ser alambrados a los pines de recepción de datos del otro MDI, y viceversa.

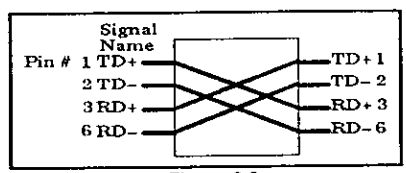


Figura 2.6

Sin embargo, cuando se instalan segmentos múltiples en una aplicación, es mucho más fácil alambrar los conectores de cable "recto" (straight through) y no preocuparse por si los cables de conexión u otros cables par trenzado en la aplicación han sido cruzados correctamente. El camino para realizar esto es hacer el cableado crossover internamente en el hub repetidor. El estándar 100BASE-TX recomienda esto, y afirma que cada puerto del hub que es cruzado internamente debe ser marcado con una "X".

- **Prueba de integridad de enlace 100BASE-TX**

El sistema de señalización usado, está basado en el sistema de FDDI de ANSI, el cual envía señales continuamente, incluso durante periodos de ocio (no tráfico) de la red. Por lo tanto, la actividad en la ruta de datos de recepción es suficiente para proveer chequeo continuo de integridad del enlace.

No obstante, los transceivers par trenzado 100BASE-TX que usan conectores MDI de 8 pines también envían y reciben pulsos. Estos pulsos son llamados **Pulsos de Enlace Rápido** (Fast Link Pulses), y se usan en el mecanismo de Auto-Negociación el cual permite a un hub detectar la velocidad de operación de un dispositivo Ethernet que este conectado a él, y ajustar la velocidad de los puertos del hub como corresponde a la Auto-Negociación descrita más adelante.

Principios de configuración de 100BASE-TX

Los segmentos Ethernet 100BASE-TX se definen como *segmentos de enlace* en las especificaciones Ethernet, los cuales están formalmente definidos como un medio punto a punto que conecta dos y solo dos MDIs. Una instalación típica usa hubs repetidores multipuerto, o hubs switching de paquetes, para proveer una conexión entre un número grande de segmentos de enlace.

Las especificaciones de 100BASE-TX permiten un segmento arriba de los 100 metros. Dos segmentos de 100BASE-TX de 100 metros pueden ser conectados juntos a través de un simple repetidor clase I o clase II. Esto provee un sistema con un diámetro total de 200 metros entre DTEs.

Topología física de par trenzado 100BASE-TX

La topología física soportada por segmentos enlazados de par trenzado es de estrella. En esta topología un conjunto de segmentos enlazados están conectados a un hub, radiando del hub a las computadoras como los rayos de una estrella.

2.3.4 Sistema de medio fibra óptica de 100 Mbps

La interfaz 100BASE-FX se muestra conectada directamente a un puerto del hub 100BASE-FX. Pueden usarse los transceivers externos unidos a un conector MII de 40 pines en la interfaz o el hub, para hacer su conexión.

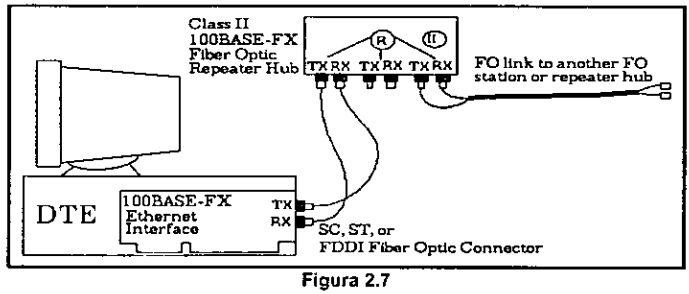


Figura 2.7

Componentes 100BASE-FX

Para construir un segmento de fibra óptica 100BASE-FX, y hacer conexiones a este se usan los siguientes componentes. Se debe enfatizar que esto es solo una introducción y que no se incluye información para construir y manejar sistemas de este tipo.

- Medio de red
- Conectores MDI
- Repetidores 100BASE-FX
- Prueba de integridad de enlace 100BASE-FX

- **Medio de red**

Este sistema de medio, está diseñado para permitir segmentos de 412 metros. Aunque es posible enviar señales sobre fibra por distancias más largas, este límite de fibra en Fast Ethernet es para asegurar que las especificaciones de cronometraje se cumplan.

La especificación de 100BASE-FX requiere dos hilos de cable de fibra óptica multimodo (MMF) por enlace, uno para transmitir datos y otro para recibir (TX a RX).

El cable fibra óptica típico usado para un segmento de enlace de fibra es un cable MMF índice graduado, con un núcleo de fibra óptica de 62.5 micras y 125 micras de revestimiento externo (62.5/125). La longitud de onda de la luz usada es de 1350 nanometros (1350 nm). Hay un estimado de pérdida de 11 dB permitido por enlace, lo que significa que la potencia total perdida a través de la fibra y conectores asociados no debe ser más alta que 11 dB (medida por un metro de potencia de fibra).

La pérdida óptica es medida con instrumentos de prueba de fibra óptica que pueden decirnos exactamente cuánta pérdida óptica habrá en un segmento dado con una longitud dada de luz. Un funcionamiento en condiciones normales de operación para fibra grado estándar en 1350 nm proveerá un rango de perdida de 1 dB a 2 dB por 1000 metros de cable. Se puede también esperar un rango de perdida de 0.5 a 2.0 dB por punto de conexión, dependiendo de que tan bien se haya hecho. Si los conectores o empalmes de fibra están hechos pobremente, o si hay aceite de los dedos o polvo en los extremos del conector, entonces podemos tener pérdida óptica más alta en el segmento.

- **Conectores MDI**

La interfaz dependiente al medio (MDI) para una liga 100BASE-FX puede ser una de las tres clases de conectores de fibra óptica. De éstas, el *conector SC* dúplex es la alternativa recomendada en el estándar. Este conector SC esta diseñado para un uso fácil; sólo es puesto en el lugar y automáticamente completa la conexión.

Otro tipo de conector que puede usarse es un conector interfaz de medio FDDI (MIC). Éste es un conector acuñado estándar usado en el sistema LAN de FDDI. Los *conectores MIC* son acuñados de varias formas, referidos como A, B, M y S, para asegurar que el cableado FDDI esta conectado apropiadamente. Así por ejemplo, sí un MIC de FDDI es usado como un MDI de 100BASE-FX, las especificaciones establecen que deben ser acuñado como un receptáculo "M". Sólo basta con ponerlo en su lugar y automáticamente completa la conexión.

El tercer tipo de conector que puede ser usado es comúnmente llamado *conector ST*. Éste es el mismo conector que se usa en un enlace 10BASE-FL. Éste es un conector tipo bayoneta que tiene una llave en un manguito interior y también un anillo bayoneta exterior.

- **Repetidores 100BASE-FX**

Las clases I y II de repetidores antes mencionados, definidos por el estándar Fast Ethernet son los que se usan.

- **Prueba de Integridad del enlace 100BASE-FX**

El sistema de señalización usado para segmentos 100BASE-FX esta basado en el sistema de señalamiento FDDI de ANSI, cuyo funcionamiento es igual al descrito para 100BASE-TX.

Principios de configuración de 100BASE-FX

Los segmentos Ethernet 100BASE-FX también están definidos como segmentos de enlace en las especificaciones Ethernet. Y al igual que para par trenzado, su instalación más común usa hubs repetidores multipuerto o switching de paquetes.

Hay que hacer notar que mientras un segmento simple 10BASE-FX puede estar arriba de los 412 metros de distancia, cuando se usan repetidores, la distancia máxima entre DTEs será menor. Si un repetidor simple clase II se usa para enlazar segmentos de fibra, entonces la distancia máxima entre los dos DTEs puede ser de 320 metros. Esta distancia máxima también se llama **diámetro de dominio de colisión máxima**. Si se usa un repetidor simple de clase I, entonces esta distancia entre los DTEs enlazados con todos los segmentos de fibra será de 272 metros. Finalmente, si se usan dos repetidores clase II, la distancia máxima entre dos DTEs puede ser de 228 metros.

Topología física de fibra óptica de 100BASE-FX

La topología física soportada es la de estrella. Representada también como un conjunto de estos segmentos enlazados en forma radial de un hub a las computadoras.

2.3.5 Sistema de medio 100BASE-T4

La interfaz 100BASE-T4 se muestra conectada directamente a un puerto del hub clase II. Los transceivers externos unidos al conector MII de 40 pines en la interfaz o el hub pueden usarse también para esta conexión.

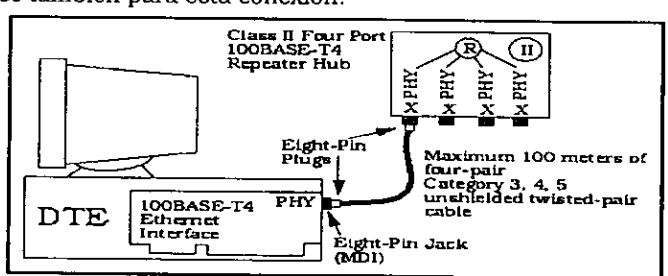


Figura 2.8

Este sistema opera sobre cuatro pares de hilos, con un sistema de señalización que hace posible proveer señales Fast Ethernet sobre cable estándar par trenzado sin blindar categoría 5 grado voz.

Componentes de 100BASE-T4

Para construir un segmento 100BASE-T4 y hacer conexiones a él se requiere:

- Medio de red
- Repetidores 100BASE-T4
- Instalación de paso 100BASE-T4
- Prueba de integridad de enlace 100BASE-T4

- **Medio de red**

El sistema de medio 100BASE-T4 esta diseñado para permitir segmentos por arriba de los 100 metros de distancia cuando se usa cable par trenzado sin blindaje categoria 3, 4 o 5 de EIA/TIA. Las especificaciones recomiendan usar cables categoría 5, cables de conexión y hardware de vínculo cada vez que sea posible, ya que la alta calidad de los componentes y cables proveerá la recepción de señales en el enlace.

Los segmentos de 100BASE-T4 están limitados a un máximo de 100 metros, para asegurar que las especificaciones del tiempo de round trip (viaje redondo) se cumplan. Esto es contrastante ya que, si se usa cable par trenzado de alta calidad en un segmento de 10 Mbps 10BASE-T, es posible alcanzar longitudes de segmentos de alrededor de 150 metros con éxito.

El estándar de cableado de EIA/TIA recomienda una longitud de segmento de 90 metros entre el cable del equipo terminal (closet), y la pared de la oficina, para tener 10 metros de cable para ayudar a acomodar cada enlace. Las pruebas de cable son las ya mencionadas en la sección de par trenzado.

El sistema de medio requiere que los 8 pines del conector MDI (estilo RJ-45) se usen.

Número del pin	Señal
1	Transmite +
2	Transmite -
3	Recibe +
4	Bidireccional +
5	Bidireccional -
6	Recibe -
7	Bidireccional +
8	Bidireccional -

Como se muestra en la tabla, de los 4 pares polarizados, un par es para transmisión de datos (TX), un par es par recibir datos (RX), y dos son bidireccionales (BI).

- **Instalación de paso (crossover) 100BASE-T4**

Requiere un paso de señal entre dispositivos conectados a un segmento 100BASE-T4, de manera que los pines de datos TX y bidireccionales en el extremo del dispositivo sean conectados a los pines de datos RX y bidireccionales del otro extremo del dispositivo y viceversa. El estándar recomienda el crossover internamente en el puerto del repetidor, y si esto se hace entonces el puerto debe marcarse con una "X".

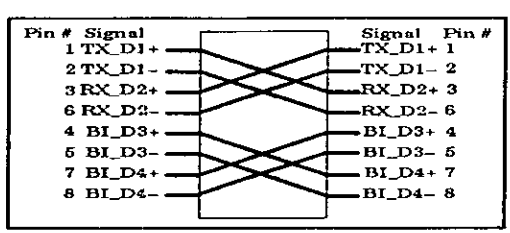


Figura 2.9

Si dos estaciones son unidas con este segmento, o si el repetidor no implementa la señal crossover internamente, entonces debe proveerse un cable especial crossover como el que muestra la figura.

El cable para un segmento 100BASE-T4 debe ser alambrado de tal forma que el par TX al final del cable, éste conectado al par RX en el otro extremo del cable, y viceversa. Así mismo, el par BI_D3 a un extremo del cable es conectado al par BI_D4 del otro extremo, y viceversa.

- **Prueba de integridad de enlace 100BASE-T4**

Los circuitos de transceivers Fast Ethernet continuamente controlan la ruta de los datos recibidos checando que el enlace este trabajando correctamente. Cuando la red está ocupada, los transceivers 100BASE-T4 envían pulsos de enlace sobre el segmento para verificar la integridad del enlace.

Es importante que las luces de enlace estén encendidas, una de cada extremo. Lo que indica que existe una ruta de señal alambrada correctamente entre ambos dispositivos. Ya que el pulso de enlace, opera más lento que las señales Ethernet actuales, las luces de enlace no son una garantía de que las señales Ethernet estén trabajando correctamente sobre el segmento.

Principios de configuración de 100BASE-T4

Sus segmentos también están definidos como segmentos de enlace en las especificaciones Ethernet. Y sus especificaciones son iguales a las de 100BASE-TX y 100BASE-FX

Las especificaciones de 100BASE-T4 permiten un segmento arriba de los 100 metros. Dos segmentos de 100BASE-T4 de 100 metros pueden conectarse juntos a través de un repetidor simple clase I o clase II. Esto provee un sistema con un diámetro total de 200 metros entre DTEs.

Topología física de par trenzado 100BASE-T4

La topología soportada es la de estrella, como en todos los casos de Fast Ethernet.

2.3.6 La Auto-Negociación

La función de auto-negociación es una parte opcional del estándar Ethernet que hace posible el intercambio de información entre dispositivos sobre un segmento de enlace. Esto, permite que los dispositivos funcionen automáticamente para alcanzar el mejor modo posible de operación sobre un enlace. La auto-negociación puede proveer velocidad automática para dispositivos multi-velocidad en cada extremo del enlace. Las interfaces Ethernet multi-velocidad pueden entonces tomar ventaja sobre las convencionales ya que son más rápidos los enlaces.

El protocolo de auto-negociación incluye sensado automático de otras capacidades. Por ejemplo, un hub que es capaz de soportar operación full dúplex en algunos o todos sus puertos, puede advertir ese hecho con el protocolo de auto-negociación. Las interfaces conectadas al hub que también soporten operación full dúplex pueden entonces configurarse a sí mismas usando el modo full dúplex en interacción con el hub.

2.3.7 Pulso de enlace rápido

La auto-negociación toma lugar usando señales de Pulso de Enlace Rápido (FLP: Fast Link Pulse). Estas señales son una versión modificada de las señales de Pulso de Enlace Normal (NLP: Normal Link Pulse) usadas para verificar la integridad de enlace, también definidas en las especificaciones 10BASE-T originales. Las señales FLP son generadas automáticamente al encender (power-up), o pueden ser seleccionadas manualmente a través de la interfaz de un dispositivo de auto-negociación.

Las señales de pulso de enlace rápido son diseñadas para coexistir con las señales NLP, de manera que un dispositivo 10BASE-T que usa señales NLP continúe detectando la integridad de enlace apropiada cada que se agrega un hub de auto-negociación que envía señales FLP. Como el pulso de enlace 10BASE-T original, las señales FLP toman lugar durante los tiempos de ocio en el enlace de red y no interfieren con el tráfico normal. Cabe hacer notar que ambos pulsos son especificados solo para medio par trenzado usando conectores de 8 pines, tal como 100BASE-TX sobre par trenzado sin blindar. Esto significa que los dispositivos de red y puertos de repetidores enlazados sobre segmentos de fibra óptica no pueden participar en la auto-negociación.

Las señales FLP son usadas para enviar información sobre las capacidades del dispositivo. El protocolo de auto-negociación contiene reglas para la configuración de dispositivos basadas en esta información.

La característica de auto-negociación es opcional, y por lo tanto el protocolo de auto-negociación es diseñado para trabajar con interfaces 100BASE-T que no soportan FLP y auto-negociación así como con las interfaces más viejas 10BASE-T que fueron construidas antes que la auto-negociación existiera. El sistema de auto-negociación, incluye una interfaz opcional que permite deshabilitar la auto-negociación, o bien forzar manualmente el proceso de negociación y seleccionar un modo operacional específico para un puerto determinado del hub.

2.4 100 VG-ANYLAN

En junio de 1995, el IEEE certificó la especificación 100VG-AnyLAN para el estándar 802.12. Sin embargo, mucho antes de esa fecha, los que la propusieron (dirigidos por Hewlett Packard Company Inc.), la presentaron como la última oportunidad de conversión para las redes de 10BASE-T. Aunque 100VG-AnyLAN tiene muchas similitudes con el protocolo 802.3, emplea métodos de acceso a datos y señalización que difieren drásticamente de los de Ethernet y Fast Ethernet.

En vez del protocolo clásico de CSMA/CD basado en colisiones que utilizan los estándares 802.3 y 802.3u, al método de acceso a datos 802.12 se le conoce como **acceso con prioridad por demanda** (DPA: Demand Priority Access), en el cuál la estación de trabajo inicia las transferencias de datos y el concentrador (hub) confirma los datos y dirige la transferencia. Difiere de CSMA/CD en dos puntos fundamentales:

- La transferencia de datos la controla el concentrador en vez del adaptador de red.
- Se eliminan las colisiones porque a cada nodo se le garantiza un turno para el envío de datos.

Teóricamente, este protocolo determinístico incrementa el ancho de banda disponible al eliminar las colisiones y las retransmisiones.

2.4.1 Creación de las tramas

Aunque 100VG admite los formatos de trama de los protocolos 802.3 y 802.5 existentes (pero no ambos simultáneamente), su protocolo no se parece a ninguno de ellos. El estándar 802.12 sugerido para la transmisión de 100 Mbps sobre cable de par trenzado sin malla (grado voz), representa una variación.

Una de las diferencias claves entre los estándares 802.3 y 802.12 que es también una de las ventajas fundamentales de este último; es su capacidad de reconocer dos niveles de prioridad en las solicitudes de transmisión: normal y alta. El nivel de prioridad lo puede establecer la estación de trabajo o la aplicación, si una solicitud de prioridad normal está pendiente durante más de 300 ms, se traslada a la cola de servicio de prioridad alta.

El DPA hace algo más que permitir que se establezca la prioridad de la transmisión. También mejora el rendimiento eliminando los datos no útiles de la red asociada con el método de acceso CSMA/CD. Además la red con DPA, que no tiene contienda para la transmisión y que por ello no presenta colisiones de paquete, es capaz de manejar más tráfico.100VG-AnyLAN también tiene algo de ventaja en cuanto a seguridad ya que el concentrador sólo transmite paquetes a través de puertos conectados a la dirección de destino del paquete. Esto reduce la posibilidad de una supervisión no autorizada de las transmisiones.

2.4.2 La arquitectura de 100VG

La topología de 100VG-AnyLAN debe ser una estrella física, sin ciclos ni ramificaciones. La pieza central de esta topología es un concentrador, llamado *concentrador raíz*, que controla el tráfico. Cada concentrador de menor nivel mantiene su propia tabla de direcciones de puerto, que contiene las direcciones de las estaciones conectadas a cada uno de sus puertos. Cuando una estación o computadora envía una solicitud de transmisión, ésta es recibida primero por el concentrador al que está conectada directamente. Si éste concentrador es el único de la red, será el concentrador raíz y por lo tanto el controlador central de la transmisión de red. Sin embargo, si el concentrador que está conectado directamente no es el raíz, enviará la

solicitud de la estación al siguiente concentrador de mayor nivel, que a su vez transferirá la solicitud de no ser el concentrador raíz. Finalmente, la solicitud de transmisión llega al concentrador raíz, quién dará permiso al concentrador local para servir la solicitud cuando llegue su turno.

Una red 100VG-AnyLAN funciona de manera parecida a un "round-robin" (turnos alternativos en rotación), porque se sondea a cada concentrador secuencialmente, y cada concentrador a su vez sondea a cada uno de sus puertos del mismo modo. El proceso es el siguiente: entre las transmisiones de los paquetes, las estaciones y concentradores se envían una señal entre sí para indicar que el canal está disponible para realizar una solicitud de transmisión. A esta señal se le llama *señal de estado libre*. Cuando una estación tiene que transmitir un paquete, envía una *señal de solicitud de transmisión* al concentrador que incluye la prioridad de la solicitud, y espera entonces el permiso del concentrador raíz para transmitir un paquete en la red.

El concentrador raíz controla todas las transmisiones de datos, determina qué concentrador de nivel inferior puede comenzar a dar servicio a las solicitudes de transmisión. Cuando el derecho a dar servicio a las solicitudes llega a un concentrador, concede el servicio siguiendo el orden de puerto (por ejemplo, puerto 1, luego el 2 y así hasta el puerto N), y después pasa el control de nuevo al concentrador de nivel superior. Las solicitudes de transmisión de prioridad alta que se producen en cualquier lugar de la red siempre toman la precedencia, y el concentrador raíz siempre permite que el concentrador local que ha recibido la solicitud conceda el servicio, y devuelva el control al concentrador que tenía el turno.

La figura 2.10 muestra la gestión de acceso con prioridad por demanda a las solicitudes de transmisión:

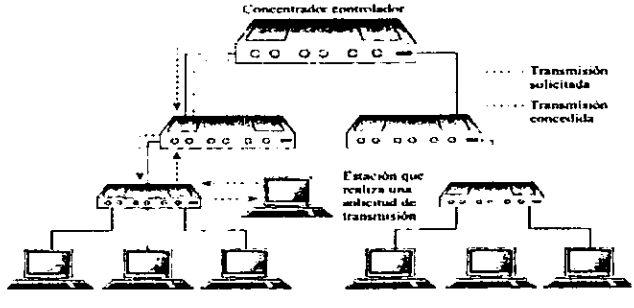


Figura 2.10

Cuando una estación o concentrador desea unirse a la red, transmite y recibe tramas a través del puerto conectado. A esto se le llama una *secuencia de tramas de aprendizaje*. Esta secuencia ayuda al concentrador a determinar si el nuevo dispositivo es una estación u otro concentrador, el tipo de trama que utiliza (802.3 u 802.5) y si se va a permitir al puerto funcionar como oyente promiscuo. Si el dispositivo que se conecta, es una estación, también determina su dirección MAC. Mientras se produce el aprendizaje, la red suspende sus operaciones de sondeo que equivale a 5 µs aproximadamente. Basándose en los resultados de la secuencia, el concentrador

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

permite que el nuevo dispositivo se una a la red o le niega el acceso. En este último caso, transmite la razón por la que no será admitido.

2.4.3 Aspectos de cableado

Las reglas de cableado para 100VG-AnyLAN son muy similares a 10BASE-T. En el estándar 802.12, los cuatro pares de cables transmiten y reciben datos, permitiendo que cada par funcione a una velocidad de señal de 25 MHz (radiofrecuencias dentro de los valores normalizados) con la utilización de cable para voz (categoría 3). Utilizando cableado de 4 pares, esta señal permite enviar y recibir datos simultáneamente.

100VG-AnyLAN admite cable UTP de categoría 3, 4 ó 5, cable STP de tipo 1 y cable de fibra óptica. Dependiendo del tipo de cable, el alcance de la red varía desde 100 metros a 2000 metros. Cabe señalarse que 100VG-AnyLAN no admite cable plano en una topología de par trenzado.

2.4.4 Aspectos del concentrador

En una red 100VG-AnyLAN, el número máximo de niveles de concentrador es cinco. Sin embargo, el rendimiento de la red será mejor si no hay más de tres niveles. La tabla siguiente muestra la distancia máxima que puede haber entre el concentrador raíz y un nodo de extremo:

Tipo de medio	No. de concentradores entre el concentrador raíz y un nodo extremo	No. de niveles en la red	Distancias máximas recomendadas entre el concentrador raíz y el nodo extremo
Categoría 3	1	2	100m
Categoría 3	2	3	75m
Categoría 3	3	4	50m
Categoría 3	4	5	25m
Categoría 5	1	2	200m
Categoría 5	2	3	150m
Categoría 5	3	4	100m
Categoría 5	4	5	50m
Fibra óptica	1	2	4km
Fibra óptica	2	3	3km
Fibra óptica	3	4	2km

Cabe considerar, que no se deben tener más de 7 puentes o conmutadores (switches) entre dos nodos cualesquiera de una red. Esto es una consecuencia del protocolo de expansión de árboles 802.1 (Spanning tree) del IEEE, no una limitación de 100 VG-AnyLAN.

2.4.5 Preparativos para cambiar a 100VG-AnyLAN

Hay que tener presente, que la ausencia de competitividad en este mercado no sólo limita potencialmente el disponer de un consejo técnico, sino que también mantiene los precios más altos que para otros protocolos mejor establecidos.

En primer lugar es muy recomendable inspeccionar la planta de cables antes de implementar 100VG-AnyLAN, eliminando con cuidado los cables de 25 pares conectados a los dispositivos que funcionan en modo promiscuo (en el cual el dispositivo supervisa todas las tramas que recibe). En segundo lugar, tendrá que comprobarse que la distancia entre los concentradores no exceda las especificaciones de 100VG-AnyLAN.

Facilidad de ampliación

El esquema de acceso con prioridad por demanda determinístico hace que 100VG-AnyLAN sea fácil de ampliar con una pequeña pérdida en el rendimiento. La mayoría de los problemas en la ampliación es que requiere un puente de traducción entre sí mismo y 10BASE-T. Y, aunque no hay limitaciones en el número de nodos de una 100VG-AnyLAN de compartición única, es una buena idea el limitar el número de nodos a 250 para mantener el rendimiento.

El alcance de red máximo para éstas redes varia de 100 m a 2000 m, dependiendo del medio utilizado. Además de poder poner en cascada hasta 5 concentradores, admite 4 saltos de repetidor en cada segmento de red (igual que Ethernet). Los problemas de cableado se deben principalmente a que cada nivel de concentradores acorta la distancia máxima permitida entre un concentrador raiz y un nodo extremo. Por ejemplo, cuando se utiliza cableado de fibra óptica, cada nivel de concentradores acorta la distancia máxima en 1 km. Así, en una cascada de 3 concentradores que utiliza cableado de fibra, la distancia máxima permitida es de 3 Km.

En el momento de escribir estas líneas, no se disponía de dispositivos de conmutación para el protocolo 100VG-AnyLAN, ni estaban anunciados, aunque entendemos que en el futuro se implementarán y mejorará su facilidad de ampliación.

Facilidad de administración

Dado que 100VG-AnyLAN admite tipos de paquete Ethernet estándar, no existen problemas de operación conjunta. Sin embargo, no tiene actualmente herramientas de administración que ayuden en la asignación y gestión del ancho de banda.

Actualmente, la única seguridad ofrecida es el funcionamiento en modo privado descrito anteriormente, que, cuando está activado, permite que los puertos reciban solamente los paquetes dirigidos al dispositivo conectado a ellos. Todos los puertos que no estén asociados con la dirección de destino reciben una señal de estado libre mientras se transmite el paquete. Aunque este nivel de seguridad es suficiente en la mayoría de las instalaciones, puede que no lo sea para ubicaciones de alta seguridad.

Rendimiento

El rendimiento es el punto fuerte de 100VG-AnyLAN. Gracias a que puede manejar tamaños de paquete de 4500 ó 1500 bytes, puede admitir los tamaños actuales de paquete medio, más pequeño y mantener un rendimiento rápido y eficiente.

La potencia real de 100VG-AnyLAN destaca cuando se ejecutan aplicaciones de multimedia. Incluso el video de movimiento completo se ejecuta bajo una carga de tráfico alta sin un parpadeo, gracias al esquema de DPA que asigna una prioridad alta a todas las tramas de video. Además, Hewlett Packard ha afirmado que tienen planes de añadirle capacidad dúplex, lo que incrementará el rendimiento aún más.

En resumen podemos decir que el esquema de DPA hace que 100VG-AnyLAN sea un protocolo robusto especialmente para aplicaciones de multimedia y video. Sin embargo, la ausencia de tolerancia a fallas y la carencia de software de administración lo hace menos adecuado para su soporte. Finalmente, dado que no cumple completamente las reglas de cableado 10BASE-T, hay que tener mucho cuidado a la hora de realizar una implementación a gran escala.

Recomendado para:

- Aplicaciones de multimedia y video por su capacidad de dar prioridad y asegurar la entrega de paquetes.
- Base instalada que no incluya cable de 25 pares y que cumpla las especificaciones de 100VG-AnyLAN.
- Grupos de trabajo avanzados, porque su esquema de acceso a datos determinístico asegurará un rendimiento consistente bajo tráfico elevado.

Ventajas:

- Bajo precio de los componentes.
- Puede dar prioridad a los paquetes.

Desventajas:

- Seguridad limitada.
- Número de vendedores limitado, aunque creciente.
- Se requiere una preparación considerable antes de implementarlo en una red 10BASE-T heredada.

2.5 GIGABIT ETHERNET

Entre las tecnologías LAN de alta velocidad disponibles hoy en día, 100BASE-T se ha puesto a la cabeza. Sin embargo, el creciente uso de conexiones 100BASE-T para servidores y equipos de escritorio, está creando una necesidad clara de tener una tecnología de red de más alta velocidad en el backbone y mejor nivel de servidor. Idealmente, ésta tecnología debe también proveer un mecanismo de actualización, un costo accesible y no requerir de grandes reestructuraciones en el esquema de red.

La solución más apropiada, ahora en desarrollo, es Gigabit Ethernet. Ésta proveerá ancho de banda de 1 Gbps para redes de área local y amplia, con la simplicidad de Ethernet a menor costo que otras tecnologías de velocidad comparable. También ofrecerá una ruta sencilla de migración para las instalaciones Ethernet actuales,

reforzando equipos finales existentes, manejando herramientas de administración y seguridad y proporcionando nuevas tecnologías de transmisión.

Gigabit Ethernet emplea el mismo protocolo (CSMA/CD), mismo formato de trama y mismo tamaño que sus predecesores Ethernet. Para la vasta mayoría de usuarios de red, esto significa que sus inversiones de red existentes pueden ser extendidas a velocidades gigabit a un costo inicial razonable sin la necesidad de capacitar a sus usuarios y grupos de soporte, ni de invertir en equipo de acoplamiento entre tecnologías.

Por todos estos atributos, además de soportar operaciones full dúplex, Gigabit Ethernet será una tecnología de interconexión de backbone ideal para usarse entre switches 10/100BASE-T así como, en conexiones para servidores de alto desempeño. Combinada con la escalabilidad y flexibilidad para manejar nuevas aplicaciones y tipos de datos, Gigabit Ethernet es la elección estratégica para redes que requieran de gran ancho de banda y de alta velocidad.

2.5.1 El surgimiento del estándar Gigabit Ethernet IEEE 802.3z

En Julio de 1996, el grupo de trabajo de IEEE 802.3 creó el equipo de trabajo de Gigabit Ethernet 802.3z. Los objetivos claves de éste fueron desarrollar un estándar que cumpliera con lo siguiente:

- Permitir operación half y full dúplex a velocidades de 1000 Mbps
- Usar el formato de trama Ethernet 802.3
- Usar el método CSMA/CD y soportar a un repetidor por dominio de colisión
- Mantener la compatibilidad con tecnologías 10BASE-T y 100BASE-T

También se identificaron tres objetivos específicos para distancias por tipo de enlace: un enlace de fibra óptica multimodo con una longitud máxima de 550 metros; un enlace de fibra óptica monomodo con una longitud máxima de 3 kilómetros; y un enlace basado en cobre con una longitud máxima de al menos 25 metros. El IEEE está actualmente investigando la tecnología que pudiera soportar enlaces con distancias de al menos 100 metros sobre cableado par trenzado sin blindar categoría 5. En resumen, el equipo de trabajo ha decidido incluir una especificación opcional para una Interfaz Independiente al Medio de Gigabit (GMII) en el plan de ésta nueva tecnología de red.

Se espera que el estándar Gigabit Ethernet esté completo mucho más rápido que otras alternativas de red de alta velocidad. El objetivo del grupo de Gigabit Ethernet es completar el estándar en 1998, aunque productos pre-estándar aparecieron antes (1997).

2.5.2 Arquitectura del protocolo Gigabit Ethernet

Se necesitaron muchos cambios para acelerar la velocidad de 100 Mbps a 1 Gbps, que se hicieron en la interfaz física. Los desafíos involucrados, se han resuelto uniendo dos tecnologías: IEEE 802.3 Ethernet y Canal de Fibra ANSI X3T11 (Fiber Channel).

La figura 2.11 muestra como los componentes claves de cada una de dichas tecnologías, han sido considerados para formar Gigabit Ethernet.

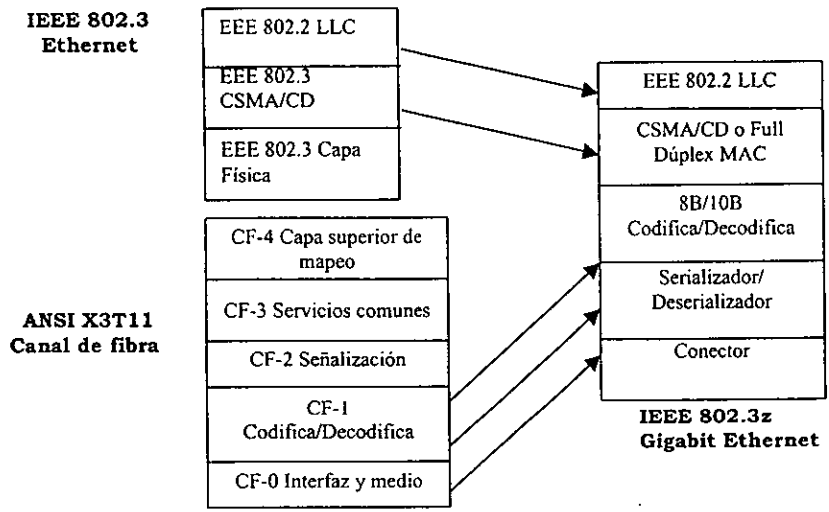


Figura 2.11

Esto significa, que el estándar puede tomar ventaja de la tecnología de interfaz física de alta velocidad del canal de fibra mientras mantenga el formato de trama IEEE 802.3, la compatibilidad y el uso de full o half dúplex (vía CSMA/CD).

El actual modelo de Gigabit Ethernet se muestra en la figura 2.12.

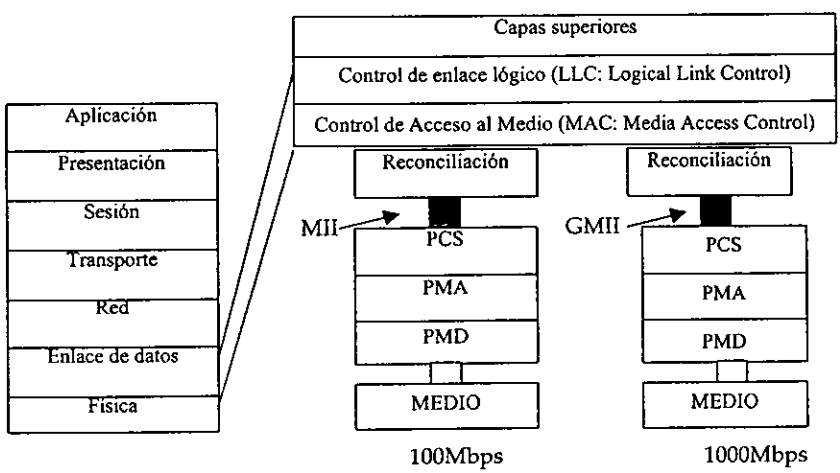


Figura 2.12

A continuación se describirán cada una de las capas del modelo Gigabit Ethernet mostrado.

Interfaz Física

La especificación de Gigabit Ethernet inicialmente usará tres medios de transmisión: láser de onda larga (LW) sobre fibra multimodo y monomodo (conocida como 1000BASE-LX) y láser de onda corta (SW) sobre fibra multimodo (conocida como 1000BASE-SX). El medio de 1000BASE-CX permite transmisión sobre cable de cobre blindado 150 ohms. El comité IEEE 802.3ab está examinando el uso de cable par trenzado sin blindar (UTP) para transmisión Gigabit Ethernet (1000BaseT); éste estándar es esperado para 1999.

La especificación dependiente al medio físico (PMD) del canal de fibra actualmente admite señalización de 1.062 gigabaudios en full dúplex. Gigabit Ethernet incrementará este rango de señalización a 1.25 Gbps. La codificación 8B/10B (que discutiremos después) permite un rango de transmisión de 1000 Mbps. El tipo de conector actual para el canal de fibra, y por lo tanto para Gigabit Ethernet, es el conector SC para ambas fibras (monomodo y multimodo).

Láseres de onda larga y de onda corta sobre medio de fibra óptica

Se soportan dos estándares de láser sobre fibra: 1000BASE-SX (de onda corta, para backbone y horizontal) y 1000BASE-LX (de onda larga, para backbones multimodo y área amplia en monomodo). Ambos lásers pueden trabajar sobre fibra multimodo, en cualquiera de sus dos tipos disponibles: de 62.5 y de 50 mm de diámetro. La fibra monomodo, incluida por el estándar de longitud de onda larga, se define para cubrir distancias de 3 kilómetros.

Las diferencias claves entre el uso de tecnologías de láser de onda corta y de onda larga es el costo y la distancia. Los lásers sobre cable fibra óptica toman ventaja de las variaciones en la atenuación. En longitudes de onda diferentes, se encontrarán disminuciones o "dips" en atenuación sobre el cable, que los lásers aprovechan para transmitir a diferentes longitudes de onda. Los lásers de onda corta están ya disponibles en la tecnología de discos compactos. Los lásers de onda larga convierten las disminuciones de atenuación en transmisiones con longitudes de onda más largas a través del medio. La consecuencia de esto es que lásers de onda corta serán más baratos, pero soportarán una distancia más corta. En contraste, los rayos láser de onda larga serán más caros pero soportarán distancias de transmisión más grandes.

La fibra monomodo ha sido usada tradicionalmente en cableado de redes para alcanzar distancias largas. Esta fibra, usando un núcleo de 9 micras y un láser de 1300 nanómetros en su longitud de onda, alcanza la transmisión más larga equivalente a varios kilómetros. Su núcleo pequeño y el láser de energía baja alargan la longitud de onda del láser y permiten distancias más largas

La fibra de 62.5 mm se usa generalmente en cableado vertical y ha sido usada también para backbone de Ethernet, Fast Ethernet y FDDI. Este tipo de fibra, sin embargo, tiene un ancho de banda más bajo (habilidad del cable para transmitir luz), especialmente con lásers de onda corta. Esto significa que lásers de onda corta sobre

62.5 micrometros transmitirán a distancias más cortas que los lásers de onda larga. La fibra de 50 micras tiene mejores características de banda ancha y transmitirá a mayor distancia con lásers de onda corta.

Cable de cobre blindado balanceado de 150 Ohms (1000BaseCX)

Éste es un nuevo tipo de cable blindado; que no es UTP. Para minimizar la inseguridad e interferencia causada por diferencias de voltajes, ambos transmisores y receptores compartirán una tierra en común. La pérdida de señal para cada conector está limitada a 20 dB para minimizar las distorsiones de transmisión. El tipo de conector para 1000BASE-CX será un conector DB-9. Se está desarrollando un nuevo conector por AMP llamado el HSSDC, el cual será incluido en la siguiente revisión del proyecto.

La aplicación principal para este tipo de cableado serán conexiones inter o intra rack. Ya que tiene la distancia limitada a 25 metros, y no trabajará en closets de columna que requieran una distancia mayor entre los equipos terminales.

Existen dos estándares para transmisión Gigabit Ethernet sobre cableado de cobre. El primero está definido por el 802.3z y es referido como 1000BASE-CX. Este estándar soporta interconexión de equipo donde la interfaz física es cobre de corto alcance (25 metros de distancia). Así mismo, el estándar usa el código 8B/10B de canal basado en fibra (periodo de línea serial de 1.25 Gbps), y corre sobre cable "twinax". Tiene la ventaja de que puede ser generado rápidamente y su costo de implementación es bajo. El segundo estándar de enlace de cobre está pensado para usarse en aplicaciones de cableado horizontal.

En marzo de 1997, se aprobó la creación de un Comité, referido como el cuerpo de tarea 802.3ab. Este nuevo grupo está enfocado al desarrollo de un estándar de capa física de 1000BASE-T para la transmisión de señal Ethernet de 1 Gbps sobre cuatro pares de cable UTP categoría 5, cubriendo distancias arriba de los 100 metros o redes con un diámetro de 200 metros. Este estándar introducirá el cableado de cobre horizontal que corre por el piso de un edificio basado en el estándar genérico de cableado estructurado, esto permitirá usar el cableado UTP ya existente. Esta obra, sin embargo, requerirá nueva tecnología y nuevo esquema de código para encontrar los parámetros establecidos y demandados por los estándares previos, Ethernet y Fast Ethernet. Esta situación llevará más tiempo que el requerido para el estándar 802.3z.

Seriador/Deseriador (serializer/deserializer)

El seriador/deseriador es el responsable de soportar esquemas de codificación múltiple y permitir presentación de estos esquemas a las capas superiores. Los datos introducidos a la subcapa física (PHY) entrarán a través de la PMD y necesitarán ser soportados por el esquema de codificación adecuado a ese medio. El esquema de codificación para el canal de fibra es 8B/10B, diseñado especialmente para transmisión por fibra óptica. La diferencia entre el canal de fibra y Gigabit Ethernet, es que el canal de fibra utiliza una señalización de 1.25 gigabaudios.

Para decodificación de una transmisión sobre UTP, se requiere un esquema de decodificación específico. Esta decodificación será desarrollada por la PHY de UTP o 1000Base-T.

Codificación 8B/10B

La capa FC-1 del canal de fibra describe la sincronización y el esquema de decodificación. FC-1 define el protocolo de transmisión, incluyendo codificación y decodificación serial de y para la capa física, caracteres especiales y control de errores. Gigabit Ethernet utilizará la misma codificación/decodificación especificada por esta capa. Este esquema es similar a la codificación 4B/5B usada en FDDI; sin embargo, la codificación 4B/5B fue rechazada por el canal de fibra por su falta de balance, que puede resultar en calentamiento dependiente de los datos, debido a un transmisor que envía más "unos" que "ceros", provocando periodos de error más altos. La codificación de datos a altas velocidades provee algunas ventajas que han sido añadidas a FC-1, como son:

- Incrementa la posibilidad de que la estación receptora pueda detectar y corregir errores de transmisión o recepción.
- La codificación puede ayudar a distinguir bits de datos de los bits de control.

En Gigabit Ethernet, la capa FC-1 toma datos decodificados tanto de la capa FC-2 como de la subcapa de reconciliación (RS), estos datos "recorren" la interfaz física del canal de fibra hacia las capas superiores de Ethernet (IEEE 802.3). La codificación toma lugar al realizarse un mapeo de caracteres de 8 bits a 10 bits. Los datos decodificados constan de 8 bits con una variable de control, que en su momento, serán codificados en un carácter de transmisión de 10 bits (similar a lo hecho en FDDI).

La codificación se realiza proveyendo a cada carácter de transmisión con un nombre denotado como *Zxx.y*. La *Z* es la variable de control que puede tomar dos valores: *D* para Datos y *K* para carácter especial. La designación *xx* es el valor decimal del número binario compuesto de un subconjunto de los bits decodificados. La designación *y* es el valor decimal del número binario del resto de los bits decodificados. Esto implica que hay 256 posibilidades de Datos y 256 para caracteres especiales, aunque solo 12 valores *Kxx.y* son válidos en el canal de fibra. Cuando los datos son recibidos, el carácter de transmisión es decodificado en una de estas combinaciones de 8 bits.

Capa MAC

La capa MAC de Gigabit Ethernet es similar a la del estándar Ethernet. Esta capa soportará ambas transmisiones full y half dúplex. Las características de Ethernet, tales como detección de colisión, diámetro de red máximo y reglas de repetidor, serán las mismas para Gigabit Ethernet. El soporte para half dúplex añade "desencadenamiento" de trama y extensión de portadora, funciones que no se encuentran en Ethernet y Fast Ethernet.

Transmisión half dúplex

Para la transmisión half dúplex, se utilizará el método de acceso CSMA/CD para asegurar que las estaciones puedan comunicarse sobre un cable simple y que tenga lugar la recuperación de la colisión. La implementación de CSMA/CD permitirá la creación de hubs Gigabit Ethernet compartidos o conexiones punto a punto half dúplex.

La limitación actual de Gigabit Ethernet es de 50 metros máximo para cableado de cobre entre estaciones con un repetidor en medio. La meta del comité de estándares es incrementar esto a 200 metros. La operación en modo half dúplex de fibra óptica tiene un máximo de 2000 metros. Gigabit Ethernet también usa cableado UTP categoría 5.

La transición en las velocidades de transmisión de Ethernet a Gigabit han incrementado los retos, en términos de la implementación de CSMA/CD. Ya que a velocidades más grandes que 100 Mbps, los tamaños de los paquetes mínimos serán más pequeños que la longitud del slot time (en bits). El **Slot time** esta definido como la unidad de tiempo por MAC de Ethernet para colisiones manejables. Esta situación, provocaría que en el caso en que dos o más computadoras conectadas a la red enviarán su paquete mínimo al mismo tiempo, y puesto que el tiempo de detección de las colisiones (slot time), es mayor al paquete en cuestión, entonces las colisiones no serían detectadas ni resueltas. Para remediar el problema del slot time, se agregan bits a la trama hasta que ésta satisfaga el slot time mínimo requerido (extensión de portadora). De esta manera, los tamaños de paquetes más pequeños pueden coincidir con el slot time mínimo y permitir la operación sin modificar el actual CSMA/CD de Ethernet.

Otro cambio para la especificación de Ethernet es la adición de "desencadenamiento" de trama. Ésta es una característica opcional en la cual, en un ambiente CSMA/CD, una estación final puede transmitir una ráfaga de tramas sobre el canal de comunicación sin tener que soltar el control. Otras estaciones en el canal aplazan la transmisión ráfaga hasta que la primera que lo utilizó lo desocupe. De esta manera la estación que está desencadenando en el canal, llenará el intervalo intertrama con bits de extensión, haciendo que el canal no se encuentre libre para cualquier otra estación final hasta que deje de utilizarlo.

Es importante señalar que los problemas de Gigabit Ethernet para la transmisión en modo half dúplex, tal como la ineficacia del tamaño de la trama (la cual maneja la necesidad de extensión de portadora) así como el tiempo de round trip (viaje redondo) de la señal en velocidades gigabit, indican que, half dúplex no es efectiva para Gigabit Ethernet.

IEEE 802.3x Transmisión full dúplex

Full dúplex provee transmisión y recepción simultáneamente en un cable simple. Se usa entre dos puntos finales, como entre switches, switches a servidores, switches a ruteadores, etc.

La transmisión full dúplex se utilizará en Gigabit Ethernet para incrementar el ancho de banda agregado de 1 Gbps a 2 Gbps para ligas punto a punto, así como para incrementar las distancias posibles para el medio particular. El uso de Ethernet full dúplex elimina colisiones en el cable; por lo tanto, CSMA/CD no necesita utilizarse como un control de flujo o acceso al medio. El estándar es llamado como IEEE 802.3x. Este estándar formaliza tecnología full dúplex y se espera que sea soportado por productos Gigabit Ethernet.

Control de flujo 802.3x opcional

Este mecanismo de control de flujo opcional, se establece entre dos estaciones en el enlace punto a punto. Si la estación que recibe al final llega a ser congestionada, ésta puede devolver una trama llamada "trama de pausa" al origen en el final opuesto de la conexión, que ordena que la estación detenga el envío de paquetes en un periodo de tiempo específico. La estación que envía esperará el tiempo requerido antes de enviar más datos. La estación que recibe puede también enviar una trama "back" con un tiempo de espera de cero y ordenar al origen para comenzar a enviar datos otra vez.

Capa de enlace lógico

Gigabit Ethernet ha sido diseñado para adherirse al formato de trama Ethernet estándar, la cual mantiene compatibilidad con la base instalada de productos Ethernet y Fast Ethernet y no requiere traducción de la trama.

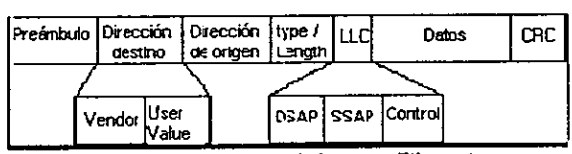


Figura 2.13. Formato de la trama Ethernet

La especificación original identifica un campo TIPO (Type), el cual se utiliza para la identificación del protocolo. La especificación IEEE 802.3x eliminó este campo, remplazándolo con el campo LONGITUD (Length), el cual se usa para la longitud en bytes del campo de datos. El tipo de protocolo en tramas 802.3x se especifica en la porción de datos del paquete. La LLC es responsable de proveer servicios a la capa de red a pesar del tipo de medio: FDDI, Ethernet, Token Ring u otro.

Para comunicarse entre la capa MAC y las capas superiores del stack de protocolo, la capa de LLC, hace uso de 3 variables diferentes para determinar el acceso a las capas superiores vía el LLC-PDU. Estas variables son el DSAP (Destination Service Access Point), SSAP (Source Service Access Point), y variable de control.

Portadora de interfaz Gigabit Ethernet (GBIC: Gigabit Ethernet Interface Carrier)

La interfaz GBIC permite configurar cada puerto gigabit de la red para trabajar con lásers de onda corta y onda larga, así como para interfaces físicas de cobre. Como estado inicial, Gigabit Ethernet soporta tres medios claves: láser de onda corta, láser de onda larga, y cobre corto.

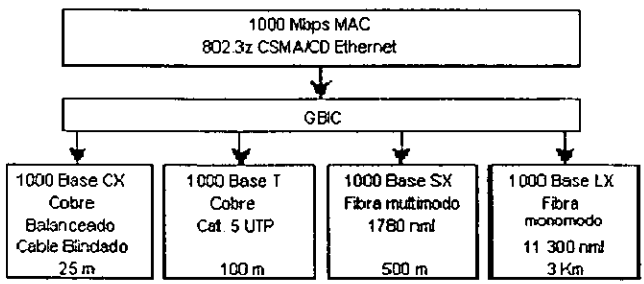


Figura 2.14

En contraste, los switches de Gigabit Ethernet sin GBICs no pueden soportar otros lásers que no sean de onda corta. Cabe notar que el comité del IEEE 802.3z provee la única especificación GBIC.

2.5.3 Productos de Gigabit Ethernet

Ya que Gigabit Ethernet es una mejora de Ethernet, los tipos de productos de Gigabit Ethernet serán completamente abiertos: switches, módulos uplink/downlink, NICs (Network Interface Card), interfaces de ruteo Gigabit Ethernet, y un nuevo dispositivo, los distribuidores bufeados (*buffered distributors*), éstos serán solo switches multipuertos Gigabit Ethernet con "backplanes" de alto desempeño, así como dispositivos que tienen ambos puertos Gigabit Ethernet y Fast Ethernet en la misma caja.

El distribuidor "buffered" es un dispositivo full dúplex, multipuerto, similar a un hub que interconecta dos o más enlaces 802.3 operando a 1 Gbps o más rápido. Al igual que un repetidor 802.3, éste dispositivo no filtra direcciones. El distribuidor envía (forwards) de todos los paquetes entrantes a todos los enlaces conectados excepto al original, proveyendo un dominio de banda ancha compartido, comparable al dominio de colisión 802.3. A diferencia de un repetidor 802.3, el distribuidor permite "bufear" (almacenar) una o más tramas entrantes en cada enlace antes de enviarlas.

Como un dispositivo de banda ancha compartido, el distribuidor debe ser distinguido de ruteadores y switches. Mientras los ruteadores con interfaces Gigabit Ethernet pueden tener backplanes que soporten ancho de banda mayores o menores a los periodos de 1 gigabit, los puertos unidos a un backplane del distribuidor "buffered" comparten 1gigabit de banda ancha. En contraste, los backplanes de switches Gigabit Ethernet multipuertos de alto desempeño, soportarán bandas anchas multigigabit.

2.5.4 Ethernet y los servicios de nivel más alto

Gigabit Ethernet provee conectividad a alta velocidad, pero no provee por sí mismo un conjunto completo de servicios tales como: Calidad de Servicios (QoS: Quality of Service), y servicios de ruteo a niveles más altos; estos servicios serán agregados vía otros estándares abiertos. Gigabit Ethernet, como todas las especificaciones Ethernet, trata el enlace de datos (capa 2) del modelo OSI, mientras TCP e IP especifican el transporte (capa 4) y la red (capa 3) respectivamente, permitiendo realizar comunicación entre aplicaciones. Cuestiones como QoS no fueron tratadas en las especificaciones originales de Gigabit Ethernet, pero deben ser tratadas a través de otros estándares. RSVP (Resource Reservation Protocol), por ejemplo, está definido en la capa de red para trabajar al lado de IP.

Varias implementaciones de Gigabit Ethernet pueden incluir uno o más de estos estándares para proveer una conexión funcional o más robusta, sin que el éxito total de Gigabit Ethernet esté sujeto a cualquiera de ellos. La ventaja de un estándar modular es que cualquier pieza puede evolucionar y ser adaptada a un ritmo determinado por la necesidad del mercado y calidad de producto.

Calidad de servicio en Ethernet. Las aplicaciones que han surgido a mediados de los 90's demandan ancho de banda consistente principalmente. Tales aplicaciones incluyen voz y video sobre LANs y WANs, distribución de software multicast y todo lo referido a éstos. Los cuerpos de los estándares han respondido con nuevas definiciones abiertas tales como RSVP y el actual trabajo en los grupos de los estándares IEEE 802.1p e IEEE 802.1Q.

RSVP está logrando aceptación en la industria, como un camino para solicitar y proveer calidad de conexiones de red. Dispuestos a tener función RSVP y entregar calidad consistente y definida en una aplicación, cada componente de red en la cadena entre el cliente y el servidor deben soportan RSVP y comunicarse apropiadamente.

802.1p y 802.1Q facilitan calidad de servicio sobre Ethernet proporcionando un medio para paquetes "tagging" (etiquetados) con una indicación de la prioridad o clase del servicio deseado para el paquete. Estas etiquetas permiten a las aplicaciones comunicar la prioridad de los paquetes a través de los dispositivos inter-red. El soporte RSVP puede ser realizado por mapeo de sesiones dentro de clases de servicio 802.1p.

Funcionalidad de la capa 3. Esta capa involucra la dirección destino MAC en el encabezado del paquete y por revisión de la dirección IP (escondida en el paquete), la subred IP puede ser determinada (realizando broadcasts), de ésta manera los paquetes pueden ser enviados directa y exactamente a los nodos intermedios de la red, lográndose así mayor eficiencia del tránsito a través de la misma.

El dispositivo clásico de la capa 3 es el ruteador, el cuál toma decisiones sobre la capa por medio de la implementación de algoritmos complejos y estructuras de datos en software. Los vendedores en éste último año han anunciado productos "IP switch" que realizan muchas de las tareas del ruteo, mejores en funcionamiento/precio que los ruteadores tradicionales. Limitar el protocolo soportado a IP ha permitido a los dispositivos optimizar tareas y realizar más trabajo con hardware dedicado.

2.5.5 Distancia máxima en la red de acuerdo a la topología Ethernet utilizada

Todas las topologías Ethernet tienen limitaciones en la longitud del segmento. La siguiente tabla muestra una comparación entre las restricciones de distancia para topologías Ethernet y Gigabit Ethernet actuales, hechas por el grupo de estándares IEEE 802.3z

	Ethernet 10 BASE T	**Fast Ethernet 100 BASE T**	**Gigabit Ethernet 1000 BASE X**
Rango de datos	10 Mbps	100 Mbps	1000 Base X (1 gigabit/segundo)
UTP categoría 5	100 m (min.)	100 m	100 m
STP/Coaxial	500 m	100 m	25 m
Fibra multimodo	2 km	412 m (half dúplex) 2 km (full dúplex)	500 m
Fibra monomodo	25 km	20 km	3 km

2.5.6 Ultimos resultados del trabajo 802.3z

Por último y basados en el trabajo realizado en el encuentro plenario de 802.3z del mes de febrero de 1998, en California, diremos que, el documento del proyecto Gigabit Ethernet está completo y el estándar va rumbo a la ratificación formal en junio de este año. Los comentarios técnicos y editoriales fueron resueltos, incluyendo la única cuestión de fibra óptica significativa que permaneció fuera de lo común: retraso de modo diferencial (DMD: Differential Mode Delay). A continuación mencionamos otros resultados que se han considerado y que es lo último de lo que se tiene documentado.

- La distancia de enlace para fibra monomodo de 1000BASE-LX se incremento de 3,000 metros a 5,000 metros.

- Se completó una solución para reducir los efectos de jitter causados por el DMD. Para 1000BASE-SX, la solución fue eliminar el transmisor de láser, introduciendo pruebas para sensibilidad y jitter de recepción. En resumen, la distancia de enlace para fibra multimodo de ancho de banda más bajo fue recortada.

- La distancia de 1000BASE-LX está especificada como 550 metros para todos los tamaños de fibra multimodo y grados intervenidos en el proyecto 4.2 de 802.3z.

- 802.3z ahora incluye especificaciones de distancias para dos diferentes valores de ancho de banda de fibra multimodo de 62.5 micras: estándar TIA (160/500 MHz/km) y estándar ISO/IEC (200/500 MHz/km).

- 802.3z ahora incluye especificaciones de distancias para dos diferentes valores de ancho de banda de fibra multimodo de 50 micras: 500/500 MHz/km como los especificados en canal de fibra y 400/400 MHz/km.

Relación de distancias confirmadas y establecidas en la reunión

Estándar (metros)	Tipo de fibra	Diámetro (micras)	Ancho de Banda modal (MHz*km)	Rango mínimo
1000BASE-SX	MM	62.5	160	2 a 220*
"	"	"	200	2 a 275**
"	"	50	400	2 a 500
"	"	"	500	2 a 550***
1000BASE-LX	"	62.5	500	2 a 550
"	"	50	400	2 a 550
"	"	50	500	2 a 500
"	SM	9	NA	2 a 5000

Notas:
* El estándar de cableado de edificios de TIA 568 especifica fibra multimodo 160/500 MHz*km.
** El estándar de cableado de edificios de ISO/IEC 11801 internacional especifica fibra multimodo 200/500 MHz*km.
*** La especificación de canal de fibra ANSI especifica fibra multimodo de 50 micras 500/500 MHz*km y fibra 500/500 MHz*km ha sido propuesta en adición a ISO/IEC 11801.

2.6 MODO DE TRANSFERENCIA ASÍNCRONO (ATM)

El ATM empezó como parte del estándar de la Red Digital de Servicios Integrados de Banda ancha (RDSI-B), desarrollado en 1988 por el Comité Consultivo Internacional para Telegrafía y Telefonía (CCITT). La RDSI-B, una extensión de la red digital de banda estrecha (que define las redes públicas de telecomunicaciones digitales), proporciona más ancho de banda y permite un flujo de datos superior al de la RDSI de banda estrecha. La figura 2.15 muestra el modelo de referencia de la RDSI-B.

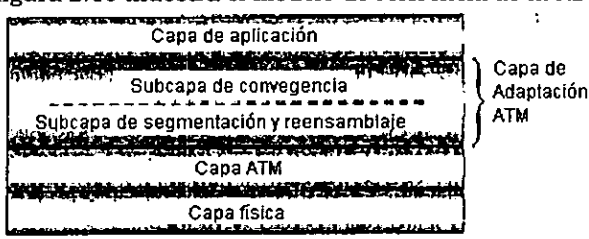


Figura 2.15. Modelo de referencia de la RDSI-B

Como puede verse, ATM queda justo encima de la capa física en el modelo. Sin embargo, no necesita hacer uso de ningún protocolo específico de la capa física. Así, la capa física podría ser FDDI, DS3, SONET o cualquier otro.

Como ya se dijo, el modo de transferencia asíncrono fue inicialmente definido por el consultivo internacional para telegrafía y telefonía, a partir del encargo recibido de las Naciones Unidas para desarrollar y recomendar estándares internacionales en materia de tecnología y uso de telecomunicaciones. Este órgano es ahora más conocido como la Unión Internacional de Telecomunicaciones (ITU), de la cual el CCITT es un comité integrante. La ITU se encarga en la actualidad de formalizar los estándares de ATM.

En 1991 se constituyó el foro de ATM, un consorcio de vendedores, compañías de telecomunicaciones y usuarios, para agilizar un acuerdo de la industria sobre las interfaces ATM en Norteamérica.

ATM es un protocolo punto a punto, por conmutación de celdas, dúplex y orientado a conexión, que asigna ancho de banda a cada estación. Utiliza multiplexación asíncrona por división en el tiempo para controlar el flujo de información a través de la red. Funciona con anchos de banda que van desde los 25 Mbps hasta los 622 Mbps, aunque la mayor parte de los esfuerzos de desarrollo (y comerciales) se destinan al ATM a 155 Mbps.

Algunos de los beneficios derivados del ATM son:

- Excelente facilidad de ampliación.
- Integración con las redes clásicas.
- Ancho de banda por demanda.
- Capacidad para manejar los tipos de tráfico por la red: voz, datos, imágenes, video, gráficos y multimedia.
- Adaptabilidad tanto al entorno LAN como al WAN.

El ATM se desarrolló como una alternativa a protocolos de transporte tales como Ethernet y anillos con testigo (Token Ring), que presentaban evidentes limitaciones de ancho de banda y de facilidad de ampliación. Sin embargo, también se desarrollo con el fin de manejar de manera simultánea múltiples tipos de datos con eficiencia mejorada. Para ello, ATM tenía que ser capaz de transmitir a gran variedad de velocidades y soportar comunicaciones en ráfagas, ya que los tráficos de voz, datos y video se comportan a menudo de esta manera. Cabe señalar que la mayor parte de la gente no se da cuenta de que el tráfico de voz a través de un circuito conmutado muestra un comportamiento de tipo ráfaga. Cabe señalar que la tecnología *cell relay* referida comúnmente como ATM es una evolución a partir de los conceptos de Frame Relay y la conmutación de circuitos multi-tasa o multi-velocidad. La conmutación de circuitos multi-tasa designa canales con tasa de transmisión fija, cell relay de igual forma permite la definición por medio de canales virtuales designados con tasas de transferencia dinámica; así mismo cell relay, toma el esquema de no llevar a cabo ningún control de errores dentro de los nodos intermedios, permitiendo la recuperación de estos a través de los protocolos de las capas superiores en los sistemas finales, esto es que, el nivel ATM no realiza ninguna retransmisión y no existe ningún reconocimiento de que las celdas han sido recibidas. Antes de entrar de lleno a describir ATM, vamos a mencionar algunos conceptos necesarios para comprender el funcionamiento de esta tecnología:

Celdas en ATM

La conmutación de paquetes, que utiliza ancho de banda sólo cuando hay tráfico de datos, se desarrolló para manejar tráficos de datos de tipo ráfaga. No obstante, la conmutación de paquetes no se comporta adecuadamente con tráficos bidireccionales en tiempo real, tales como el video interactivo. ATM supera dicha limitación al emplear *celdas,* que son paquetes de longitud fija, en lugar de variable. Cada celda ATM contiene 48 bytes de datos útiles y 5 bytes de cabecera, tal y como se muestra en la figura 2.16.

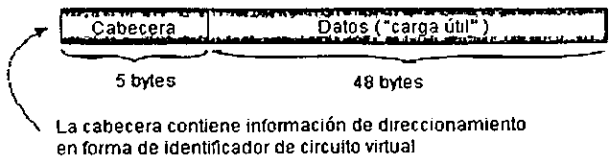


Figura 2.16

Las celdas de longitud fija ATM presentan numerosas ventajas con respecto a los paquetes de longitud variable, como son:

- **Capacidad de conmutación vía hardware.** La conmutación ATM, que es el procesado de celdas de longitud fija (de manera sencilla, predecible y fiable), puede realizarse a nivel hardware, en lugar de utilizar software costoso e intensivo en cálculo.
- **Niveles de servicio garantizados.** Los retrasos de interconexión y los de las colas de conmutación son más predecibles en el caso de celdas de datos de longitud fija. Por esta razón, pueden diseñarse los conmutadores para proporcionar niveles de servicio garantizados para todo tipo de tráfico, incluyendo la voz y el video.
- **Procesamiento paralelo.** Las celdas de longitud fija permiten que los conmutadores de retransmisión de celdas funcionen en paralelo, para velocidades que exceden en gran medida la capacidad de las arquitecturas de conmutación de tipo bus.
- **Capacidad de procesamiento de voz.** Aunque las celdas ATM sólo necesitan ancho de banda cuando hay datos que transmitir, también pueden proporcionar el equivalente a las divisiones temporales de un multiplexor por división en el tiempo, para tráfico continuo. Como resultado, ATM puede manejar igual de bien tráfico continuo en tiempo real, como voz digitalizada, y tráfico en ráfagas, como transmisiones de LAN.

La celda ATM se utiliza para transportar datos transmitidos entre conmutadores. Cada segmento de datos de 48 bytes se coloca en una celda junto con 5 bytes de cabecera, para conformar una celda ATM de 53 bytes. La cabecera de la celda contiene la información necesaria para llevar a cabo la conmutación.

ATM no utiliza ancho de banda compartido. En su lugar, cada puerto de un conmutador ATM se dedica a un usuario. Un conmutador ATM establece una conexión virtual entre un nodo transmisor y un nodo receptor. Dicha conexión se lleva a cabo basándose en la dirección de destino de cada celda, y dura justo lo que se tarda en transferir cada celda. Las transferencias de datos pueden realizarse en paralelo y a plena velocidad de la red. Ya que cada celda sólo se transmite al puerto asociado con su dirección de destino específica, ningún otro puerto recibe la celda y, por ello, se propicia que el tráfico sea reducido y, como, ventaja adicional, una seguridad elevada.

Conmutación ATM y conexiones virtuales

Para comunicarse a través de la red ATM es necesario que las aplicaciones establezcan de antemano una *conexión virtual (VC)* entre conmutadores. Una VC constituye una ruta de transmisión para una celda ATM, estableciendo una conexión punto a punto entre uno o más conmutadores. Las VC pueden establecerse de dos maneras. La primera, *los circuitos virtuales permanentes (PVC),* pueden ser configurados

manualmente por el administrador de la red. A cada PVC se le asigna un ancho de banda que garantiza la calidad de servicio de una estación concreta. Los administradores de la red configurarán PVC para las aplicaciones críticas que requieran constantemente la mayor prioridad, o para las conexiones permanentes como las que se establecen entre ruteadores (encamiadores) y puentes. La segunda manera de establecer una VC es el *circuito virtual conmutado (SVC).* Un SVC es una VC establecida "sobre la marcha" cuando lo necesita la aplicación.

Identificador de circuito virtual.

La cabecera de la celda también incluye dos campos de dirección, el *identificador de camino virtual (VPI)* y el *identificador de canal virtual (VCI),* que, de manera conjunta, ocupan 3.5 bytes y definen *el identificador de circuito virtual,* que es la ruta a seguir por una celda para llegar a un conmutador concreto. Dichos campos se actualizan en cada conmutador del camino. Los identificadores de circuito virtual marcan las celdas de una conexión concreta, y los conmutadores transfieren los datos en una VC mediante conmutación hardware, gracias a la marca de la conexión de la VC localizada en la cabecera de la celda. Todavía son importantes los problemas de congestión y encaminamiento en la VC entre varios conmutadores en un proceso estándar. La gestión de la congestión es muy importante, ya que la pérdida de una pequeña cantidad de celdas (por ejemplo, un 0.1 %) tiene como resultado una pérdida de tramas dramáticamente grande (por ejemplo, un 20 %). Como esto no es aceptable, se están estudiando y evaluando de manera activa diferentes alternativas.

Todas las celdas ATM son del mismo tamaño lo que permite disponer de:

- **Ancho de banda garantizado.** Los paquetes de longitud variable pueden provocar retrasos en el tráfico de los conmutadores, de la misma manera que los coches se ven obstaculizados en los cruces cuando los camiones de gran tamaño realizan giros en ellos.
- **Alto rendimiento.** Gran volumen de datos puede transitar concurrentemente por una única conexión física.
- **Conmutación hardware.** A corto plazo este hecho incrementa la tasa de throughput, y a la larga favorecerá la explotación tecnológica de los avances en precio frente a rendimiento, a medida que aumente la potencia de los procesadores y decaiga su costo.
- **Asignación de prioridad a los datos.** ATM puede proporcionar una respuesta determinista, que es esencial para aplicaciones sensibles a los retrasos, tales como la transmisión de video y audio o el transporte de flujos de datos interactivos, de carácter crítico.

Orientado a conexión, significa que la conexión debe establecerse entre las computadoras de transmisión y de recepción, antes de empezar a transferir datos. Cada punto intermedio de conmutación debe ser identificado, y se le ha de informar acerca de la existencia de la conexión. Cada paquete se encamina por separado y, por ello, debe incluir la dirección completa de su punto de destino.

La transmisión dúplex permite transmitir sobre un par de hilos y recibir sobre otro par de manera simultánea, haciendo posible utilizar casi por completo ambos pares, obteniendo velocidades de transferencia altas y sostenibles. Al permitir transmisiones

dúplex, ATM duplica el ancho de banda efectivo de las transmisiones semidúplex clásicas utilizadas por la mayor parte de los protocolos de red.

Tal y como se mencionó previamente, las redes ATM deben establecer una conexión entre las estaciones de emisión y recepción antes de comenzar a transmitir las celdas. Dicha conexión entre dos estaciones es lo único que el conmutador ATM debe tener en cuenta. A diferencia de un ruteador, el conmutador ATM selecciona la ruta entre la estación emisora y la receptora, e informa a los conmutadores intermedios de la misma para asegurar que los recursos para la transmisión de la celda a lo largo de la red se asignen adecuadamente. Una vez establecida la ruta para la transmisión de una celda, el conmutador ATM asigna un número de conexión a cada enlace punto a punto a lo largo de la ruta. Los números de conexión se escogen independientemente para cada uno de los enlaces punto a punto en el camino de transmisión. Un camino queda constituido a partir de cierto número de dichos enlaces, estando los mismos unidos por conmutadores. Esto se traduce en la posibilidad de que una celda contenga, potencialmente, un número de conexión distinto para cada enlace. Cada conmutador cambia los números de conexión de cada celda según transfiere la misma de un enlace a otro. Este cambio permite que los campos asociados a los números de conexión sean sólo lo suficientemente largos como para poder identificar las conexiones manejadas por un solo enlace.

Esto permite que ATM haga uso de números de conexión bajos, en lugar de utilizar las direcciones tan largas que requieren la mayor parte de los protocolos. Así, ATM es más eficiente, ya que los números aprovechan mejor el espacio existente en la celda y, con ello, el ancho de banda, siendo también más rápido, al permitir la utilización en los conmutadores de tablas de conversión pequeñas.

ATM proporciona distintas calidades de servicio para acomodar los distintos tipos de tráfico. Una estación solicita el ancho de banda adecuado para cada conexión, y la red ATM automáticamente asigna dicho ancho de banda, al usuario. En realidad, el ancho de banda no se asigna de manera dedicada así como así, si no que se comparte con los otros usuarios, pero asegurando la calidad de servicio solicitada. Esto es posible gracias a que la red controla el número de conversaciones simultáneas.

Para acceder a la red, una estación o computadora solicita un circuito virtual entre los puntos origen y destino. Durante el establecimiento de la conexión, la estación del extremo puede solicitar la calidad de servicio que necesita para satisfacer los requisitos de transmisión, siendo confirmada por los conmutadores ATM sólo si existen suficientes recursos disponibles para ello. La calidad de servicio garantizada resulta particularmente útil a la hora de transportar comunicaciones interactivas en tiempo real, tales como voz y video. ATM utiliza un protocolo conocido como *interfaz usuario-a-red* (UNI: User-to-Network Interface) para asignar niveles de ancho de banda dedicado a las estaciones y a las aplicaciones.

Interfaz usuario-a-red (UNI)

Los protocolos UNI de ATM proporcionan múltiples clases de servicio y de reserva de ancho de banda durante el establecimiento de una conexión sobre una conexión virtual conmutada.

La UNI define la compatibilidad (interoperabilidad) entre el equipo del usuario y el puerto del conmutador ATM. Una UNI pública define la interfaz entre un servicio público de una red ATM, admitiendo habitualmente una interfaz SONET o DS3. Por otro lado, una UNI privada define la interfaz entre un usuario y un conmutador ATM privado, presentando por lo general una interfaz a par de cobre o a fibra óptica.

El protocolo UNI implementado en los productos debe coordinar el ancho de banda asignado localmente entre otros conmutadores y segmentos de LAN. También debe admitir cierta variedad de sistemas operativos de red que garanticen calidad de servicio. Ambos aspectos afectan a la compatibilidad entre equipos de la red ATM, y deben ser considerados por los administradores de la red al seleccionar sus productos.

2.6.1 ATM y el modelo OSI

ATM llega mucho más allá en el modelo ISO-OSI que la mayoría de los protocolos de transporte, tal y como muestran las figuras siguientes.

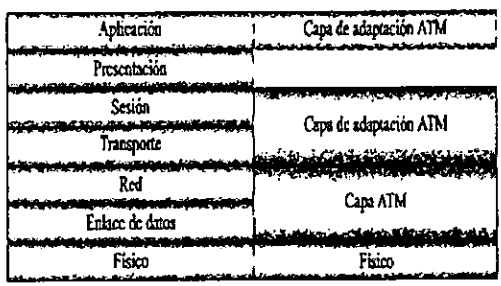


Figura 2.17

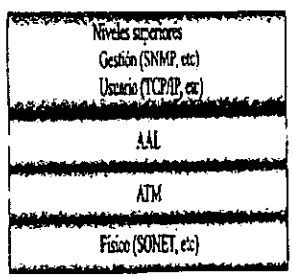


Figura 2.18

Por ello, para sacarle todo el partido a ATM, así como para integrarlo en el protocolo de red existente, deben desarrollarse aplicaciones que tengan en cuenta las implicaciones de alto nivel del modo de transferencia asíncrono.

La capa Física

El aspecto más importante del nivel físico es que ATM no define ningún tipo de medio específico. Soporta incluso aquellos utilizados en otros sistemas de comunicaciones. Varias especificaciones de interoperabilidad aún se encuentran bajo desarrollo. Los expertos industriales, ratifican a la **red óptica síncrona** (Synchronous Optical Network, SONET), como el medio de transporte físico para ATM tanto en aplicaciones WAN como LAN. Se recomienda también FDDI (100 Mbps), canal de fibra (155 Mbps), OC3 SONET (155 Mbps) y T3 (45 Mbps) como la interfaz física para ATM.

La capa de ATM

Esta capa es la responsable de transportar la información a través de la red, utilizando conexiones virtuales. Las conexiones son virtuales porque aunque los usuarios pueden conectarse fin a fin, las conexiones sólo se realizan cuando las celdas necesitan ser

enviadas. Cabe mencionar que la conexión no es dedicada para uso exclusivo de una sola conversación, aunque a la vista del usuario así parece.

La capa de adaptación de ATM (AAL: ATM Adaptation Layer)

La capa AAL reside directamente sobre la capa de ATM. Es en esta capa donde ATM convierte el tráfico de usuario de las aplicaciones al formato de ATM, y donde se proporcionan los mecanismos para las aplicaciones orientadas y no orientadas a conexión (como X.25 y tráfico en redes de área local, respectivamente), aplicaciones con tasas de transferencia variables y aplicaciones con tráfico que requiera velocidad constante (como video y multimedia). En otras palabras esta capa desarrolla el mapeo necesario entre la capa de ATM y los protocolos de las capas superiores, es decir, se encapsúla el tráfico de las aplicaciones superiores del usuario dentro del formato de ATM. Esta capa además debe resolver los problemas de flujo de datos para la aplicación y la variación del retraso de la celda. En realidad, la capa AAL se compone de dos subcapas, la subcapa *de convergencia* (CS: Convergence Sublayer) y la de *segmentación y reensamblado* (SAR: Segmentation And Reassembly).

- **Subcapa de convergencia (CS)**

Permite la retransmisión de voz, video y tráfico de datos a través del mismo elemento de conmutación. Interpreta los datos que le llegan desde la aplicación de la capa superior y los prepara para su procesamiento en la subcapa de segmentación y reensamblado. El CS desarrolla el procesamiento de retrasos de celdas, la sincronización de fin a fin y el manejo de celdas perdidas o mal insertadas. Obviamente, las operaciones y funciones llevadas a cabo por la subcapa de convergencia varían dependiendo del tipo y el formato de los datos recibidos

- **La subcapa de segmentación y reensamblado (SAR)**

Antes de que una aplicación transmita datos por una red ATM la subcapa de SAR *segmenta* los mismos en celdas de datos de ATM de 48 bytes. Una vez que dichas celdas alcanzan su destino, la subcapa de SAR las *reensambla* en datos de alto nivel y las transmite a los dispositivos locales apropiados.

- **AAL-5**

Ya que ATM puede transportar distintos tipos de tráfico, existen varios protocolos de adaptación, funcionando de manera simultánea, en la capa de adaptación. Por ejemplo, las redes de área local suelen utilizar el protocolo AAL-5, diseñado específicamente para manejar este tipo de tráfico variable. En la subcapa de convergencia del AAL-5, se añade un campo de 8 bytes que incluye la longitud de los datos y una comprobación de errores, a cada trama (o bloque) de información del usuario (hasta 64 KB de longitud) que llega de la aplicación de nivel superior. La trama AAL-5 se separa en un flujo de celdas de datos de 48 bytes mediante la subcapa SAR. En la estación de recepción esta subcapa reensambla las celdas en tramas, y la CS las procesa y elimina el campo de 8 bytes asociado a la longitud de los datos y a la comprobación de errores. La trama se pasa, a continuación, al protocolo de nivel superior.

El AAL-5 es la base de la emulación de LAN, una tecnología clave en la integración y migración hacia redes ATM.

2.6.2 Clases de Calidad de Servicio ATM (QoS: Quality of Service)

Dado que ATM puede soportar cualquier tipo de tráfico, éste debe ser identificado como tal para preservar los parámetros de calidad de servicio (QoS) que requieren cada uno de ellos por separado. Por ello, se hace necesario que existan distintivos para cada uno de los servicios, debido a esto, todo tipo de tráfico puede tomar lugar dentro de una misma conexión lógica. Esta conexión lógica se basa en una estructura identificada por dos partes que son: *el canal virtual* (VCI) y *la ruta virtual* (VPI).

Para mantener los parámetros de garantía de comunicación y la calidad de servicio requerida por la información que transporta ATM, el forum ATM ha definido 4 clases de servicio en la capa de adaptación ATM (AAL) referidos como QoS:

1. Clase A: AAL 1
2. Clase B: AAL 2
3. Clases C y D: AAL 3
4. Clases C y D: AAL 5

Clase A. La clase A o *tasa de bit constante* (CBR: Constant Bit Rate), provee un canal virtual de transmisión con ancho de banda fijo. La CBR es utilizada primeramente por el tráfico característico por un flujo continuo de bits a una tasa regular, con un ancho de banda altamente sensible al retraso e intolerante a la pérdida de celdas tal como el video en tiempo real y el tráfico de voz.

Clases B y C. Estas clases se refieren a la *tasa de bit variable* (VBR: Variable Bit Rate), el cuál tiene una naturaleza de ráfaga (bursty) como en aplicaciones de voz o video que utilizan compresión. La **clase B** es tráfico VBR en tiempo real (RT-VBR), donde el retraso de fin a fin es crítico, tal como la video conferencia interactiva. La **clase C** es tráfico en tiempo no-real (NRT-VBR), donde el retraso no es tan crítico, tal como video playback, preparación de cintas y mensajes de video por correo.

Clase D. El tráfico de este tipo es dividido en 2 clases: *tasa de bit disponible* (ABR: Available Bit Rate) y *tasa de bit sin especificar* (UBR: Unspecified Bit Rate). Estas clases son para el tráfico de red LAN con características de ráfaga y aquellos datos que pueden ser más tolerantes al retraso y pérdida de celdas. UBR es un servicio de mejor esfuerzo que no especifica la tasa de bits o los parámetros de tráfico y no garantiza la calidad en el servicio. Proyectado como una manera para hacer uso del exceso del ancho de banda existente, UBR puede ser sometido a tener celdas perdidas y desecho de todos los paquetes. ABR de la misma manera es un servicio de mejor esfuerzo, pero difiere de UBR en que es un servicio de administración, basado en la tasa de celdas mínima (MCR: Minimum Cell Rate) y con una pérdida de celdas.

Una red ATM, en el momento que una aplicación necesite establecer una conexión entre dos usuarios deberá negociar un contrato de tráfico que especifica la clase de servicio de la conexión. Las clases de servicio ATM cubren un rango de parámetros de

servicio y garantías de QoS. Las garantías de servicio pueden definir niveles mínimos de ancho de banda disponible, límites superiores del retraso de las celdas y celdas perdidas. Por esta razón ATM entrega importantes ventajas sobre las tecnologías de redes de área local (LAN) y de área amplia (WAN). Con la promesa de un ancho de banda escalable y los parámetros de calidad de servicio requeridos de forma garantizada, lo cuál, facilita el desarrollo de nuevas clases de aplicaciones tales como multimedia y videoconferencias.

2.6.3 Topología de una red ATM

ATM está formado por una topología de malla de conmutadores. Esto lleva a la conclusión de que cualquier punto en la red puede ser alcanzado desde cualquier otro punto mediante múltiples rutas. Además como limitación tiene únicamente las características de atenuación del medio utilizado. Los conmutadores de malla son generalmente dispositivos multipuertos que realizan la conmutación de las celdas. Este conjunto de conmutadores ATM son interconectados por enlaces ATM punto a punto o interfaces. Los conmutadores soportan dos tipos de interfaces: La interfaz de red-usuario (UNI) y la interfaz de red a red (NNI: Network Node Interface). La interfaz UNI, como ya se mencionó, interconecta los sistemas finales ATM (hosts, enrutadores, etc.) a un conmutador ATM, mientras que la interfaz NNI puede ser definida de manera precisa como una interfaz que conecta a dos o más conmutadores ATM. En otras palabras una NNI es cualquier enlace físico o lógico que cruza entre dos conmutadores ATM intercambiando el protocolo NNI. Un esquema representativo de la topología ATM se muestra a continuación con la figura 2.19.

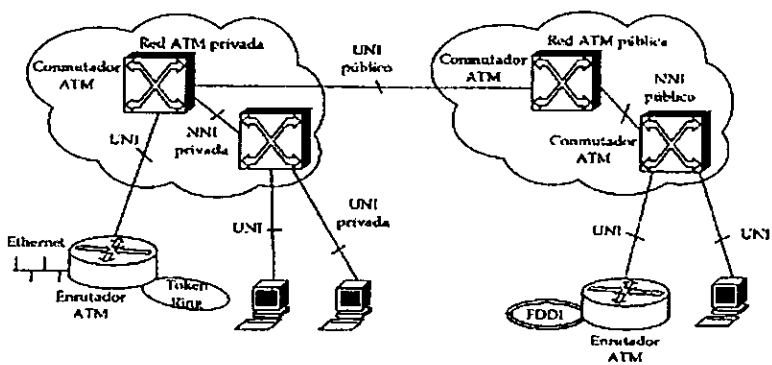


Figura 2.19

2.6.4 Funcionamiento de ATM

La combinación de conmutación de celdas y las conexiones punto a punto con números de conexión bajos permiten que el ATM fragmente las tareas, básicas de red en dos componentes distintos: determinación de la ruta y reenvío de los datos (conocidos habitualmente como encaminamiento y conmutación) manejando cada uno de ellos con una tecnología distinta. A modo de ilustración, veamos cómo se transmite una celda por una red ATM.

Determinación del camino

La determinación del camino es una tarea intensiva en cálculo, típicamente realizada en software, que requiere un conocimiento dinámico de la topología global de la red. La determinación del camino en ATM se hace mediante el establecimiento de conexiones virtuales, y sólo ocurre una vez en cada sesión de transferencia de datos. El ATM selecciona un mismo camino para todas las celdas de la conexión durante el establecimiento de la misma. Tras el establecimiento de la conexión, sólo se llevan a cabo sencillas operaciones para la transferencia de la celda, requiriendo un sistema diferente para la conexión. La parte de establecimiento de conexión de ATM debe estar basada en protocolos no orientados a conexión. Según esto, cada paquete que viaja por una red clásica ha de contener toda la información de encaminamiento globalmente significativa, y cada paquete debe procesarse en los enrutadores antes de que los datos sigan avanzando. Esta evocación constante de la determinación del camino supone el desperdicio de costosos recursos, derivando en un cuello de botella ocasionado por la mala utilización de los enrutadores.

Para ilustrar el problema de encaminamiento resuelto por la arquitectura ATM, consideremos un proceso de copia de seguridad en una red. Supongamos que tenemos que realizar una copia de seguridad de 2 gigabytes, que residen en un servidor de una red con encaminamiento. El programa que realizará la copia creará probablemente 10 millones de paquetes de 200 bytes, puesto que 200 bytes es el tamaño de la unidad de transferencia utilizada en las redes con encaminamiento. A cada uno de estos 10 millones de paquetes se le asignará una dirección global de red, y cada enrutador procesará por separado cada uno de los 10 millones de paquetes (incluso aunque fluyan constantemente a través del mismo camino). Esto se traduce en que cada enrutador de la ruta debe examinar la cabecera de capa de red de cada paquete, y componer separadamente y de nuevo la ruta para cada uno de ellos, a pesar de que la ruta sea idéntica para cada uno de los 10 millones de paquetes, con lo que hay un gran desperdicio de recursos de proceso.

El conmutador ATM establece la ruta sólo una vez mediante una conexión virtual (VC) y le asigna después un identificador de conexión. Los conmutadores de dicha ruta reciben información referente al ancho de banda requerido por la VC, así como instrucciones sobre cómo interpretar adecuadamente el identificador de la conexión. Tras ello, todas las celdas con ese identificador de conexión se conmutan por hardware a lo largo de la ruta, permitiendo que la función de cálculo de rutas se dedique a dar servicio a nuevas conexiones. De esta manera, las celdas carecen de direcciones de encaminamiento complejas, ya que solo se marcan con un pequeño identificador temporal de la conexión, que los conmutadores ATM saben convertir en el camino definido mediante la VC.

Reenvío de datos

Es una función de hardware intensiva que necesita capacidad de conmutación del orden de gigabits. La conmutación ATM basada en celdas puede realizarse con gran sencillez y, al igual que en la conmutación Ethernet, por completo en hardware. Se realiza en conmutadores ATM que trabajan sobre celdas ATM. Según esto, las celdas se conmutan por hardware a lo largo del camino previamente establecido para la VC,

durante toda la sesión. ATM constituye fundamentalmente un formato para el funcionamiento de los conmutadores, y no proporciona protocolos para la validación del acceso. Cada puerto de un conmutador se comporta en muchos aspectos como una estación. La información de la cabecera de la celda recién recibida se utiliza para buscar la información de reenvío necesaria para encaminar la celda en el conmutador. También, se verifica la existencia de errores en ella, eliminándose las que presenten fallas. La información de esta cabecera se modifica en cada conmutador, para representar la ruta hasta el siguiente. El direccionamiento de las celdas ATM es de carácter local al conmutador, en contra de lo que sucede con las direcciones MAC, que identifican a los usuarios individuales con valores únicos a nivel local y global.

Conmutadores ATM

Los conmutadores ATM permiten establecer una conexión por puerto. Algunos conmutadores son sin bloqueo, en el sentido de que pueden admitir un enlace de soporte (backbone) equivalente a la suma de las velocidades de los puertos de entrada. Además, transfieren el tráfico desde la entrada hacia la salida sin procesos intermedios de almacenamiento y reenvío. Se utiliza almacenamiento intermedio sólo si varias entradas intentan acceder a la misma salida de manera simultánea. A pesar del almacenamiento ocasional, ATM es todavía superior a los lentos enrutadores tradicionales basados en el almacenamiento y reenvío.

La operación básica de un conmutador ATM es simple: una celda proveniente de un enlace sobre un valor conocido de VCI/VPI, busca el valor de conexión en una tabla de translación local para poder determinar el puerto de conexión de salida y el nuevo valor VPI/VCI de la conexión sobre ese enlace; y entonces retransmite la celda sobre ese enlace con los identificadores de conexión apropiados. La operación de transmisión del conmutador, es simple, ya que las tablas de translación son previamente establecidas antes de que se lleve a cabo alguna transmisión. Dependiendo de como se establezcan las tablas, se determinará el tipo de conexión, la cuál puede ser: *conexión virtual permanente* (PVC) o *conexión virtual conmutada* (SVC). Es importante mencionar que estos conmutadores pueden utilizarse como concentradores o dispositivos de comunicación de área extendida, que transmite celdas ATM entre redes LAN remotas.

La base de las redes de soporte con velocidades de gigabits para ATM está constituida por los elementos de conmutación hardware ampliables. La función de conmutación ATM consta de dos partes: el hardware de conmutación, que es quien realmente lleva a cabo la misma, y el punto de control de la conmutación, que gestiona la estructura de conmutación mediante:

- La gestión de peticiones de conexiones virtuales (VC).
- El conocimiento de la topología de la red ATM.
- El mantenimiento de las bases de datos de reenvío.
- La capacitación de la gestión de red ATM basada en SNMP.

Consideraciones de cableado

La topología ATM se basa en una red de switches, lo que quiere decir que cualquier punto de la red puede alcanzarse desde cualquier otro a través de diversos ruteadores

que involucran diferentes conexiones entre los conmutadores. ATM no precisa de protocolos de capa física específicos para ello ni tampoco presenta limitaciones de distancia o alcance que las especificadas. Se logra así simplificar la construcción del cableado, ya que no existen reglas que obstruyan su diseño. Sin embargo, se realza la importancia de la documentación, pues al no existir reglas, sería prácticamente imposible descifrar una instalación incorrectamente documentada.

Medios admitidos por el ATM

La independencia del medio es una de las motivaciones claras del ATM. Existen muchas especificaciones de capa física, desde 25 Mbps, incluyendo varias entre 100 y 155 Mbps, y llegando hasta los 622 Mbps. A 155 Mbps, ATM admite UTP de categorías 3, 4 y 5, STP tipo 1, fibra óptica, fibra óptica multimodo y fibra óptica monomodo para redes de área local.

Interfaz física para redes de área extensa

La interfaz de WAN a 155 Mbps para redes públicas de compañías de telecomunicaciones estará basado en la red óptica síncrona (SONET). Como ya se mencionó anteriormente, SONET constituye un esquema de transporte de capa física aceptado internacionalmente, que se desarrolló a principios de los años ochenta.

2.6.5 LAN virtuales

La naturaleza orientada a conexión del ATM y el rendimiento derivado de la conmutación hardware de las celdas permiten crear redes virtuales. Una **LAN virtual** es una lista de direcciones de tipo control de acceso al medio (MAC) o de red de dispositivos, independientes de los puertos físicos. Un dispositivo puede acceder a cualquier otro dispositivo de la misma LAN virtual. Pueden definirse filtros entre éstas de igual manera que pueden hacerlo los ruteadores.

Pueden formar parte de la misma LAN virtual dispositivos que se encuentren conectados a medios distintos. Más aún, los usuarios pueden cambiar la localización física de sus equipos a cualquier segmento de la subred virtual sin necesitar reconfigurar la dirección.

Las LAN virtuales capacitan a los administradores de red para agrupar lógicamente los dispositivos con independencia de su localización física, proporcionando anchos de banda dedicados y servicios a cada uno de ellos.

Los usuarios pueden conectarse a cualquier puerto de la red, y la LAN virtual se encarga del resto. Además del filtro de direcciones, las LAN virtuales proporcionan:

- Traslados, incorporaciones y cambios sencillos.
- Asignación de ancho de banda.
- Características de seguridad.

Uno de los principales problemas de los administradores de red que deben manejar redes de encaminamiento de grandes dimensiones, es el inmenso esfuerzo administrativo necesario para llevar a cabo traslados, incorporaciones y cambios. Resulta especialmente complejo en redes con Protocolos Internet (IP), donde cada LAN física está asociada a una subred lógica, tal y como lo muestra la figura 2.20.

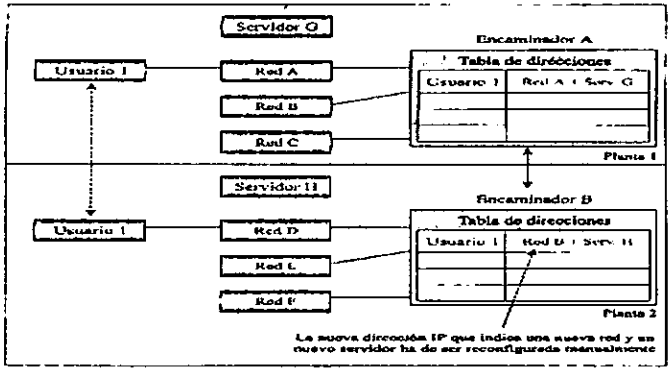


Figura 2.20

Si un usuario tiene que trasladarse de una planta del edificio a otra, suele ser necesario reconfigurar la estación de trabajo con una dirección IP válida en la nueva subred. Para manejar dichos cambios, los administradores de redes heredadas tienen que reconfigurar manualmente los ruteadores. Las LAN virtuales, sin embargo, eliminan todo este proceso, permitiendo que se agrupen de manera lógica los dispositivos con independencia de su localización física, proporcionando anchos de banda dedicados y servicios a cada uno de ellos. Esquemáticamente esto se ve en la siguiente figura 2.21.

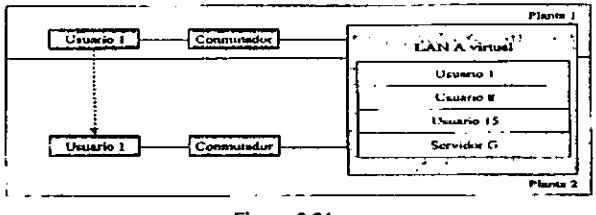


Figura 2.21

Esto es, el usuario se conecta, a cualquier puerto de la red, y la LAN virtual se encarga del resto. Las redes virtuales identifican la dirección física de un nuevo dispositivo y la asocian a una dirección de capa de red basándose sólo en asignaciones previas, sin intervención humana en el sistema, o en el equipo del usuario.

Los conmutadores ATM proporcionan alto rendimiento en el reenvío de datos: toda la información se convierte en celdas con el formato común de 53 bytes. A diferencia de los conmutadores de paquetes que procesan mediante software paquetes de longitud variable, los conmutadores ATM o de reenvío de celda siempre manipulan unidades de datos uniformes y de tamaño pequeño. Así se permite que las funciones clave se implementen en hardware, cuyo resultado es que el procesamiento y la conmutación

de celdas son muy rápidos, además de la posibilidad de construir grandes redes manteniendo retardos de propagación aceptables. Por otra parte ATM permite conexiones redundantes que incrementan la tolerancia a fallos. Sin embargo, para permitir que la red sea lo suficientemente rápida con velocidades de varios gigabits por segundo, ATM no proporciona detección de errores ni retransmisiones, por lo que el futuro usuario debe tenerlo en cuenta.

Seguridad

Mediante el uso de procedimientos explícitos para la iniciación de la comunicación, los mecanismos de seguridad pueden implementarse llamada a llamada, en lugar de paquete a paquete, de tal manera que los usuarios se vean privados automáticamente del acceso a recursos ajenos. La red podría determinar de manera inteligente qué tráfico debe cursarse a partir de la identidad del emisor y el destinatario. Más aún, pueden implementarse mecanismos de identificación que restrinjan el acceso del usuario a la totalidad de los recursos de red. La naturaleza orientada a conexión del ATM también asegura que el tráfico de datos sólo se encamina a su verdadero destino: no se desperdician inútilmente recursos de red para difusiones innecesarias, ni se compromete la seguridad. Este comportamiento elimina la necesidad de incorporar protocolos de difusión y de filtrado para mejorar la eficiencia.

Seguridad y LAN privadas

Las LAN virtuales pueden servir para incrementar la seguridad, al permitir que los administradores de la red utilicen LAN virtuales para definir restricciones de acceso entre grupos de dispositivos, proporcionando una férrea seguridad. Más aún, los conmutadores ATM proporcionan mecanismos de seguridad a nivel de puertos al permitir a los administradores que restrinjan las subredes virtuales a determinados puertos físicos.

Costo de utilización

De las tecnologías de alta velocidad, probablemente ATM sea la más cara. Los productos ATM son propensos a costar más a causa del empaquetamiento en celdas y de los servicios adicionales. Sin embargo, además de los altos costos de los adaptadores y conmutadores ATM, hay que tener en cuenta si la formación y la consultoria son dependientes del vendedor y del producto. Si se cambia de vendedor, los costos tendrán que incluir una parte destinada a gastos de formación e integración.

2.6.6 Emulación de LAN

Por su parte la emulación de redes LAN conocida como ELAN se basa en dos estándares, uno es responsabilidad del forum ATM el de *emulación de LAN ATM* y el segundo establecido por el IETF (Internet Engineering Task Force) basado en el método IP clásico sobre ATM referido como *RFC1577*. Los dos estándares asumen que los usuarios de ATM tendrán adaptadores de sistema para sus computadoras de escritorio soportando una interfaz UNI ATM, y que serán conectados hacia un conmutador ATM. Los conmutadores normalmente soportarán ambos puertos, conexiones hacia estaciones o sistemas de servidor y troncales ATM. Algunos conmutadores además

soportarán estaciones no-ATM. La emulación de LAN es un conjunto de servicios que realizan la traducción entre los protocolos de alto nivel de los servicios de protocolos no orientados a conexión y los protocolos de ATM de bajo nivel orientados a conexión, tal y como muestra la figura 2.22.

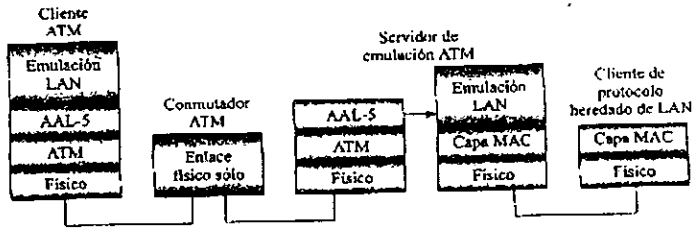


Figura 2.22

Como ya se ha mencionado, la capa de adaptación de ATM (AAL) da formato a los datos como celdas de ATM (de 48 bytes), proceso que se conoce como *segmentación*. Una vez que las celdas de ATM alcanzan su destino, se reconstruyen en datos de nivel superior y se transmiten a los dispositivos locales respectivos en un proceso conocido como *reensamblado*. Ya que ATM puede transportar distintos tipos de tráfico, dentro de la capa de adaptación existen varios protocolos de adaptación funcionando de manera simultánea. El protocolo de adaptación sobre el que se basa la emulación de LAN es el AAL-5.

En el convertidor de ATM a LAN del extremo de la red (inter-red), la emulación de LAN resuelve los problemas de conexión de datos para todos los protocolos (con y sin encaminamiento), resolviendo las direcciones de LAN y ATM en la capa MAC. La emulación de LAN es totalmente independiente de los protocolos, los servicios y las aplicaciones de nivel superior.

Como la emulación de LAN tiene lugar en los dispositivos inter-red y en los dispositivos terminales, es totalmente transparente para la red ATM y para los dispositivos anfitriones de las redes Ethernet y de anillo con testigo.

La figura 2.23 muestra a continuación el funcionamiento de la emulación de LAN en una LAN heredada.

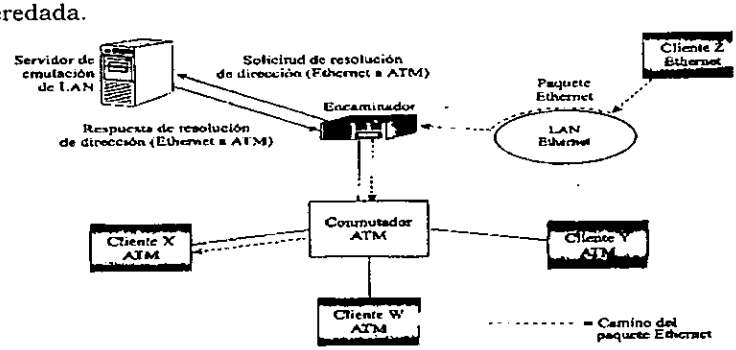


Figura 2.23

Las PCs del entorno Ethernet acceden a los servidores de alto nivel con interfaces ATM a través de conmutadores LAN/ATM. Como la emulación de LAN hace parecer a ATM, como una LAN clásica, las técnicas estándar de enlace permiten que el conmutador LAN/ATM proporcione conectividad independiente del protocolo. No es preciso modificar las PCs heredadas, que experimentan un incremento en su rendimiento a causa de la elevada capacidad de entrada/salida del servidor, gracias a la interfaz ATM de alta velocidad. Además, se benefician del ancho de banda dedicado proporcionado por la implementación conmutada de la LAN.

Los estándares de emulación de LAN del foro de ATM también contemplan la implementación de emulaciones de múltiples LAN dentro de una misma red. La emulación de una LAN se implementa por medio de un modelo cliente-servidor, más o menos de la siguiente manera: Un cliente de la emulación de LAN, como por ejemplo el software de una estación de trabajo, convierte las direcciones MAC en direcciones ATM. Cada cliente se conecta al servidor mediante una conexión virtual. Sólo los clientes que se conectan a un mismo servidor obtienen visibilidad mutua, y pueden comunicarse entre sí de forma directa. La segmentación a nivel lógico de la red entre múltiples funciones del servidor (pudiendo ser dispositivos autónomos, software de los equipos de usuario o módulos de conmutación ATM) permite la coexistencia de múltiples emulaciones de LAN sobre una misma red física.

La figura 2.24 muestra el aspecto físico y lógico de una emulación de múltiples LAN.

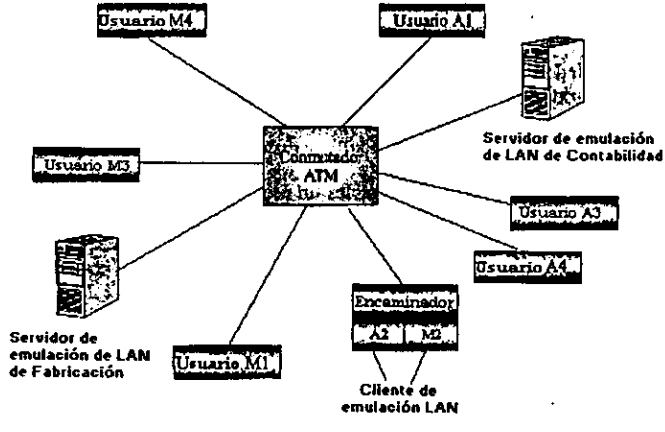


Figura 2.24

En su componente físico, el ruteador ejecuta dos clientes de emulación de LAN (A2 para el departamento de contabilidad y M2 para el de fabricación). El servidor de cada departamento lleva la cuenta de sus propios clientes a través de una base de datos residente. Cuando el usuario de contabilidad A1 envía un paquete al usuario de fabricación M1, el servidor de contabilidad comprueba si se genera una coincidencia dentro de su base de datos. Si no se produce, pasa la dirección MAC al ruteador (A2/M2), quien reenvía el paquete al servidor del departamento de fabricación para que se lo entregue a M1.

La presentación lógica se parece al aspecto físico de una LAN de hoy en día, siendo así consistente con el propósito de la emulación de una LAN. Los clientes de los departamentos se comunican directamente entre sí, y con los servidores e indirectamente con los demás departamentos, a través de un ruteador de red.

Emulación de LAN y LAN virtuales conmutadas

Ya existen productos comerciales, como por ejemplo el conjunto de aplicaciones de gestión de red Trascend de 3Com, que permiten a los gestores de red definir múltiples emulaciones de LAN. Cuando distintas redes de área local emuladas se comunican entre sí a través de uno a más conmutadores de una red ATM, al resultado se le conoce como *LAN virtual conmutada,* tal y como se muestra a continuación:

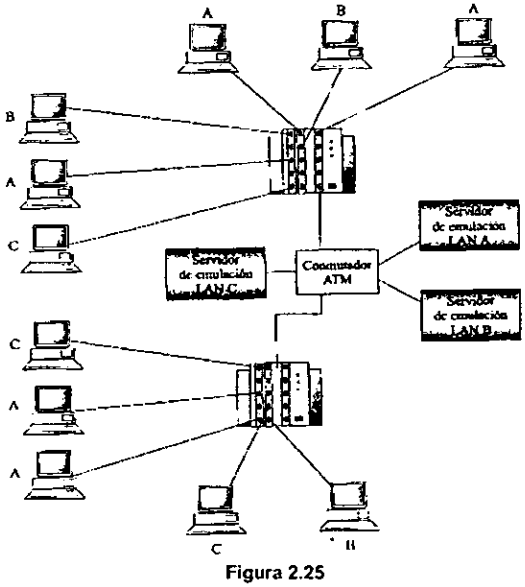


Figura 2.25

La gestión de LAN virtuales puede ser bastante compleja, ya que en este caso no basta con la gestión de la conectividad física. También es preciso supervisar y gestionar las interconexiones lógicas en la LAN. En las LAN virtuales conmutadas, el encaminamiento deja de ser un cuello de botella físico, pasando a ser una función de proceso lógica que los conmutadores ATM pueden manejar eficientemente.

La emulación de LAN virtuales conmutadas proporciona las mismas ventajas que las LAN virtuales más comunes:

- Traslados, incorporaciones y cambios sencillos.
- Seguridad para los grupos de trabajo.
- Cortafuegos en prevención de difusiones incontroladas.
- Control del flujo que permite utilizar mejor el ancho de banda de la red.

Todas estas ventajas están disponibles sin necesidad de adquirir equipos adicionales ni de volver a cablear los segmentos de la red. Los administradores de red pueden gestionar los segmentos mediante la redefinición de grupos dentro del sistema de gestión de red, o reconfigurando el software del dispositivo de usuario y/o el conmutador ATM.

Aunque la emulación de LAN ATM simplifica en gran medida la creación de grupos de trabajo virtuales todavía es necesario utilizar ruteadores para gestionar tanto la difusión como la resolución de direcciones, tal y como muestra a continuación:

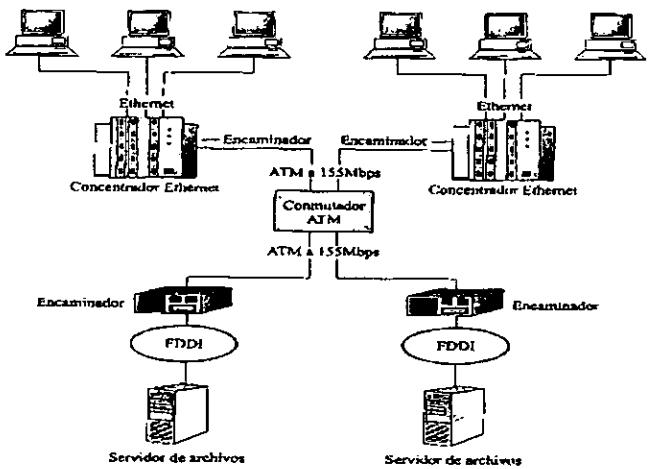


Figura 2.26

A medida que se amplia la red con enlaces de soporte de mayor velocidad, el ruteador debe procesar el tráfico de dichos enlaces a velocidades de transmisión más altas para evitar la creación de cuellos de botella. Aunque algunos ruteadores de gama alta incluyen interfaces de ATM diseñadas para reenviar paquetes a velocidades de 155 Mbps, el diseño de los ruteadores convencionales no permite aprovechar todas las ventajas, del rendimiento del ATM.

Una arquitectura de LAN ATM ampliable hace uso de todas las funciones de un ruteador de manera distribuida, lo que permite que el costo asociado a las funciones de encaminamiento se incremente paralelamente según crece la red. Las funciones de encaminamiento son intensivas en proceso, pero se utilizan con poca frecuencia, mientras que las funciones de reenvío de paquetes requieren poco proceso, pero alto rendimiento.

En un ruteador distribuido, las funciones de reenvío de paquetes se llevan a cabo en los dispositivos de acceso a la red, tal y como se muestra en la figura 2.27.

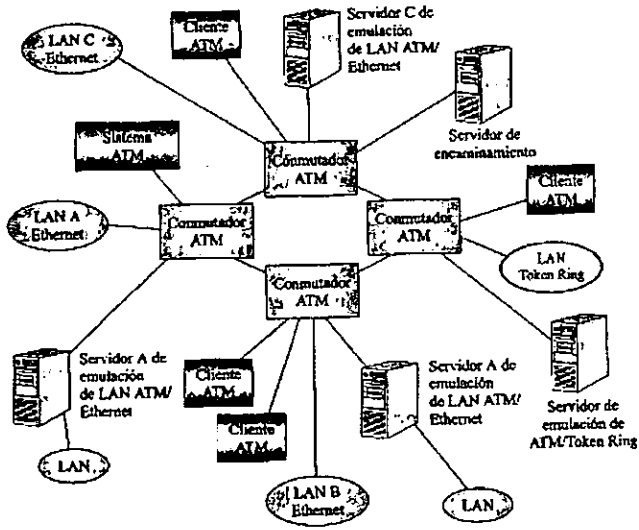


Figura 2.27

Los conmutadores ATM se diseñan de manera que puedan desempeñar muchas de las funciones asociadas a los ruteadores (seleccionar el camino óptimo a través de la red, proporcionar interfaces) LAN y WAN, y proporcionar seguridad interna, control de flujo y gestión del ancho de banda. Como resultado, los ruteadores evolucionan hacia dispositivos inter-red, cuya función principal es la conexión de múltiples LAN al conmutador ATM.

La manera más sencilla de hacer que un ruteador utilice ATM es hacer uso de PVC a través de la infraestructura de conmutación. Pero también se eliminan dos de las mejores ventajas del ATM: la conexión dinámica y la asignación de ancho de banda.

Aunque los ruteadores de inter-red son, hoy por hoy, los favoritos de los vendedores de equipos ATM, la mayor parte del sector sufre cierta agitación a causa de un nuevo tipo de ruteador denominado *ruteador virtual*. Éste combina un *servidor de encaminamiento* central con un cierto número de *conmutadores multicapa,* que son dispositivos de hardware casi tan rápidos como los conmutadores convencionales de la capa MAC, pero mucho más inteligentes que enlazan las LAN existentes. Los ruteadores convencionales constituyen cuellos de botella porque, calculan el camino independientemente para cada paquete, en cambio, en un ruteador virtual, la interconexión entre LAN se lleva a cabo en el conmutador multicapa.

El conmutador multicapa reenvía los datos utilizando los campos del paquete MAC o de la capa de red, sin gestionar la asignación de ruta ni los cambios de topología (de eso se ocupa el servidor de encaminamiento). Cada puerto del ruteador multicapa puede tener asignada su propia dirección de subred, tal y como sucede con los ruteadores convencionales. Y al igual que sucede con un ruteador de inter-red, varios puertos pueden compartir la misma dirección de subred.

El servidor de encaminamiento se encarga de ejecutar los protocolos de encaminamiento y de mantener una descripción clara de las topologías de inter-red y ATM, pudiendo actuar, incluso, como un servidor de difusión y resolver las peticiones de direcciones. En lo que respecta a las estaciones de usuario, el ruteador virtual se encarga de todas las funciones asociadas a un ruteador físico: proceso del protocolo, actuar como puente, encaminamiento y filtrado.

Dispositivos ATM para encaminamiento inter-red

Un dispositivo para *encaminamiento inter-red* es aquel que convierte paquetes de una LAN Ethernet o de anillo con testigo a las estructuras de celdas de ATM, y viceversa. Para transportar tráfico a través de la red de ATM los dispositivos de extremo en la red (inter-red) convierten los flujos de datos no ATM, en celdas. La incorporación de nuevos tipos de tráfico requiere la incorporación de nuevos dispositivos inter-red, a instalar donde exista demanda para ese tipo de tráfico.

El ruteador inter-red de ATM se aleja radicalmente de los ruteadores convencionales, que son productos constituidos a partir de multiprocesadores simétricos diseñados para manejar una carga equilibrada de tráfico entrante y saliente. Cada CPU está asignado a una función: cálculo y gestión del camino, establecimiento y gestión de la conexión de ATM o reenvío de datos. Los ruteadores inter-red, por otro lado, presentan un diseño asimétrico que permite crear a partir de una base inicial de conmutación un conjunto de pequeños ruteadores modulares, indefinidamente ampliables, que exploten el enorme ancho de banda y la redundancia de un soporte de ATM fuertemente entrelazado.

Los ruteadores inter-red también están diseñados de manera tal, que resuelvan el problema de latencia en los ruteadores convencionales. La latencia asociada a un ruteador multiprotocolo medio es bastante grande (variando desde los cientos hasta los miles de microsegundos) e impredecible. Los ruteadores inter-red se diseñan para latencias constantes de 50 microsegundos por dispositivo. Este rendimiento es equiparable a los del ATM, que son razonables para datos sensibles al retardo, tales como la voz o el video.

Probablemente el principal problema, y más difícil de abordar, de la migración hacia redes ATM sea la carencia de las gamas de productos. En la actualidad, pocos vendedores pueden proporcionar el equipo necesario para instalar una red ATM completa, razón por la que es necesario combinar productos de diversos vendedores, y la compatibilidad entre equipos (interoperabilidad) es prácticamente imposible. El mayor obstáculo es, la falta de una planificación concienzuda y sólida de una arquitectura ATM por parte de los vendedores.

La tecnología ATM es aún muy costosa, y la mayor parte de los segmentos de red no necesitan anchos de banda de 155 Mbps o 622 Mbps. Por tanto, la migración hacia una red conmutada debe considerarse un proceso compuesto por pasos evolutivos, según vayan apareciendo nuevas tecnologías. Así, que es conveniente planificar la implementación en fases: primero los soportes (backbones) (sobre todo los soportes de conjuntos de edificios), los segmentos que deban transmitir abundante video e, incluso, el tráfico de voz digitalizada de las centrales telefónicas (PBX).

La transición hacia ATM hará preciso tener en cuenta los juegos de protocolos, tanto de lugares específicos como a nivel de la red global.

Una aproximación incremental a la migración a ATM combina lo mejor de las distintas tecnologías mejorando de tres maneras la inversión en red existente:

1. El despliegue del ATM alarga la vida útil de la infraestructura existente de red, al incrementar considerablemente su rendimiento.
2. Al combinarlo con ciertas habilidades tales como la emulación de LAN, ATM mejora la gestión y el manejo de la red, permitiendo configuraciones de redes virtuales.
3. Las ampliaciones incrementales mantienen la inversión económica y el riesgo técnico a niveles bajos, mientras madura la tecnología ATM.

Las figuras siguientes muestran una manera de incorporar paulatinamente ATM, comenzando por la incorporación de un soporte ATM.

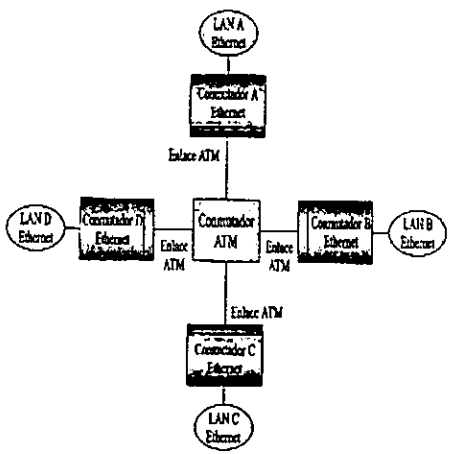


Figura 2.28. Paso 1

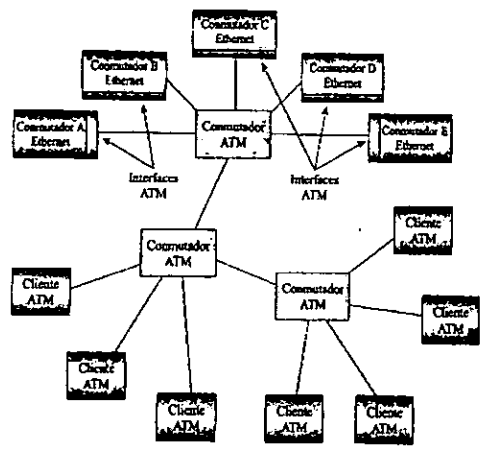


Figura 2.29. Paso 2

La planificación de la red pasa a incorporar segmentos de grupo de trabajo ATM, utilizando emulación de LAN para permitir que todos los usuarios de la red se comuniquen entre sí. Por último, un ruteador de soporte colapsado (un único ruteador de alto rendimiento) conecta múltiples segmentos en una red lógica.

Emulación LAN ATM (LANE: LAN Emulation)

El objetivo principal del servicio LANE es habilitar el acceso de las aplicaciones actuales, sobre una red ATM por medio de pilas de protocolos como IP, NetBIOS, IPX, etc., como si estuviesen sobre una red LAN tradicional. LANE trabaja al nivel de la subcapa MAC y habilita al tráfico de las redes heredadas Ethernet, Token Ring o FDDI, correr sobre ATM sin tener que modificar las aplicaciones, sistemas operativos de red o adaptadores de escritorio. Como su nombre lo indica, emula una red de área local tradicional (heredada) sobre una red ATM.

Este protocolo define mecanismos para emular de manera lógica un segmento de red local Ethernet (802.3) o Token Ring. Definiendo así, un servicio de interfaz para protocolos de capas superiores, con lo cual las estaciones finales de sistemas heredados pueden utilizar LANE para conectarse a otros sistemas heredados, como también a servidores conectados directamente a ATM, enrutadores, concentradores y otros dispositivos de red.

Funcionamiento de Emulación LAN

La función básica del protocolo LANE es la de resolver las direcciones MAC en direcciones ATM. Para esto, la emulación de LAN es conformada por una colección de servicios que trasladan la información entre los protocolos de las capas superiores (orientados a la no conexión) y los de capas inferiores (orientados a conexión). Cabe mencionarse que el protocolo actual de LANE no define una encapsulación individual para FDDI, por lo que un paquete FDDI debe ser mapeado dentro de una emulación de red LAN Ethernet o Token Ring. Las dos nuevas tecnologías en redes LAN; Fast Ethernet (100Base T) y 100VG-AnyLAN (IEEE 802.12) pueden ser mapeadas sin cambio dentro de los formatos y procedimientos LANE Ethernet y Token Ring, a partir de que ellos ocupan el mismo formato de datos.

Como se explicó anteriormente, ATM puede llevar múltiples tipos de tráfico y requiere de varios protocolos de adaptación, los cuales operan de manera simultánea (desde AAL-1 hasta AAL-5). Siendo AAL-5 el protocolo sobre el cuál trabaja la emulación LAN.

La emulación LAN se sitúa por encima del AAL-5 en la jerarquía de protocolos. En la conversión ATM a LAN al nivel de red, la emulación LAN resuelve los problemas de datos para todos los protocolos, ya sean enrutables o no. Es también, completamente independiente de los protocolos de capas superiores, servicios y aplicaciones.

Componentes de LANE

La especificación LANE esta basada en un modelo cliente servidor; una red LAN emulada se lleva a cabo en un servicio de emulación LAN y múltiples LECs comunicándose a través de un enlace llamado LUNI.

Una red LAN emulada es constituida por las siguientes entidades:

- *Cliente LANE (Cliente de Emulación de LAN o LEC)*

Un LEC es una combinación de agentes de software y hardware implantados; dentro de dispositivos de red o sistemas finales, para el manejo de envio de datos, resolución de direcciones, y otras funciones de control. También provee una interfaz de servicio de LAN estándar para cualquier protocolo de la capa superior del sistema final. Cada componente de red puede soportar múltiples instancias de un LEC, permitiendo de esta manera que múltiples redes LAN emuladas puedan existir simultáneamente sobre la misma red física.

Cada LEC es identificado por una dirección ATM única, la cuál es asociada con una o más direcciones MAC, las cuales pueden ser alcanzadas a través de la dirección ATM.

En el caso de una NIC ATM, por ejemplo, el LEC puede estar asociado con una sola dirección MAC, mientras en el caso de un conmutador de red LAN, el LEC debe estar asociado con todas las direcciones MAC que se pueden alcanzar a través de los puertos de ese conmutador de LAN, los cuales son asignados para una ELAN particular. Se debe notar que en el último caso, este conjunto de direcciones puede cambiar esto es, que tanto direcciones de nodos MAC pueden darse de alta/baja, como rutas particulares ser reconfiguradas ya sea por cambios lógicos o físicos en la topología de red LAN (por ejemplo, al utilizar el protocolo de árbol expandido o "Spanning tree").

Las especificaciones actuales de LANE definen dos tipos de redes LAN emuladas, una para Ethernet y otra para Token Ring, pero no permiten la conectividad directa entre un LEC que implanta a una y otro que implanta a la otra. Es decir, LANE no intenta resolver el problema de traducción (puenteo) entre tecnología. Los dos tipos de ELANs solo pueden ser interconectados a través de un enrutador ATM que actúe como un cliente de cada ELAN.

Existen dos tipos de LECs, proxy y no proxy.

Un **LEC proxy** es aquel que representa la dirección MAC de otros dispositivos además de la de él mismo. En otras palabras, actúa como un puente.

Un **LEC no-proxy** es un dispositivo como un anfitrión que tiene una dirección MAC única, es decir la dirección de él mismo solamente.

La versión 1.0 de LANE, permite a los servidores distinguir entre estos tipos de LECs, para agregar eficiencia en la resolución de direcciones. En este caso, el servidor mantiene dos árboles punto-a-multipunto, uno para LECs proxy y otro para LECs no-proxy. Los LECs se identifican así mismos como proxy y no proxy, cuando se conectan a una red LAN emulada.

Cuando llega un mensaje LE-ARP (LAN Emulation Address Resolution Protocol), el servidor (LES) verifica su tabla de direcciones y responde si encuentra el mapeo, con la dirección ATM apropiada. Si no encuentra el mapeo en sus tablas, el LES puede asumir que la dirección MAC está asociada a un LEC proxy. Éste entonces direcciona la petición hacia aquellas estaciones sobre el árbol punto-a-multipunto proxy para su resolución.

Servicio LANE

El servicio LANE consiste de tres entidades, un servidor de emulación LAN (LES), un servidor de broadcast y desconocido (BUS) y por último, un servidor de configuración (LECS). La especificación LANE no especifica algún lugar en especial donde deban estar localizados los tres servidores, cualquier dispositivo o dispositivos con conectividad ATM deberán ser suficientes. Aunque, por desempeño y eficacia, la mayoría de los proveedores implantan los componentes con funciones de servicio sobre los equipos de red, tales como conmutadores o enrutadores ATM, en lugar de estaciones.

- *Servidor de emulación de LAN (LES: LAN Emulation Server)*

La entidad LES, es el centro de control para una LAN emulada, ya que realiza el manejo de resolución de direcciones y control de información. Su primer tarea es la de registrar y resolver las direcciones MAC a direcciones ATM.

Existe solamente un LES lógico por cada red LAN emulada (ELAN), y para poder pertenecer a una ELAN particular significa tener un control de relación con ese servidor LES. El LES implanta la función de control para una ELAN particular. Cada LES es identificado por una dirección ATM única.

Todos los dispositivos registrados dentro de un mismo servidor LES llegan a ser parte de una misma ELAN. Esta red LAN emulada es esencialmente una capa MAC basada en una red LAN virtual, definiendo un dominio de broadcast común entre todas las estaciones finales registradas en un mismo servidor LES.

- *Servidor de Broadcast y Desconocido (BUS: Broadcast and Unknown Server)*

Este servidor está diseñado para ser multicast, el cuál, es usado para llevar tráfico hacia direcciones con destino desconocido, direccionar tráfico de broadcast y tráfico multicast, hacia clientes dentro de una ELAN particular.

Cada LEC está asociado con un sólo servidor BUS por ELAN pero pueden existir múltiples servidores BUS dentro de una ELAN particular.

Los servidores LES y BUS, trabajan conjuntamente para transferir tanto tráfico unibroadcast como de broadcast. Generalmente estos servidores son localizados dentro de un solo dispositivo.

- *Servidor de Configuración de Emulación de LAN (LECS: LAN Emulation Configuration Server)*

El servidor LECS, es una entidad que asigna clientes LANE individuales a redes LAN emuladas particulares. Esto se lleva a cabo, al dirigir a estos clientes hacia el LES que corresponde a una ELAN determinada. Además, mantiene una tabla de las asociaciones resultantes.

El LECS puede determinar la asignación de un LEC individual a una determinada ELAN, basado en la localización física del LEC (como se especifica en la dirección ATM del LEC) o por su asociación lógica (cuando se definen VLANs o redes virtuales). Es por esta razón, que el servidor LECS es generalmente configurado por el administrador de la red con la información inicial que indica a que red LAN virtual pertenece cada LEC (donde una LAN virtual corresponde a una ELAN).

Existe lógicamente un servidor LECS por dominio administrativo, y este sirve a todas las ELANs dentro de ese dominio.

Como se puede observar, el software que entrega el servicio de emulación LAN se encuentra implantado principalmente en estos servidores lógicos: LES, BUS y LECS.

Como funciona el servicio de Emulación LAN ATM

A continuación se explica como trabajan conjuntamente los diferentes componentes del LUNI para implantar la especificación LANE.

Iniciación y configuración

Al encender un dispositivo final (LEC), en principio se debe obtener la información de configuración (su propia dirección ATM) del servidor LECS para poder unirse a una red LAN emulada. El LEC entonces establece una conexión de configuración con el LECS.

Una vez que el LEC obtiene la dirección del servidor LES, establece una conexión directa (VCC) con él. Una vez hecho esto, el LES asigna al LEC con un identificador LEC único (LECID: LEC Identifier). El LES, entonces registra la dirección MAC y dirección ATM del cliente LEC. A partir de este momento, el cliente LEC puede resolver el mapeo de direcciones MAC a direcciones ATM.

Una vez conectados, el LEC le envía alguna información importante como es: su dirección ATM, su dirección MAC, su tipo de LAN y su máximo tamaño de frame. El servidor LECS responde con el tipo de LAN emulada actual (Ethernet o Token Ring), el tamaño máximo de frame actual, y la dirección ATM de un servidor LES (dependiendo si es por redes virtuales o por localización física).

La primera dirección que necesita el LEC es la dirección del servidor BUS, para lo cuál envía una petición de la dirección MAC con el valor de todos los bits en uno (dirección de broadcast) al servidor LES.

Cuando un LEC recibe un frame de datos unicast de las capas superiores para su transmisión, este primero verifica sus tablas locales para ver si conoce la dirección ATM asociada con la dirección MAC. Si no se encuentra en sus tablas locales, el LEC tiene entonces tres opciones:

- Puede emitir el frame hacia la red para inicializar la resolución de la dirección MAC a una dirección ATM.
- Puede retener el frame hasta que pueda aprender la dirección ATM del destino y establecer hasta entonces una conexión directa.
- Puede dirigir el frame hacia el servidor BUS para mantener los datos en movimiento. En este caso, el BUS responde en forma de servidor broadcast (envía el paquete hacia cada uno de los clientes de la red LAN emulada por medio de inundación). Esta opción se explica con detalle a continuación:

Cuando un LEC origen envía los frames hacia el servidor BUS, de manera simultánea, envía una petición LE-ARP hacia el servidor LES, tratando de que resuelva la dirección MAC desconocida. Si el LES reconoce este mapeo, puede contestar directamente sobre el Control Directo VCC al LEC origen. Si no reconoce el mapeo, éste redirige la petición hacia todos los clientes por medio de una conexión de control distribuido para solicitar una respuesta de un LEC que conozca la dirección MAC de la petición.

El destino, al reconocer su dirección MAC envía un LE-ARP de respuesta hacia el servidor LES, el cual incluye las direcciones ATM tanto del LEC originario de la petición como la del LEC destino. El servidor LES envía el mensaje de respuesta con la dirección ATM del destino hacia todos los LECs (en una modalidad de broadcast) para que todos los LECs puedan aprender esta dirección especial. El ciclo termina cuando el LEC fuente reconoce su propia dirección contenida en el mensaje de respuesta. En este punto, ha aprendido la dirección ATM de la dirección MAC desconocida y puede establecer una conexión directa con el LEC destino.

Generalmente, cualquier dirección MAC no conocida por el LES, deberá encontrarse sólo en un cliente LEC proxy (un concentrador o un puente) y no dentro de una tarjeta NIC ATM, y solamente los LECs que no son ATM (dispositivos detrás de un dispositivo proxy) necesitan necesariamente recibir LE-ARPs redirigidos por el dispositivo proxy. Para llevar esto a cabo, algunos dispositivos LECs pueden registrarse con el LES como un nodo "proxy", indicando que este puede ser alcanzado a través de otra dirección (la dirección del dispositivo LEC proxy). El LES entonces tiene la opción de establecer controles distribuidos VCCs de manera que los LE-ARPs sean solo enviados de tales LECs proxy.

Mientras el cliente LEC origen espera la respuesta de la petición del LE-ARP, el BUS correspondiente, por medio de inundación enviará paquetes hacia todos los LECs registrados. Esto debe realizarse, en el caso de un dispositivo pasivo se encuentre detrás de un conmutador LAN (LEC proxy). El procedimiento de inundación es análogo al utilizado por el mecanismo de árbol expandido usado por los puentes tradicionales para paquetes con destino desconocido, de aquí el nombre del servidor. Generalmente una vez que un paquete es inundado por medio del servidor BUS el destino responde con un LE-ARP de respuesta.

Si se recibe una respuesta al LE-ARP, el LEC puede establecer una conexión directa (VCC) hasta el nodo destino, y utilizarla para transferir los datos en lugar de la opción de inundación del servidor BUS. Antes de que se realice la conexión directa, el LEC origen necesita dar de baja la ruta de inundación del BUS y utiliza el procedimiento llamado "desecho" (flush) para asegurar que todos los paquetes previamente enviados por medio del BUS hayan sido entregados al destino y posteriormente se de baja el método de inundación, una vez realizado esto, se puede hacer uso de la nueva ruta con la conexión directa de datos. Este mecanismo se lleva a cabo para poder garantizar la preservación del orden de los frames.

Si no se recibe una respuesta del LE-ARP, el LEC continuará enviando paquetes vía el servidor BUS, y regularmente seguirá enviando peticiones de LE-ARP hasta que se reciba un LE-ARP de respuesta.

Cada LEC construye su propia tabla de direcciones MAC, direcciones ATM y conexiones VCC. Si una dirección MAC particular no ha estado activa durante algún tiempo, un LEC eventualmente desechará esta dirección de su tabla, es decir, cuando no existen direcciones MAC asociadas con una conexión VCC de datos directos, el LEC puede desechar la conexión.

Basándose en la versión 1.0 de LANE, todas las implantaciones de clientes LEC estandarizados son garantizados para interoperar, pero por otro lado, no existe una manera estandarizada por la cuál servidores de múltiples proveedores actualmente puedan intercomunicarse, la segunda versión de la emulación LAN (2.0 actualmente bajo desarrollo) definirá protocolos servidor-a-servidor que permitirán el trabajo conjunto de servidores multiproveedor incrementando la escalabilidad y robustez de LANE. Mientras tanto los administradores de redes deberán escoger sus funciones de servicio de un sólo vendedor para asegurar una amplia interoperabilidad ATM.

Múltiples redes LAN Emuladas

El estándar de emulación LAN del forum ATM, también soporta la implantación de múltiples redes LAN emuladas dentro de una sola red ATM. La emulación LAN está basada en el modelo cliente-servidor, cada cliente se conecta al servidor a través de una conexión virtual. Sólo aquellos clientes conectados al mismo servidor pueden aprender acerca de las otros clientes y comunicarse directamente. Lógicamente la segmentación de la red es a través de múltiples funciones de servidor (LECS, LES y BUS) los cuales pueden ser dispositivos en modo único (stand alone), o como software en los sistemas finales o en módulos de conmutador ATM. Permitiendo a múltiples redes LAN emuladas coexistir simultáneamente sobre la misma red física por tal motivo, la intercomunicación entre redes LAN emuladas requiere de un puente o enrutador convencional. Sin embargo, el protocolo LANE solamente define los mecanismos de operación dentro de una sola red LAN emulada (ELAN).

Una red *LAN Virtual* (VLAN) resulta cuando existen varios dominios LANE diferentes a través de uno o más conmutadores ATM. Esta red desarrolla grupos de trabajo más seguros y puede crear una protección contra ráfagas de broadcast para un mejor uso de la red.

Un mensaje de broadcast proveniente de un LEC, sólo puede alcanzar a otros LECs de la misma red VLAN, pero no a otros, de esta manera, estaciones finales que no pertenecen a la misma VLAN no desperdician recursos procesando datos no relacionados con su grupo de interés. Las redes Virtuales o VLANs simplifican la administración de la red al permitir la estructuración de grupos de trabajo, basándose en el interés común de los usuarios y no en la localización física de las computadoras. Los administradores de la red, pueden adicionar, mover, cambiar o simplemente redefinir la agrupación de los grupos de trabajo además de poder configurar los dispositivos finales a través de una sesión remota. Todo esto se lleva a cabo sin la necesidad de cambiar el sistema de cableado o adicionar nuevos dispositivos a la red.

Limitaciones de Múltiples redes LAN Emuladas

Como se puede observar, se requiere un número de conexiones VCCs para establecer y mantener una red LAN emulada. Cada LEC tiene conexiones VCC desde y hasta el servidor LES y el servidor BUS, las cuales pueden ser bidireccionales o unidireccionales en el peor caso (se requiere 4 conexiones unidireccionales por LEC).

Los servidores no son capaces de soportar un número infinito de VCCs, por tal motivo, existe un limite para el número de LECs que puede contener una red LAN emulada.

LANE 2.0 frente a LANE 1.0

LANE 2.0 fue desarrollado por el forum ATM específicamente para dirigir algunos de los defectos de LANE 1.0. Primeramente soportar QoS, grupos multicast y escalabilidad.

Esta especificación fue aprobada como estándar en julio de 1997 y esta constituida por dos estándares separados: la Interfaz de Usuario a Red LANE (LUNI) y la Interfaz de Red a Red LANE (LNNI). El estándar LUNI, tal como en LANE 1.0 define la operación del LEC y su operación con servicios LANE y otros LECs. El protocolo LNNI define un método que permite a múltiples entidades de servicio LANE comunicarse con alguna otra en una ELAN.

A diferencia de 1.0, LANE 2.0 permite que los servicios sean distribuidos a través de dispositivos múltiples en la misma ELAN. Lo que permite escalar el tamaño de una ELAN y la distribución de LANE al procesar múltiples dispositivos.

LANE 2.0 también agrega la habilidad de tener múltiples grupos multicast en una ELAN particular. Con LANE 1.0 solo hay un BUS, el cual se usa para la transmisión de todo broadcast, multicast y tráfico desconocido. Cada LEC recibe todo el trafico del BUS, esté o no interesado en él. LANE 2.0 permite Servidores Multicast en adición al estándar BUS de LANE.

Si un usuario quiere tener un servidor de video multicast en la red, podría ponerse en un grupo multicast selectivo. El grupo podría tener su propio Servidor Multicast Selectivo (SMS), y los LECs registrarían a miembros de este grupo al inicializarse. Solo los clientes registrados para recibir esa corriente de video por unión al grupo multicast, lo podrían recibir. El SMS provee una función multicast de la capa MAC.

En LANE 1.0, cada LEC crea un VC (canal o conexión virtual) directo de datos con cada uno de los otros LEC que se comunica en una ELAN. Esto es, cada LEC requiere tener su propio VC directo de datos, si dos dispositivos terminales tienen cada uno cinco LECs configurados a ellos, requerirán cinco VCs separados entre ellos. LANE 2.0 permite un VC directo de datos para usarse por múltiples LECs en un dispositivo final. Dos dispositivos extremos con cinco LECs cada uno podría solo requerir un VC entre ellos. Esta característica requiere un nuevo formato de encapsulación de frame para usarse por LANE 2.0 que no se usa en LANE 1.0.

La diferencia importante entre estos tipos de frame es la trama LLC de LANE 2.0 que incluye un campo de "ELAN-ID". Si se multiplexan las tramas de múltiples LECs en un simple VC, el dispositivo que recibe al final del VC solo necesita checar el campo ELAN ID para determinar cual LEC envió la(s) trama(s).

LANE 1.0 no soporta cualquier característica QoS; provee un servicio UBR estricto. LANE 2.0 provee localmente Servicio de Calidad (QoS) administrado para comunicación entre LECs. Los mecanismos del protocolo están provistos para determinar si un sistema final remoto es capaz de soportar un QoS deseado. Cada QoS definido localmente puede incluir un indicador de si un conjunto VCC con ese QoS puede compartirse con otros protocolos o aplicaciones.

LANE 2.0 permite al administrador de la red asignar por LEC parámetros QoS por arriba de ocho calidades de servicio. Su diseño se basa en la especificación 802.1p de IEEE, la cual define ocho niveles de prioridad.

Cada ELAN puede ser configurada con ocho conjuntos de parámetros QoS. Por ejemplo, cada nivel de prioridad pudiera ser asignado a una conexión de periodo de bit constante (CBR), variable (VBR), available (ABR) o no especificado (UBR) y podría definir los parámetros de trafico para cada uno.

Multiprotocolo Sobre ATM (MPOA)

Una vez que el forum ATM terminó su especificación de emulación LAN versión 1.0 (la cuál define como puentear tráfico proveniente de redes heredadas), puso su atención hacia como puede ser enrutado el tráfico sobre una red ATM.

Para esto se desarrolló el estándar referido como Multiprotocolo Sobre ATM (MPOA: Multiprotocol Over ATM) el cuál, es un método nativo de protocolo de interconectividad en red para sintetizar, enrutar y puentear tráfico de protocolos diversos sobre ambientes conmutados ATM. Es decir, provee métodos unificados para sobreponer los protocolos de capa 3 sobre ATM.

De acuerdo al documento, MPOA define una arquitectura de servidor de enrutamiento (arquitectura de enrutamiento virtual) en el cual los conmutadores consultarán una entidad de enrutamiento central cuando tengan la necesidad de conocer donde se deben enviar los datos. Para ello, el MPOA espera que definan varios protocolos diferentes, incluyendo un protocolo conmutador a servidor (comunicación entre el servidor de enrutamiento y el conmutador) y un protocolo interservidor (mantendrá la información en diferentes servidores de enrutamiento en la misma red).

Control de Flujo

La *congestión* es definida como el estado de elementos de red en el cuál, debido a la sobre carga de tráfico, la red no es capaz de garantizar una Calidad de Servicio (QoS) en las conexiones establecidas en el momento de la congestión, ni tampoco las nuevas peticiones de conexión. El control de flujo trata de minimizar los efectos de la congestión.

Cuando varios conmutadores ATM se enfrentan a la congestión, descartan celdas de acuerdo al parámetro CLP (Cell Loss Priority). La voz y el video no son tolerantes a la pérdida de celdas. Por otro lado, el tráfico de datos es más tolerante a la pérdida y retraso de datos, pero si las celdas que contienen información de un paquete de alto nivel son desechadas, el paquete entero, tiene que ser retransmitido. Considerando que los paquetes IP son 1500 bytes de largo y los paquetes FDDI son de 4500 bytes, la pérdida de una sola celda puede significar retransmisiones significantes, además de agravar más la congestión.

Es por esto que para redes ATM de mayor tamaño y que lleven diferente tipo de tráfico se hace necesario el manejo de mecanismos más sofisticados para el control de la congestión.

El forum ATM consideró dos enfoques. El primero, está basado en un esquema salto-a-salto con concesión-de-crédito (credit-granting), donde el conmutador o una estación final no pueden enviar celdas sobre una conexión dada, hasta que ésta le haya proporcionado el crédito de ancho de banda. Este enfoque no fue ampliamente aceptado por varios vendedores, ya que su implantación requeria utilizar nuevos chips, ocasionando que los conmutadores, actuales de ATM llegaran a ser obsoletos. El segundo enfoque, esta basado en un control de velocidad fin-a-fin. En éste, la celdas que pasan a través de un conmutador y que experimenten congestión serán marcadas con un bit en su encabezado. La estación destino observará el status de este bit y enviará una celda especial de regreso a la estación fuente, ocasionando que esta, retarde o acelere el envío de las celdas. Esto es fácil de implantar en los conmutadores, pero aumenta la tarea de procesamiento en las estaciones terminales.

2.6.7 ATM y voz

Aunque se resalta el hecho de que ATM es un sistema válido para el transporte de tráfico de voz, se ha progresado muy poco en el desarrollo de tecnología ATM orientada a este fin. Por el momento no existe un protocolo de capa de adaptación ATM optimizado para el manejo de tráfico de voz. Los protocolos AAL existentes manejan el tráfico vocal de forma muy poco eficiente. Tanto que de hecho, las redes Tl/T3 basadas en el estándar de multiplexación por división en el tiempo son capaces de transportar a menudo muchas más conexiones de voz que las redes ATM Tl/T3. Así, salvo que haya contemplado el costoso paso a SONET (las interfaces le proporcionarán un ancho de banda tan grande que probablemente no vuelva a pensar en ATM), es mejor esperar un poco para implementar ATM para voz.

2.6.8 Aspectos de la migración hacia ATM

Es posible que la instalación de ATM requiera cambios importantes en el diseño y equipamiento de la red. Los conceptos y reglas que rigen el ATM son muy distintos de los utilizados en la mayor parte de los protocolos de redes de área local o extensa. Si el objetivo final del ATM es servir a las redes públicas de área extensa, va a ser necesario utilizar direcciones largas para acomodar a los millones de dispositivos potenciales de una red pública. Como resultado, habrá que desarrollar un esquema que permita traducir las direcciones cortas de las redes de área local a las direcciones largas de ATM. También existe un problema de compatibilidad entre equipos (interoperabilidad): los productos de ATM de vendedores distintos no funcionan de manera conjunta, y las LAN de ATM tienen capacidad limitada para interactuar con otros protocolos de LAN. La instalación y configuración, entre otros, obstaculizan la interconexión entre ATM y redes LAN existentes. Saber estos aspectos es preciso para asegurarse de adoptar la solución adecuada, tanto a corto como a largo plazo. Por tanto, cualquier integración y/o migración de protocolos de red heredados hacia entornos conmutados ATM, dedicados y orientados a conexión requerirá una cuidadosa planificación.

Especificaciones de interfaces incompletas

Aunque UNI dispone de una especificación bien fundamentada y estable, el foro de ATM debe aún especificar y estandarizar otras interfaces que aseguren la compatibilidad entre equipos de las redes ATM. La interfaz red-red para redes privadas o P-NNI, es una de esas interfaces.

La P-NNI es todavía inestable y en gran manera sigue asociada a cada fabricante, encargándose del arbitrio de las conexiones virtuales, el control de congestión y gestión de la topología. Sin una definición estable de la P-NNI, los fabricantes no pueden desarrollar equipos ATM que garanticen una compatibilidad suficiente entre equipos.

Emulación de LAN

La integración de protocolos en uso tales como Ethernet, anillo con testigo y FDDI constituye un gran obstáculo para la aceptación generalizada de ATM en entornos de LAN. Siendo un protocolo extremo a extremo, orientado a conexión, ATM no admite tal cual los mecanismos de trabajo de los protocolos de LAN heredados.

Las redes Ethernet instaladas no van a desaparecer a corto plazo. De hecho, continuará creciendo durante algún tiempo, sobre todo a causa de su bajo costo, alta estandarización, extensiones con otras tecnologías (como conmutadores Ethernet) y el gran número de instalaciones en funcionamiento. Por tanto, resulta obvio el hecho de que, salvo que se proporcione un esquema que permita integrar el parque de redes existente, el ATM seguirá siendo un nicho tecnológico sólo para bolsillos aislados o para usuarios muy avanzados.

La emulación de LAN en ATM es la tecnología de migración que permite que las estaciones que ejecutan aplicaciones existentes incluso aquellas que requieren características propias de protocolos heredados se adapten a los servicios de ATM. La emulación de LAN consiste en un programa que emula el funcionamiento de una red de área local convencional. Proporciona un puente entre los protocolos de LAN heredados y los segmentos de ATM. La emulación de LAN es enrevesada, ya que el ATM se comporta en muchos aspectos de manera muy distinta a como lo hacen los protocolos de transporte de LAN más convencionales. Además, las estaciones de ATM tendrán que proporcionar mecanismos para las operaciones de difusión y multi-difusión que habitualmente se utilizan en Ethernet y anillos con testigo. Adicionalmente, el ATM utiliza un esquema de direccionamiento de 20 bytes, mientras que Ethernet y los anillos con testigo utilizan direcciones MAC de 48 bits. Ésta es la razón por la que la emulación debe resolver la diferencia entre direcciones MAC y ATM.

Lo que hace que la emulación de LAN falle

Hay muchos aspectos que dificultan la implementación de emulaciones de LAN. Entre ellos puede citarse

- Resolución de direcciones.
- Admisión de difusión y multi-difusión.
- Velocidad.
- Establecimiento de la conexión.

Para proporcionar el rendimiento necesario para enlazar satisfactoriamente redes heredadas y ATM es necesario que los dispositivos de emulación de LAN realicen la conversión y conmutación a velocidades equivalentes a las de transmisión.

Como ya se mencionó anteriormente, ATM es un servicio de transporte orientado a la conexión. Los protocolos de LAN heredados, por otro lado, son no orientados a conexión, lo que significa que envían los paquetes conteniendo la dirección completa del receptor, y sin establecer primero una conexión. La estación receptora supervisa todos los paquetes transmitidos sobre el medio y acepta los que están dirigidos a ella. Con tan sólo 5 bytes de cabecera, las celdas ATM no pueden albergar la dirección completa en cada celda. Por esta razón, adaptar los protocolos de red existentes, que requieren la dirección de destino completa, al ATM, orientado a conexión y que utiliza conmutación de celdas, representa un gran reto.

La interfaz LUNI se ha desarrollado para dar solución a este problema de compatibilidad entre equipos. El protocolo LUNI permite que la red ATM y los dispositivos de inter-red controlen las conexiones virtuales necesarias para la transmisión, así como la emulación no orientada a conexión de una LAN.

Aspectos de la migración aplicables al equipo de usuario

Aunque el ATM se considera principalmente como una solución para los enlaces de soporte, la mayor parte de las redes ATM son hoy en día grupos de trabajo en los que las estaciones y los servidores se conectan directamente a un conmutador ATM. Aunque generalmente estos grupos de trabajo son pequeños y están geográficamente centralizados, lo que simplifica la implementación, quedan aún ciertos puntos a considerar como los siguientes:

- **Medios compatibles**

Revisar la infraestructura de red actual ya que la mayor parte de los productos comerciales ATM funcionan con fibra multimodo y par trenzado de cobre, sin blindar, de categoría 5, a velocidades de entre 25 Mbps y 155 Mbps. A causa de sus características de atenuación, la distancia máxima para el cable de categoría 5 es de unos 100 metros. La fibra multimodo, sin embargo, permite conexiones con longitudes máximas, de 2000 metros. Debe pues, asegurarse que las necesidades de cableado satisfacen estos requisitos.

- **Compatibilidad con las aplicaciones**

Al ser ATM un protocolo de bajo nivel, las aplicaciones que ya se tienen pueden ejecutarse sobre una red ATM. La mayoría de las veces, estas aplicaciones utilizan TCP/IP o, si son para PC, Novell NetWare o Windows de Microsoft. Para obtener el máximo rendimiento del ATM se deben elegir, siempre que sea posible, aplicaciones que saquen el máximo provecho de las habilidades de ATM en lo que respecta al ancho de banda dedicado y la asignación de prioridades a los datos.

- **Compatibilidad con las computadoras**

En un grupo de trabajo ATM cada estación de trabajo debe disponer de una tarjeta de interfaz de red (NIC) ATM. La NIC tiene que ser compatible con el bus de la estación de trabajo, así como con la propia estación y su sistema operativo de red. Es importante que la tarjeta NIC se haya probado con anterioridad, tanto con el tipo de estación de trabajo como con los conmutadores ATM que se vayan a utilizar.

2.6.9 Aspectos de integración en WAN

Aunque es posible, con cierta frecuencia, integrar ATM en redes de área extensa (WAN) sin sustituir ningún equipo, se tendrá que contar con algún equipo adicional, conocimiento profundo de las interfaces ATM en juego y una cuidadosa planificación.

Hay cuatro puntos fundamentales necesarios para una correcta interconexión en área extensa, que son:

- Interfaz pública usuario-red (UNI).
- Interfaz pública red-red (NNI).
- Interfaz entre compañías de telecomunicaciones (ICI).
- Interfaz para intercambio de datos (DXI).

Interfaz pública usuario-red (UNI)

Como ya se mencionó anteriormente, el protocolo UNI de ATM proporciona diferentes tipos de servicios y modos de reserva del ancho de banda durante el establecimiento de conexiones virtuales conmutadas. Define la compatibilidad entre equipos; entre el equipo del usuario y el puerto del conmutador ATM. Una UNI pública define la interfaz entre una red ATM de uso público, y suele ir ligada a interfaces tales como SONET o DS3, constituyendo el enlace entre el usuario y el conmutador de la red pública ATM de la compañía de telecomunicaciones.

Interfaz pública red-red (NNI)

Como también mencionamos anteriormente, el protocolo NNI proporciona un mecanismo de arbitrio de la conexión virtual, control de congestión y gestión de la topología en conexiones a redes ATM públicas o privadas. Constituye el enlace entre los conmutadores ATM de un servicio de transporte de datos en una red ATM pública.

Interfaz entre compañías de telecomunicaciones (ICI)

El protocolo ICI define los mecanismos de interconexión en redes ATM de área extensa, permitiendo establecer enlaces entre redes ATM de dos compañías distintas.

Interfaz para intercambio de datos (DXI)

El protocolo DXI proporciona una interfaz ATM estándar para los equipos heredados, admitiendo el encaminamiento en ATM al estar basado en paquetes en vez de celdas.

Al utilizar, a diferencia de las interfaces basadas en celdas, tramas del estándar HDLC (control del enlace de datos de alto nivel), no necesita hardware adicional para cursar tráfico de paquetes. Por tanto, es el protocolo que permite conectar el equipo existente a una red ATM.

Para ilustrar cómo afecta cada una de las interfaces descritas a la implementación de una red ATM, podemos hacer uso de la figura 2.30, donde se muestra cómo se puede integrar un enlace de soporte ATM de área extensa en una red FDDI y 10BASE-T ya existente.

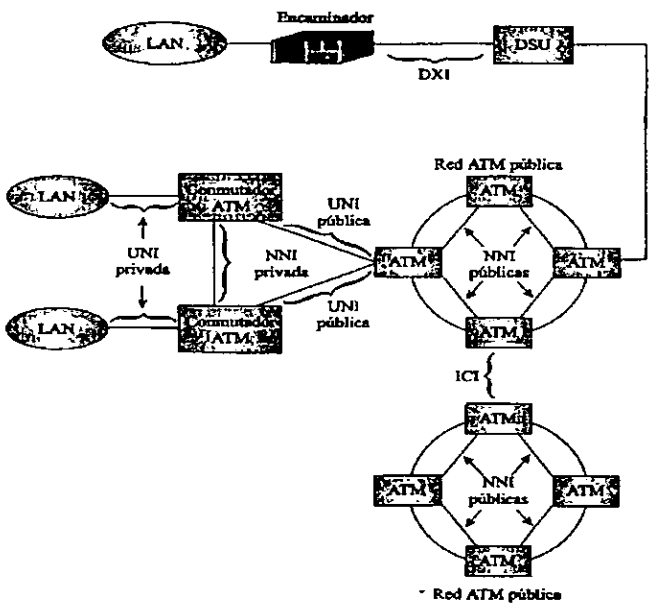


Figura 2.30

El ancho de banda asociado al soporte de la red FDDI es de 100 Mbps, compartido por todos los dispositivos conectados a él. El conmutador ATM de área extensa mostrado en la figura 2.30 tiene ocho puertos, cada uno de 155 Mbps. Como los 155 Mbps están asignados a cada dispositivo conectado, el ancho de banda total es 8 veces 155 Mbps o aproximadamente, 1.2 Gbps. En realidad, el ancho de banda total de este ejemplo estará entre 155 Mbps y 1.1Gbps, en función del tipo de tráfico y su utilización.

Tanto en el ruteador FDDI como en el conmutador 10BASE-T se instaló una UNI de ATM, para que ambos dispositivos pudiesen conectarse al conmutador ATM. La conexión WAN al conmutador ATM se realiza a través de una interfaz para intercambio de datos (DXI) con el servicio de multiplexación, que típicamente toma la forma de una CSU/CDU especial. Gracias a la DXI, además de multiplexar el tráfico cursado por el enlace de área extensa, el servicio de multiplexación lleva a cabo las tareas de segmentación y reensamblado del AAL, permitiendo así que los dispositivos no ATM accedan al nuevo hardware ATM de la red.

2.6.10 Facilidad de ampliación

El ATM puede añadir facilidad de ampliación a los protocolos de red heredados. Más aún, según aumenta el número de usuarios y conmutadores, una fracción mayor de la capacidad de conmutación se destina a los enlaces de soporte, antes que a los enlaces de interfaz con los equipos de usuario.

Los conmutadores ATM ampliables para LAN, disponibles actualmente en el mercado, pueden soportar hasta 100 puertos de 155 Mbps en configuración sin bloqueo. Junto con dispositivos de acceso a Ethernet dedicados, los conmutadores proporcionan los cimientos necesarios para una red de 1000 usuarios Ethernet en modo sin bloqueo. Según madure el mercado de ATM, se conseguirán redes de 1000 puertos de 155 Mbps, 10,000 puertos Ethernet sin bloqueo. La necesidad de redes sin bloqueo o de conexiones extremo a extremo de alta velocidad no es imprescindible para justificar la utilización de ATM. Aunque el máximo beneficio del ATM se obtiene en configuraciones LAN sin bloqueo, también puede utilizarse en configuraciones con bloqueo para maximizar el aprovechamiento del ancho de banda.

En una configuración con bloqueo, la suma de los anchos de banda de los puertos excede el ancho de banda del enlace de soporte, y puede presentarse contención en dicho enlace. Al instalar ATM, es posible que la carga de procesamiento de las estaciones de trabajo con que se cuenta no haga uso de la totalidad del ancho de banda disponible. En tal caso, pueden conectarse a la red más usuarios de los que la capacidad del enlace de soporte podría admitir en una configuración sin bloqueo. Cuando comiencen a aparecer aplicaciones para estaciones de trabajo que consuman un gran ancho de banda, tanto el ancho de banda como la capacidad de conmutación pueden ajustarse para dar lugar a una configuración sin bloqueo. Una red ATM con bloqueo puede superar ampliamente el rendimiento de una LAN que comparta el medio, si se combina con técnicas de gestión de tráfico adecuadas.

2.6.11 Facilidad de administración

Los soportes de ATM resultan más fáciles de administrar que los habituales en la mayoría de las redes con encaminamiento, ya que el ATM elimina la mayor parte de la complejidad involucrada en la configuración de las grandes redes interconectadas entre sí, que presentan diferentes esquemas de direccionamiento y procedimientos de encaminamiento. Los concentradores (hubs) ATM proporcionan conexiones entre dos puertos cualesquiera del concentrador, con independencia del tipo de dispositivo conectado a él. La dirección de los dispositivos está preasignada, facilitando así el envío de un mensaje. De hecho, la gestión de red simplificada puede ser la razón fundamental por la que muchos usuarios migren a soluciones basadas en ATM, incluso antes de tener en cuenta los requisitos de rendimiento.

2.6.12 Otros aspectos a tener en cuenta

Implementar un soporte con ATM implica considerar muchos aspectos puestos en juego por los demás protocolos, tales como: Seguridad, tolerancia a fallos, requisitos de ancho de banda y sistemas de administración.

A la hora de implementar una red ATM de área extensa, uno de los mayores retos que se puede afrontar es la localización de una compañía de telecomunicaciones que proporcione ATM a un precio razonable. Aunque la mayor parte de los proveedores de servicios digitales ofrecen ATM, su disponibilidad no está del todo generalizada a causa de la falta de demanda.

Las principales compañías de telecomunicaciones reconocen que el ATM es, definitivamente, el futuro en temas de conexión de redes de área extensa, y entienden que elimina las barreras entre LAN y WAN. Sin embargo, no todas las compañías de telecomunicaciones locales (LEC) ni las compañías de interconexión (IXC) han instalado redes digitales ATM/SONET integradas con el fin de proporcionar servicios de red privada de datos a un costo razonable. Y cuando lo hagan, puede suponerse que cargarán los elevados costos de instalación de las nuevas redes al consumidor. Las buenas noticias son que el ATM transporta más tráfico con costos reducidos, lo que traerá, un cierto ahorro para el usuario. Pero eso puede tardar algún tiempo.

Podemos decir que el conjunto ATM representa una excelente promesa para casi cualquier red. Proporciona *rendimiento y funcionalidad* antes nunca vistas para:

- Transferencia electrónica de dinero.
- Anotaciones de voz y memorándum.
- Videos didácticos interactivos.
- Desarrollos en diseño y fabricación, en los que se implique objetos de datos complejos que residan en procesadores distintos y geográficamente dispersos.

Recomendado para:

- Aplicaciones de video y multimedia, por su capacidad de asignar anchos de banda dedicados a las aplicaciones y de asignar prioridades a los datos.
- Soportes, por su facilidad de ampliación, alto rendimiento y seguridad.
- Redes de área extensa, por su capacidad de integrar sin esfuerzo WAN y LAN, con alto rendimiento.
- Redes muy dispersas, por la ausencia de limitaciones de distancia.

No recomendado para:

- Redes pequeñas, por su alto costo.
- Redes que deben mantener la infraestructura existente de protocolos de red heredada, por la carencia actual de interfaces estándar para la integración de protocolos diversos en ATM.

Puntos fuertes:

- Alto rendimiento.
- Facilidad de ampliación.
- Ancho de banda dedicado.
- Potencialmente desplegable con carácter universal.
- Seguridad.

Puntos débiles:

- Compatibilidad entre equipos (por el momento).
- Alto costo.
- Moderada tolerancia a fallos.

Probablemente el ATM sea el futuro tanto en protocolos de transporte como en interconexión de redes en general. Como ya se ha dicho, muchos vendedores se han apresurado a proclamar sus planes para sistemas y productos ATM pero, al escribir estas líneas, simplemente no hay sistemas completos disponibles, abiertos, viables y con compatibilidad entre diferentes equipos basados en ATM.

2.7 RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI)

Los primeros estándares de RDSI que definían las interfaces digitales de extremo a extremo aparecieron en 1984, presentados por el CCITT, quien emitió estándares de definición adicionales en 1988. La RDSI estaba considerada como un avance fundamental por un par de razones. En primer lugar, especificaba servicios de red digital que se entregarían sobre las redes telefónicas digitales integradas ya existentes. Segundo, ofrecía un rendimiento máximo de 2 Mbps en el enlace local y 64 Kbps o 128 Kbps en el área extensa. En el momento de comenzar a emerger la RDSI de banda estrecha, el tope de velocidad de los módems analógicos era de 9,600 bps.

Actualmente RDSI se considera una manera rentable de proporcionar:
- Acceso remoto a usuarios que llaman a las LAN de sus compañías.
- Un enlace adecuado para algunas conexiones de LAN a LAN.
- Tráfico de fax entre centrales de ancho de banda elevado.
- Acceso de alta velocidad a Internet.

La RDSI es un servicio flexible que conmuta automáticamente entre dispositivos distintos conectados a él. Por ejemplo, proporciona servicios digitales a un teléfono, una máquina de fax o una PC, los cuales se pueden conectar a la misma interfaz de RDSI. La RDSI también se puede utilizar como enlace de acceso local a redes de retransmisión de tramas (frame relay) y X.25.

La RDSI es un servicio que se compone de dos tipos de canales: *canales de portadora* y *canales de señalización*. Uno para transmitir datos y el otro para manejar la señalización de administración y el control de llamada respectivamente. Los proveedores de RDSI han combinado estos dos tipos de canales para construir dos tipos diferentes de ofertas de servicio de RDSI: la *Interfaz de velocidad básica* y *la Interfaz de velocidad primaria.*

Canales de portadora

Los canales de portadora, o canales B, sólo transportan datos de usuario; de ahí el nombre de "portadora", a través de la red RDSI. Los canales B son canales de conmutación de circuitos de 64 Kbps del mismo tipo que el utilizado en una llamada de teléfono de voz normal, aunque los canales B de RDSI son digitales en vez de los

analógicos utilizados en el servicio telefónico básico antiguo (POTS). Los canales B se toman durante la llamada y después se liberan cuando se termina la misma. Pueden conectar dos locales de RDSI cualesquiera.

Canales de señalización

El canal de señalización o canal D está separado de los canales B, proporcionando señalización fuera de banda para establecer, controlar y liberar las llamadas. Debido a que esta señalización se realiza en un canal separado, las llamadas se establecen mucho más rápido que si la información de señalización tuviese que compartir ancho de banda con los datos reales. Por ejemplo, el canal D proporciona a la red el número del destinatario mientras los datos esperan ser transmitidos en los canales B. Por lo tanto, en cuanto se establezca la llamada, puede comenzar la transmisión. La señalización del canal D es una función de las capas: física, de enlace y la de red en relación con el modelo OSI, como se muestra en la figura 2.31.

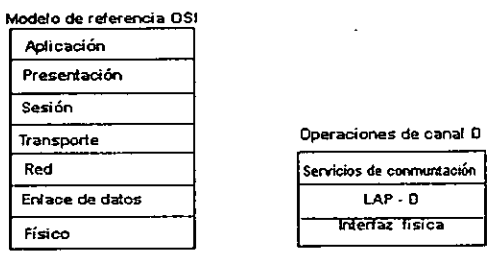


Figura 2.31

A continuación se describirá brevemente el funcionamiento de los protocolos de señalización de canal D dentro del modelo de referencia OSI.

Funciones de la capa física

El protocolo de la capa física de RDSI establece una conexión de conmutación de circuitos a 64 Kbps. También define la interfaz física para el *adaptador de terminal de red,* que se mencionará un poco más adelante, y que soporta, la conexión de múltiples dispositivos simultáneamente. Este protocolo gestiona las funciones de prueba y de supervisión de circuitos.

Funciones de la capa de enlace de datos

Este protocolo establece los trayectos virtuales de las tramas de datos a través de las redes. Gestiona también las funciones de control de llamada y señalización a través del *procedimiento de acceso al enlace para canal D* (LAP-D), que es el procedimiento que funciona a través de la señalización, o canal D.

Funciones de la capa de red

El protocolo de esta capa maneja todos los servicios de conmutación de circuitos y de conmutación de paquetes. La capa de red crea la información de direccionamiento y de determinación de camino que utiliza la capa de enlace de datos para establecer los trayectos virtuales.

Como ya se ha mencionado, los proveedores de RDSI han desarrollado dos ofertas de servicio estándar, o *interfaces de velocidad.* Llamadas individualmente como, Interfaz de velocidad básica (BRI, Basic Rate Interface) e Interfaz de velocidad primaria (PRI, Primary Rate Interface).

2.7.1 Interfaz de velocidad básica de RDSI

La Interfaz de velocidad básica (BRI) consta habitualmente de dos canales B a 64 Kbps para transmisión de datos, más un canal D a 16 Kbps que proporciona la señalización para los canales B. Con el equipo adecuado, se puede unir los dos canales B de la BRI para obtener un ancho de banda máximo de 128 Kbps. Por lo tanto, la BRI es adecuada para conectar oficinas pequeñas, redes de área local de tamaño pequeño a mediano o para usuarios que trabajen en casa y se quieran conectar a la LAN de su compañía.

Aunque hemos dicho que la BRI consta, habitualmente de dos canales B a 64 Kbps. Algunos proveedores de RDSI ofrecen BRI con un canal B y un canal D, o con sólo un canal D. El canal D proporciona la señalización de fuera de banda que define realmente la RDSI y convierte al servicio en lo que es.

2.7.2 Interfaz de velocidad primaria de RDSI

Los canales de la Interfaz de velocidad primaria (PRI) están disponibles para los clientes de RDSI que necesiten más ancho de banda del que puede proporcionar una BRI. Se basan en la velocidad de DS 1 de 1544 Mbps e incluyen 23 canales B y un canal D a 64 Kbps para realizar la señalización. Los canales B se pueden agrupar en una de las configuraciones siguientes, conocidas en la terminología de las compañías de telecomunicaciones de central local como *servicios H*:

Canal H. Este tipo de canales son funcionalmente equivalentes a los canales B pero operan a velocidades mayores de 64 Kbps. La función principal es la de transmitir la información del usuario que requiere tasas mayores a 64 Kbps y un poco más de 100 Mbps, como por ejemplo, video digital y audio a alta velocidad, resolución para televisión, teleconferencia, transferencia de archivos a alta velocidad, etc. Existen varios tipos de canal H, los cuales se muestran en la siguiente tabla:

Canal	Tasa de transmisión (Kbps)	Tasa múltiplo de canales B	Tasa múltiplo de canales H0
H0	384	6	1
H10	1472	24	4
H11	1536	24	4
H12	1920	30	5
H21	32768	512	-
H22	44160	690	115
H4	135168	2112	352

Las líneas se pueden utilizar como enlaces de alta velocidad para transferir archivos grandes y otras secuencias continuas de datos o se pueden subdividir con un multiplexor para proporcionar canales para dispositivos múltiples. Al proporcionar una gran variedad de opciones de servicio, la PRI se puede configurar para que maneje video comprimido, videoteléfonos y teleservicios.

La RDSI y su equipo de apoyo realizan realmente gran parte del procesamiento y señalización de datos que solían ser responsabilidad exclusiva del equipo de la central principal del proveedor. El transferir estas funciones desde la central principal a una PC es una de las causas de gran dificultad y confusión a la hora de pedir, configurar y localizar averías en la RDSI. Por lo tanto, se hace necesario hablar de las funciones en cuestión: lo que son, lo que se les ha hecho tradicionalmente y cómo la RDSI ha cambiado todo eso.

Una llamada de *servicio telefónico básico antiguo (POTS)*, es el tipo de llamada analógica que hemos realizado y recibido casi todos desde que somos capaces de marcar un teléfono, no requiere demasiado del equipo situado en nuestros hogares.

Todo el procesamiento de voz y datos tiene lugar en el conmutador de la central principal del proveedor local. Nuestros teléfonos analógicos simplemente se ponen en contacto con el conmutador de la compañía telefónica y le dicen a quién queremos llamar y el conmutador hace el resto. En esencia, nuestros teléfonos analógicos no son mucho más que amplificadores con teclados.

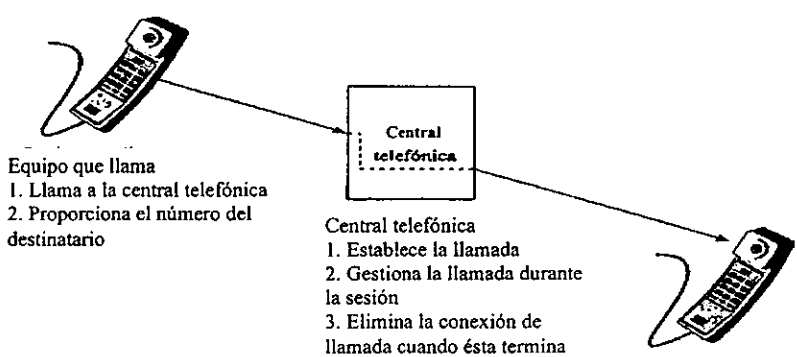


Figura 2.32. Servicio telefónico básico antiguo (POTS)

Por el contrario, una llamada de RDSI requiere que el equipo del local del cliente sea mucho más sofisticado. Los teléfonos de RDSI y adaptadores de PC deben ser capaces de procesar información y determinar qué tipo de señal (voz, datos, fax, etc) se está recibiendo, y responder encaminando los datos al dispositivo adecuado. La figura 2.33, muestra el camino de una llamada de RDSI desde su local hasta su destino, pasando por la red pública conmutada.

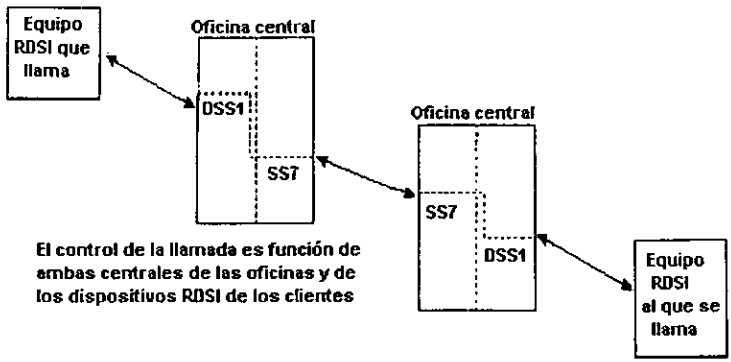


Figura 2.33

Primero se establece la llamada cuando el equipo establece una conexión con el conmutador de la central utilizando el *Sistema 1 de señalización de abonado digital* (DSS1: Digital Subscriber Signaling System 1).

Una vez que se ha establecido la llamada entre su local y la central mediante DSS1, se establece la siguiente etapa del viaje. La señalización que se necesita para encaminar la llamada dentro de la red pública conmutada no es DSS1. En su lugar, las compañías telefónicas públicas utilizan un sistema llamado *Sistema 7 de señalización* (SS7: Signaling System 7), que puede manejar tanto llamadas digitales como analógicas. Por lo tanto, en la compañía telefónica las instrucciones de DSS1 se convierten en señales SS7. El SS7 es un conmutador en modo de paquete que gestiona el control de llamada, incluyendo el establecimiento y la liberación de la llamada.

Cuando la llamada llega a la última central de su camino, se convierte a su formato DSS1 original para su transmisión desde dicha central a su destino final, el "equipo" con el que quería comunicarse. En este caso, se necesita que el equipo local de RDSI interactúe con DSS1 y SS7, algo que nunca se requirió ni se diseñó en el teléfono POTS. Es esta interacción con dos sistemas de señalización externos grandes y complejos la que ocasiona muchas de las pesadillas de configuración asociadas con el pedido, instalación y utilización de RDSI.

Hay un requisito de DSS1 que requiere conocer los detalles de DSS1 y SS7 mientras se utilice RDSI. Es un *Identificador de perfil de servicio* (SPID: Service Profile Identifier). Los SPID son números de identificación asignados a su línea de RDSI en el momento en que es establecida por proveedor de la central local. Es muy importante recibir este número y guardarlo en un sitio seguro, porque al configurar el equipo correspondiente se requerirá la introducción de un SPID. Como se puede ver, el SPID identifica los procesos lógicos individuales conectados a la interfaz de RDSI y evita la contención entre procesos diferentes en el bus de RDSI en el caso de que se reciban llamadas mientras un dispositivo está utilizando activamente el canal B. Éste es el procedimiento en DSS1 que le permite conectar varios dispositivos a una línea de RDSI. Además, el SPID, junto con otro parámetro requerido por DSS1, el *identificador de terminal* (TEI), identifican el equipo de RDSI real conectado a la interfaz de RDSI.

Un solo TEI podría tener múltiples SPID asociados a él. La negociación entre los SPID es difícil y complicada, tanto, que a algunos proveedores de RDSI les ha parecido más sencillo el admitir la contención de bus, y por lo tanto permitir sólo un SPID en cada canal de portadora.

2.7.3 Servicios de RDSI

Los servicios proporcionados por la RDSI operan en niveles de protocolo superiores a los de las conexiones telefónicas simples. Estos servicios utilizan los canales B para transmitir y el canal D para señalización. Enseguida se describen brevemente estos servicios.

- **Servicios de portadora**

Son los servicios que transportan los datos de extremo a extremo. Son de dos tipos:

1. En modo circuito.
2. En modo paquete.

Modo circuito frente a modo paquete

El *modo circuito* es bastante parecido a la conmutación de circuitos convencional. En él, se establece una conexión entre el equipo que llama y el llamado, y el circuito permanece dedicado a esa conversación hasta que una de las partes desconecta. Las dos partes son las únicas que, pueden utilizar la conexión mientras mantienen la llamada. Incluso si no se están transmitiendo datos, durante la llamada, todo el ancho de banda asociado a ese circuito está dedicado a esa llamada. Esto puede ser un desperdicio, dado que muchas conversaciones son fundamentalmente "aire muerto".

El *modo paquete* resuelve el problema del ancho de banda dedicado y sin utilizar. Este divide una sola conversación en fragmentos pequeños, da a cada uno de estos fragmentos una dirección y un número de secuencia, y los envía a través del cable (junto con paquetes de muchas otras conversaciones). Debido a que cada paquete tiene su propia dirección, puede compartir ancho de banda con otros paquetes sin mezclar las transmisiones de datos. Además, cada paquete podría seguir un camino diferente hasta el equipo llamado. Esto se muestra en la figura 2.34.

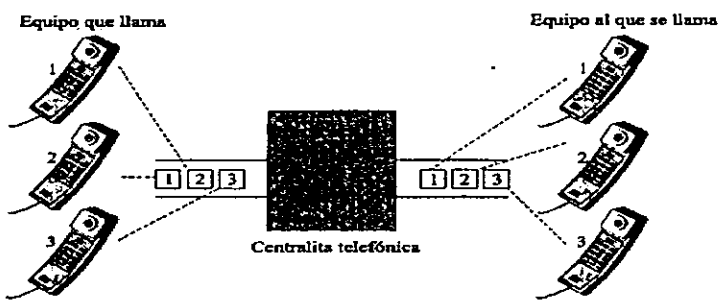


Figura 2.34

La transmisión en modo paquete no malgasta tanto como el modo circuito, ya que varias conversaciones utilizan la misma conexión. Por lo tanto, cuando una conversación no está transmitiendo nada, las otras conversaciones que comparten la conexión pueden utilizar ese ancho de banda libre para transmitir más datos propios. Finalmente, eso significa que la compañía de telecomunicaciones necesita menos equipo de conmutación de paquetes que de circuitos para admitir el mismo número de conversaciones.

Los servicios de portadora de RDSI ofrecen tanto, servicios en modo circuito como en modo paquete. El modo circuito utiliza canales B para transmitir los datos y el canal D para controlar la llamada. El modo paquete puede utilizar tanto los canales B como los D para transmitir datos. Generalmente, los servicios en modo circuito son mejores para tráfico de voz y los servicios en modo paquete para tráfico de datos, pero esto no siempre es cierto. Los servicios de portadora en modo paquete de RDSI ofrecen un servicio de circuito virtual que puede manejar muy bien tráfico analógico, como de voz.

- **Servicios suplementarios**

Estos servicios suplementarios son servicios que se añaden a los servicios de portadora que proporcionan una funcionalidad añadida. Pueden variar de un proveedor de RDSI a otro, por lo que ésta es sólo, una lista representativa de los tipos de servicio que se pueden encontrar:

1. **Presentación de la identificación de la línea que llama.** Es similar al "ID del que llama" que está disponible cada vez más para las llamadas entrantes en la mayoría de los sistemas telefónicos públicos. Identifica el número del equipo entrante.

2. **Número de equipo múltiple.** Este servicio asigna un número de teléfono distinto a cada dispositivo conectado a la interfaz de RDSI. Por ejemplo, suponga que tiene un teléfono, un módem y un dispositivo de fax en una interfaz de RDSI. Con este servicio, cada uno de ellos tendrá su propio número de teléfono. Por tanto, cuando llega una llamada para el teléfono, es éste el que suena, si es para el fax, es éste el que responde y con el módem pasa lo mismo.

Es importante mencionar que en RDSI, a los números de teléfono se les conoce como números de directorio o DNs.

Oferta de llamada

Son servicios como la transferencia de llamada y reenvío de llamada que le permiten controlar a dónde va la llamada después de llamar a su número. Este servicio comprende lo siguiente:

- **Transferencia de llamada**. Servicio similar a una PBX. Cuando se contesta una llamada, y se necesita enviarla a otra persona, ésta se le puede transferir.

- **Reenvío de llamada si está ocupado**. Este servicio permite que las llamadas sean dirigidas a otro número si llegan cuando está ocupado el teléfono.

- **Búsqueda de línea**. Conocido en el mundo de las PBX como grupo de búsqueda, la búsqueda de llamada define un grupo de teléfonos que pueden contestar cualquier llamada que llegue a algún teléfono del grupo. Esto permite que una llamada entrante llame (de teléfono en teléfono) a cada teléfono del grupo hasta que le contesten.

- **Espera de llamada**. A diferencia del POTS familiar, cuando llega una llamada a la línea de RDSI, no se interrumpe la conversación. Esto se debe a que la señalización se realiza en el canal D por separado (a eso se debe que el canal D sea tan importante). Esto es útil especialmente cuando se utiliza el módem ya que las llamadas entrantes no interrumpirán la conexión de datos, es decir, se puede mantener la espera de llamada mientras se utiliza el módem.

- **Retención de llamada RDSI**. Permite retener múltiples llamadas simultáneamente sin asignar una conexión distinta a cada una. RDSI también ofrece la multiconferencia.

- **Teleservicios**

Los teleservicios son servicios sofisticados que la RDSI puede proporcionar porque funcionan en capas superiores en el modelo de referencia OSI. Aunque no se utilizan demasiado actualmente en México, a menudo se les considera la dirección futura de la RDSI. Algunos de los teleservicios son:

- **Telefax**.- Permite fax de grupo 4 que utiliza información digital a 64 Kbps.
- **Teletexto**.- Proporciona mensajería de extremo a extremo entre dos dispositivos utilizando conjuntos de caracteres normalizados.
- **Videotexto**.- Mejora los servicios de teletexto añadiendo un buzón de correo, de texto y gráficos.
- **Videotelefonía**.- Proporciona un servicio de transmisión de televisión sobre la RDSI.

2.7.4 Implementación de RDSI en una red de área local

Lo primero a verificar antes de la implementación, es si se cuenta con una compañía telefónica que proporcione el conmutador RDSI. En caso de que si lo haya es necesario conocer cómo se implementa la RDSI en el conmutador para poder configurar los dispositivos de la red para que se comuniquen con él. La clave de cómo está implementada la RDSI en el conmutador, está contenida en dos informaciones que se deben obtener de la LEC (Local Exchange Carrier):

1. Qué protocolo de RDSI (NI-1 o NI-2) utilizan.
2. Qué tipo de conmutador de RDSI tienen.

Protocolos nacionales RDSI-1 (NI-1) y RDSI-2 (NI-2)

El protocolo NI-1 es el protocolo de BRI utilizado por la Regional Bell Operating Companies (RBOC). Como tal, permite que todos los dispositivos que cumplen con NI-1 se conecten a cualquier conmutador que sea compatible con este mismo protocolo. Está surgiendo, en EEUU, una versión más moderna del protocolo, llamada NI-2.

Si los dispositivos de RDSI y el conmutador del proveedor admiten el protocolo, NI-1 o el NI-2, entonces esa es toda la información de compatibilidad que se necesitará. Sin embargo, hay que tomar en cuenta que NI-1 es utilizado fundamentalmente por la RBOC. Puede ser que otras LEC no utilicen este protocolo, y por tanto, para configurar un dispositivo de RDSI para que se comunique con el conmutador, se necesitará conocer el fabricante del conmutador. Como sabemos en México, los servicios digitales apenas se introdujeron. Por lo que habría una serie de complicaciones al querer implementar una red RDSI.

Una vez comprobado lo anterior, el siguiente punto a considerar es el cableado, que va ir desde el conmutador de RDSI de la LEC hasta la instalación donde se ubique la red local. Si fuese posible, el acceso local sería mediante un cable de fibra óptica. Sin embargo, es bastante probable que los accesos sean a base de cobre debido al alto costo de la fibra. En este caso, el cable de acceso local de par trenzado no debe tener más de 5.4 kilómetros de longitud. Si supera esta longitud, la compañía telefónica puede instalar un repetidor de medio alcance entre la central y la instalación propia. Este repetidor regenera la señal de RDSI y duplica la distancia permitida entre la central y la instalación.

Aunque el conjunto de cables de acceso local cumpla estas especificaciones, puede que no esté preparado para RDSI. Esto regularmente se debe a que el cable local puede tener conexiones que salgan de él. A estas conexiones se les llaman *puentes de conexión* y se supone que no deberían estar ahí, pero a veces, cuando la compañía telefónica instala un cliente nuevo, despliegan una línea desde la instalación del cliente y la une, o conecta, a un registro local sin utilizar que halla sido abandonado por un antiguo cliente, como, se muestra en la figura 2.35.

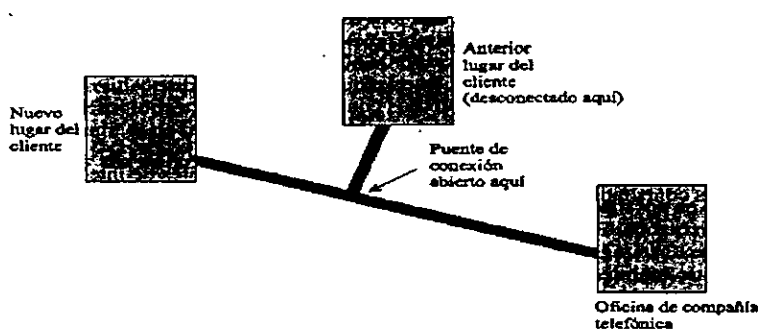


Figura 2.35

La derivación del antiguo cliente está desconectada de su emplazamiento, pero todavía está unida a lo que ahora es el nuevo registro local. Dichas derivaciones pueden provocar distorsiones de señal que habitualmente no afectan a las señales analógicas, pero afectan drásticamente con RDSI. Por lo tanto, se deben eliminar los puentes de conexión.

Una vez hecho esto, la LEC tendrá que verificar su línea para eliminar los dispositivos que estuviesen instalados para acondicionar líneas analógicas. El acondicionamiento supone un ajuste de las líneas para reducir la distorsión de la señal. Desafortunadamente, las técnicas que reducen esta distorsión para señales analógicas realmente pueden provocar distorsión en señales digitales.

Finalmente, el LEC verificará la línea nueva para ver si cumple las especificaciones de RDSI. Si lo hace, está lista para llevar a cabo las conexiones. Si no, la compañía telefónica tendrá que instalar otra línea.

Suponiendo que la compañía telefónica local sea capaz de proporcionar servicios de RDSI a la instalación, el paso siguiente es seleccionar el equipo adecuado para utilizar ese servicio. Se necesitarán principalmente dos equipos: un *adaptador de terminal de red* (NTA, network terminal adapter) y un *adaptador o un puente de RDSI.*

Adaptador de terminal de red

Un NTA es un dispositivo que conecta su equipo de datos o telefónico a la línea de RDSI de la compañía telefónica de central local. En EEUU, por ejemplo, es el cliente el que compra e instala el NTA, mientras que en otros países incluyendo el nuestro, es la compañía telefónica la que lo posee y mantiene.

El NTA conecta tanto el *equipo de terminal* (TE) como el *adaptador de terminal* (TA) al cableado local. Los dispositivos TE son equipos como teléfonos y computadoras que satisfacen RDSI. Los TA son interfaces como los adaptadores que conectan equipo que no es de RDSI al servicio RDSI.

En EEUU, el NTA está conectado al servicio de RDSI de la compañía telefónica local a través de la *interfaz U.* El equipo del cliente se conecta. al NTA a través de una *interfaz S/T,* que se describe más adelante, y que permite que se conecten y se direccionen hasta ocho dispositivos con el dispositivo NTA. La figura 2.36 muestra el dispositivo NTA y los 8 puntos de conexión posibles para los dispositivos TE y TA.

Figura 2.36

Es importante saber que no todos los dispositivos de NTA son iguales. Puede que algunos tengan sólo dos conectores; uno, para equipos de datos y otro para un teléfono. Si hay dispositivos adicionales, se encadenan en margarita.

El equipo de NTA proporciona tres tipos diferentes de interfaces para los dispositivos conectados. Se describen aquí:

1. **Interfaz U.** Esta interfaz transmite información dúplex en un único par de cable. Esto significa que la información viaja en ambas direcciones simultáneamente. La interfaz U sólo admite un dispositivo.
2. **Interfaz S/T.** Esta interfaz divide la señal de RDSI en dos trayectos: transmisión y recepción. Cada señal se transporta en un par distinto, y se pueden conectar dispositivos múltiples.
3. **Interfaz R.** Esta interfaz permite la conexión de un teléfono de POTS a su servicio de RDSI. El teléfono funcionará, pero no proporcionará todas las características de un teléfono de RDSI conectado, a una interfaz S/T.

Adaptadores de RDSI

Los adaptadores de terminal de RDSI, llamados habitualmente, módems de RDSI, pueden ser modelos internos o externos, igual que los módems analógicos. Y estos dos modelos tienen los mismos beneficios y desventajas que sus primos analógicos: los módems internos admiten velocidades de transferencia de datos superiores, mientras que los externos proporcionan más información de diagnóstico y control.

Si se selecciona un adaptador de terminal de RDSI que se conecta a una computadora a través de un puerto serie, se hará necesaria la instalación de un controlador de puerto serie que sea compatible con el mayor ancho de banda de RDSI. En caso contrario, el puerto, serie se convertirá en un cuello de botella, y todo ese ancho de banda extra por el que se está pagando será inútil. Por ejemplo, la velocidad de datos por puerto serie más alta admitida por Microsoft Windows para Trabajo en grupo 3.11 es de 19,200 bps (considerablemente por debajo de los 64 Kbps habituales de RDSI). Hay varios controladores de alta velocidad para puertos serie tanto en el mercado comercial como de libre distribución, como TurboCom/2 de Pacific CommWare.

Por otra parte algunos de estos adaptadores tienen dispositivos de NTA integrados, lo que puede ahorrar algo de dinero, además de tiempo y problemas cuando se configuren los dispositivos por primera vez. Sin embargo, también puede limitar el número de dispositivos que se pueden conectar a la línea de RDSI, al número de puertos S/T que suministra el vendedor del adaptador a menudo muchos menos que los proporcionados por NTA externos.

No todos los adaptadores de terminal de RDSI admiten más de un canal B. Si se piensa contratar más de un canal B, primero hay que asegurarse de que el adaptador de terminal de red lo admita. Además, se debe comprobar que el equipo seleccionado pueda puentear canales B múltiples si se espera aprovechar la ventaja del ancho de banda posible de 128 Kbps o más, combinando los canales de portadora.

El servicio de RDSI requerirá teléfonos de RDSI, a no ser que su adaptador de terminal tenga una *interfaz R,* que admite los teléfonos analógicos estándar. También se pueden utilizar adaptadores extras, que convertirán los teléfonos analógicos existentes en teléfonos de RDSI. Sin embargo, no hay que olvidar que los teléfonos analógicos no pueden aprovechar las ventajas de algunos servicios especiales de RDSI, como la ID del que llama.

La instalación de RDSI en LAN requiere que haya un puente o ruteador con una interfaz RDSI, como se muestra en la figura 2.37.

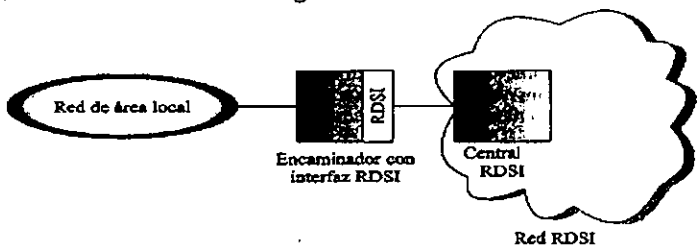


Figura 2.37

Entre los vendedores de ruteadores que ofrecen actualmente interfaces de RDSI destacamos a Cisco y Ascend. El ruteador está conectado directamente al cable de RDSI, por lo que debe estar configurado para encaminar tráfico a los segmentos adecuados e interactuar con la red RDSI. Esto implica muchas de las tareas de la configuración de una PC autónoma, incluyendo los SPID y DN correctos.

Configuración e instalación

Ahora que la conectividad a RDSI se está abaratando y está más disponible, compañías de todos los tamaños la están instalando debido a su ancho de banda mejorado y, por lo tanto, mayor funcionalidad, que ofrece sobre la gran variedad de líneas a 56 Kbps.

Sin embargo, la implementación de RDSI no es tan simple como lo era la instalación de esas líneas a 56 Kbps. Los aspectos a considerar antes, durante y después de la instalación de la RDSI son los siguientes:

- *En primer lugar: pedir lo que se desea*

Dado que no todas las compañías telefónicas de central local ofrecen RDSI, y no todas pueden ofrecer el tipo de RDSI que se necesita en la implementación, lo primero que se tiene que determinar es qué características de RDSI se necesitan y después asegurarse de que la compañía telefónica de central local pueda proporcionarlos. Así mismo es muy conveniente hacer una lista de todas las aplicaciones que consumen ancho de banda y que se desean implementar. Esto, será vital para seleccionar el servicio de RDSI que se necesita. Así mismo, la interfaz de velocidad (BRI o PRI) que se elija dependerá completamente, del número de conexiones y la cantidad de ancho de banda que se necesite.

Muchos usuarios de RDSI veteranos piensan que el componente de RDSI más pequeño que mantiene las propiedades de la RDSI es la BRI: dos canales B y un canal D. Eso no es verdad, la molécula real de la RDSI es un único canal D. Por tanto, para una BRI, se podrían tener dos canales B y uno D, o un canal D y uno B o simplemente un canal D. Esto proporciona la posibilidad de ampliar la conexión de RDSI para satisfacer todas las necesidades. Además, como ya se dijo, la PRI tiene anchos de banda distintos, como son:

- 384 Kbps (6 canales B).
- 1.472 Mbps (24 canales B a 56 Kbps).
- 1.536 Mbps (24 canales B).
- 1.92 Mbps (30 canales B).

Una vez decidido cuántos canales pedir, se necesita encontrar qué modo de transmisión de datos va a utilizar cada canal. Como ya se dijo, los servicios de RDSI pueden ser en modo circuito o en modo paquete. En el momento de escribir estas líneas, la RDSI ofrecía 10 servicios en modo circuito distintos y 3 en modo paquete (y se pretendía incrementarlos), cada uno de ellos diseñado para transmitir un tipo distinto de datos. Generalmente, se prefieren los servicios en modo circuito para voz y otras transmisiones analógicas, mientras que los servicios en modo paquete están más adaptados para los datos. Sería conveniente que en el momento de la implementación se contacte a un encargado de RDSI para que explique con detalle cada tipo de servicio de portadora que ofrece, y así seleccionar el más adecuado.

Una vez considerado y decidido lo anterior, es el momento de llamar a la compañía telefónica para pedir la RDSI. Es muy importante recordar que antes de implementar RDSI se debe investigar si hay alguna compañía que provea este tipo de servicio.

Una vez encontrado el servicio, puede que el encargado de recibir los pedidos le diga que el servicio de RDSI disponible es de 56 Kbps. Aunque esto no es realmente RDSI, no es necesariamente malo. Este servicio a 56 Kbps es RDSI, adaptado para funcionar en los sistemas TI existentes de la LEC, y se ofrece por lo general en sitios donde todavía no se dispone de RDSI completa a 64 Kbps. Los protocolos de RDSI populares pueden utilizar el servicio a 56 Kbps hasta que se disponga del servicio completo a 64 Kbps, por lo que no es necesario evitarlo simplemente porque no sea lo mejor.

Además, mientras se habla con el encargado de recibir los pedidos de la LEC, puede que éste utilice un término del tipo de *conjuntos de líneas*. Un conjunto de líneas es un término utilizado por el foro de usuarios de RDSI nacionales (NIUF) para describir las diferentes combinaciones de canales B (de 0 a 2) con el canal D y los tipos de información (datos en modo circuito, datos en modo paquete y/o voz) que desee transmitir sobre estos canales. Por ejemplo, el conjunto de líneas 1 no tiene canales B y sí un canal D en el cual se pueden transmitir datos en modo paquete. El conjunto de líneas 6 tiene un canal B en el cual se puede transmitir voz y un canal D para transmitir datos en modo paquete. Las diversas combinaciones de canales y tipos de llamada están identificadas por un número, y actualmente existen los conjuntos de líneas que van desde 1 al 29. Para evitar tener que memorizar todos los números de conjunto de líneas y sus descripciones correspondientes, simplemente se puede decir al encargado cuántos canales B y D se desean, y qué tipo de información se quiere transmitir sobre ellos. El encargado también deberá preguntarle por los *conjuntos de características*. Como hemos mencionado, un conjunto de características es otro término del NIUF que describe una combinación de servicios de datos en modo circuito o modo paquete y/o los servicios de gestión. Al menos hay 10 conjuntos de características diferentes, que lo detallan todo, desde la velocidad de productividad de datos a opciones de reenvío de llamada. Por tanto es conveniente pedir al encargado que nos proporcione la última información acerca de los conjuntos de características disponibles, y estudiarlos para realizar la elección.

Finalmente, después de haber seleccionado el número de canales, el tipo(s) de llamada que se van a admitir esos canales y las características e interfaces deseadas, se habrá terminado el proceso del encargo. La LEC local deberá enviar una carta o formulario confirmando el pedido y especificando los servicios contenidos en él, incluyendo también el número(s) de teléfono de la nueva conexión(es), además de algo llamado número de identificación de perfil de servicio (SPID). Es importante anotar estos números y guardarlos bien para el momento de configurar el equipo de RDSI.

- *Consideraciones de cableado*

El cableado de RDSI utiliza ocho clavijas, como se muestra en la figura 2.38.

Figura 2.38

Por lo tanto requiere conectores RJ-45. Además, el cableado de RDSI es directo, por lo que, se requieren cables de RDSI especiales para conectar los adaptadores de RDSI y/o puentes para el jack de RDSI.

- *Rendimiento*

La RDSI realmente no tiene un rendimiento de alta velocidad tan bueno. El ancho de banda disponible máximo en una BRI es de 128 Kbps, sólo en el caso de que ésta incluya dos canales B y que el equipo a conectar y los proveedores del servicio admitan el puenteado de dos canales juntos. El ancho de banda disponible máximo a través de una PRI es de 1.92 Mbps, por medio del canal H12, que consta de 30 canales B y un canal D a 64 Kbps. De nuevo, el equipo y todos los participantes (la compañía telefónica de central local, el proveedor de software de acceso y el cliente) deben admitir el puenteado de los canales B.

El estándar de RDSI de banda ancha admitirá velocidades de transmisión de datos de hasta 622 Mbps. Sin embargo, todavía no se ha terminado este estándar, por lo que el tope de RDSI permanece en la velocidad de RDSI de banda estrecha: 1.92 Mbps.

- *Administración y tolerancia a fallos*

Aunque RDSI, por su propia naturaleza, proporciona muchos servicios diferentes de administración de llamadas y de control, la administración del servicio de RDSI en sí está completamente en manos de la compañía telefónica. Por lo tanto, el optimizar y localizar errores en un servicio de RDSI es una tarea tediosa y a menudo sin resultados positivos que involucran al proveedor del servicio. En cuanto a la tolerancia a fallos, puede ser que el proveedor de RDSI sólo tenga un conmutador preparado para RDSI en cada zona. Si es así, cuando algo vaya mal en ese conmutador, no habrá servicio hasta que se repare.

- *Facilidad de ampliación*

RDSI es probablemente el protocolo de alta velocidad de área extensa más fácil de ampliar. Con el equipo y los servicios adecuados, se puede ampliar partiendo de una conexión de módem a 14.4 Kbps hasta 1.92 Mbps. Sin embargo, el configurar el equipo y los servicios para que admitan esta ampliación no es nada simple, y a veces simplemente no es posible obtener la cooperación necesaria de los vendedores para hacerla realidad.

- *Disponibilidad y precio*

La RDSI está disponible actualmente en la mayoría de las zonas metropolitanas principales, y su disponibilidad se está extendiendo con rapidez. A medida que aumente dicha disponibilidad, los precios de las tarjetas de PC para RDSI caerán drásticamente. Ahora ya se puede conseguir un módem de RDSI con un NT-1 incorporado por 200 dólares aproximadamente.

El precio de los servicios de RDSI varía mucho. En ciertas zonas, durante promociones especiales dirigidas por la compañía telefónica, la instalación de RDSI es gratis. En otras zonas, durante momentos de tarifas máximas, la instalación de RDSI puede costar hasta 400 dólares por línea. Las tarifas mensuales varían mucho también, desde 30 hasta 100 dólares por línea y por mes.

2.7.5 El futuro de RDSI de banda ancha

El ITU-T está trabajando actualmente en las especificaciones del modelo de RDSI de banda ancha, que se muestra a continuación:

Figura 2.39

El ITU-T entregará hasta 622.08 Mbps de transmisión de datos dúplex. Estas velocidades de datos elevadas admitirán transmisiones interactivas bidireccionales, difusión multimedia de almacenamiento y reenvío y servicios de mensajería y recuperación multimedia.

El estándar RDSI-B es también la base para ATM, parece que ATM y RDSI-B son la dirección en la que van las redes de voz y datos completas.

Ventajas

RDSI es un protocolo fácil de ampliar y de costo asumible. En las zonas en las que está disponible, puede ser bastante barato de implementar y ampliar.

Desventajas

RDSI tiene algunas desventajas principales que superar ya que simplemente el pedir servicios de RDSI requiere un nivel de experiencia que la mayoría de los administradores de red ocupados no tienen tiempo de desarrollar. El convertirse en un experto de la instalación y configuración de los dispositivos de RDSI, especialmente en zonas de LEC distintas, normalmente no es una opción para la mayoría de los administradores de red. Eso implica la contratación de integradores y consultores, y a su vez, eso significa un gasto adicional elevado. Además, el conseguir la cooperación de varios vendedores y proveedores puede ser difícil. A pesar de la larga historia de la RDSI, todavía no es muy conocida por el personal técnico de muchos proveedores. Puede pasar un tiempo antes de que las compañías telefónicas de central local puedan entrenar a sus empleados para que proporcionen el nivel de servicio en pedidos, selección, instalación y localización de averías que, requieren la mayoría de los administradores de red.

El ancho de banda máximo de la RDSI de banda estrecha también tiene un límite bastante inferior al de otros protocolos de área extensa de alta velocidad prometedores, por lo que puede ser una parada intermedia en el camino hacia protocolos como ATM.

Así, RDSI se recomienda para:

- Acceso a Internet.
- Multimedia.
- Tráfico de voz y datos combinado.

Y no es recomendado para:

- Tráfico sólo de voz (hay opciones más simples y baratas).
- Tráfico sólo de datos (ya que hay otras opciones más simples y baratas).

3.- ESTADO ACTUAL DE LA RED DEL INSTITUTO DE INGENIERÍA

3.1 DESCRIPCIÓN DE LA ORGANIZACIÓN ACTUAL DE LA RED

3.1.1 Estado del backbone de la red del Instituto

Actualmente la red del Instituto de Ingeniería trabaja en base a una tecnología Ethernet 10BASE-T, con topología física de estrella, usando como centro de la estrella un equipo MMAC-5 de Cabletron Systems que da cabida a todas las conexiones de fibra provenientes de los edificios enlazados en la red. El esquema de cableado de fibra tiene una configuración de anillo a través de 3 pares de fibras ópticas multimodo entre la conexión de los edificios que conforman el backbone, la estructura del cableado, esquemáticamente está como se muestra en la figura 3.1.

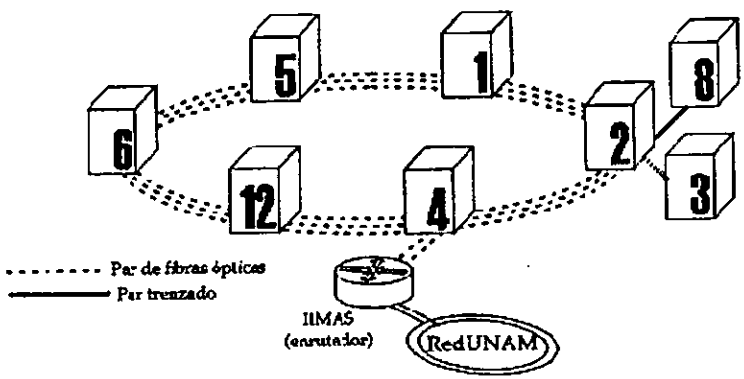


Figura 3.1

Como podemos ver en la figura, se cuenta con un enlace entre los edificios 1, 2, 4, 12, 6 y 5 quienes conforman el anillo principal, además del edificio 2, salen dos ramas que proporcionan señal a los edificios 3 y 8. El servicio que se da al edificio 8 es mediante cable par trenzado de cobre (UTP), ya que en este edificio hay una densidad de nodos de red muy pequeña y no se justifica un enlace de fibra óptica, además de que dada su ubicación física, esto es, que se encuentra muy cerca del edificio 2 no hay ningún problema al usar UTP. Por su parte el ramal del edificio 3, sí usa un par de fibras ópticas multimodo, ya que ahí existe una mayor concentración de nodos. Además de lo anterior, cabe señalar que dichos nodos se encuentran divididos en dos secciones una parte en el ala frontal y otra en el ala posterior del edificio, por lo que la distancia de UTP excedería los 100 metros permitidos y acarrearía problemas en la transmisión de datos, debido a esta situación se optó por instalar fibra óptica.

En el siguiente plano (figura 3.2) podemos ver de una manera más real, la ubicación de los edificios y la ruta que sigue la fibra óptica.

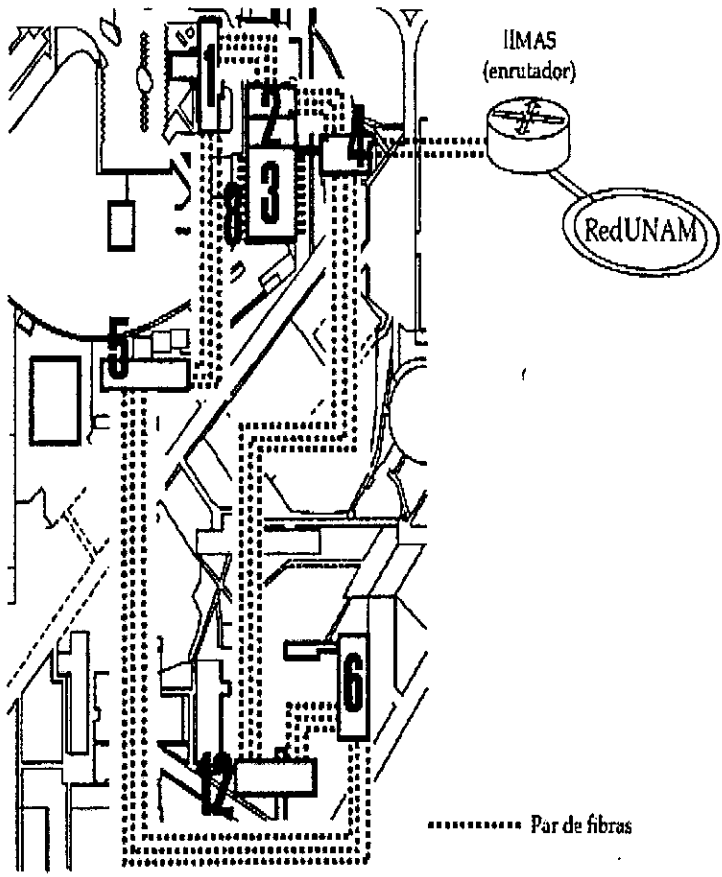
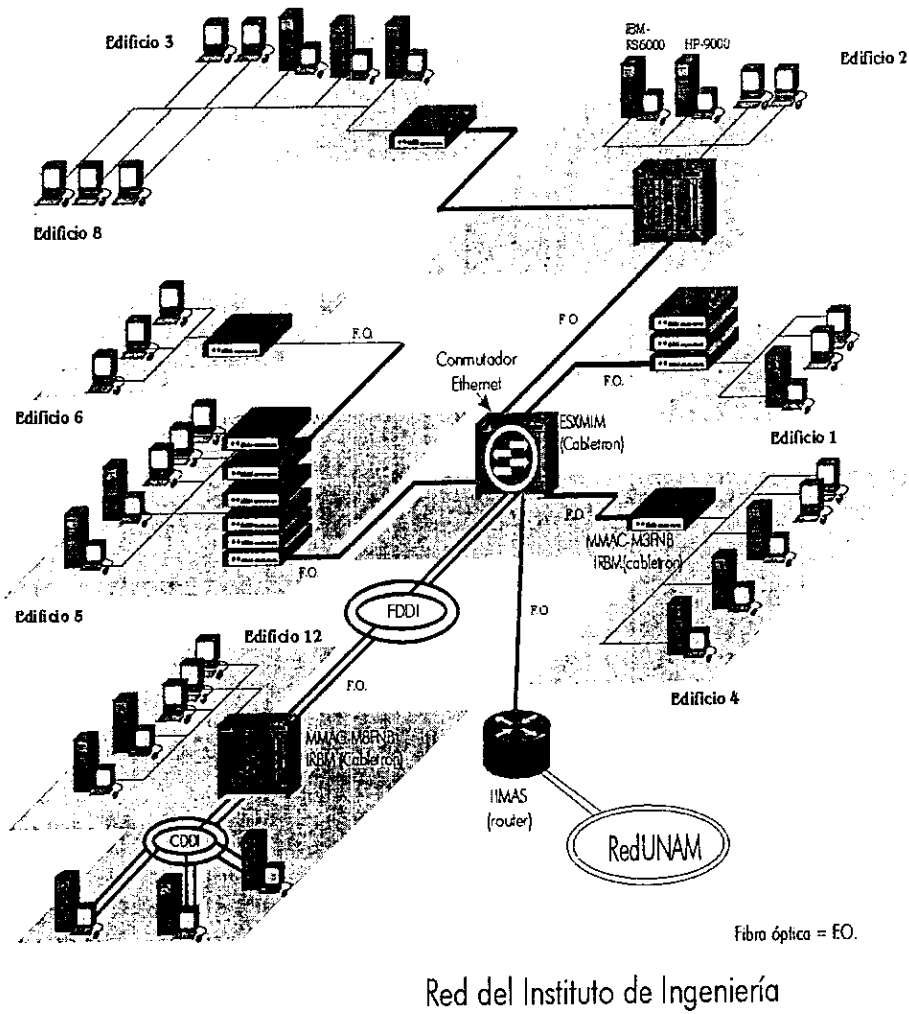


Figura 3.2

Siguiendo con el esquema del backbone principal, y como se mencionó anteriormente, la configuración potencial del cableado de fibra permite formar un anillo, sin embargo, dado que no se utilizan todas las fibras en todas las secciones del anillo, en realidad se tiene un esquema de estrella tal y como se muestra en el figura 3.3.



Red del Instituto de Ingeniería

Figura 3.3

La ubicación de los registros bajo los cuales va el tendido de cable rudo de fibra óptica, se muestra en el plano siguiente (figura 3.4), la numeración de los registros, sólo es una sugerencia del recorrido a seguir para revisar físicamente el tendido así como para dar una idea del número de registros por los que pasa el cableado.

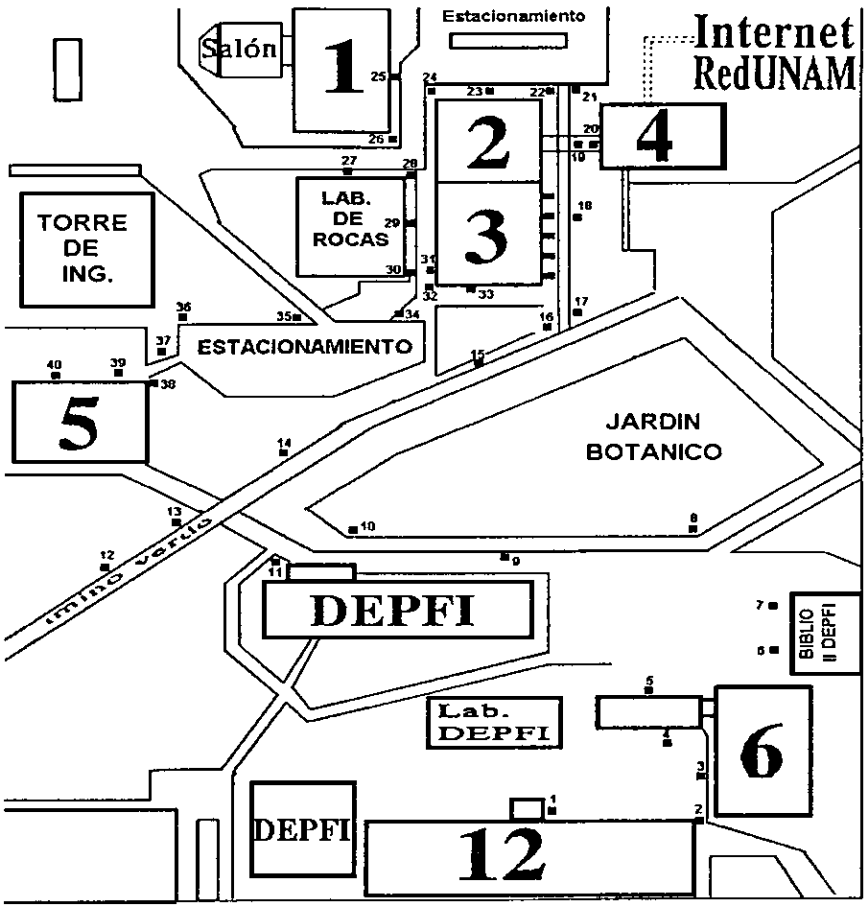


Figura 3.4

El esquema de estrella une con un par de fibras, a cada uno de los edificios principales, así pues, en cada cuarto de telecomunicaciones hay un distribuidor de fibras, en donde hay 6 hilos de llegada y otros 6 de salida, en el distribuidor se toma un par de fibras para alimentar el equipo correspondiente y se realiza el puenteo de los 2 pares restantes para llevar la señal a los siguientes edificios, de esta manera y como lo plantea el esquema, todas las fibras parten del switch ubicado en el edificio 4, de ahí se lanza una acometida de cable de fibra óptica rudo, por los registros hasta llegar al edificio 2 de donde se usa un distribuidor para tomar un par y conectarlo al equipo local, en el mismo distribuidor se puentean los pares restantes (2) para que se lance nuevamente una acometida de fibra, en cable rudo, hasta el edificio 1. Una vez en este edificio, se hace nuevamente uso de un distribuidor para tomar un par de fibras para el servicio local y puentear otro par para que continúe su trayectoria. Este último par de fibras llega hasta el edificio 5, en donde se toma la señal y se realiza un

puente entre los concentradores, esto es que se recibe la señal para utilizarla localmente pero también provee un par de fibras de salida para que lleve la señal a otro edificio, en este caso el edificio que depende directamente del 5 es el 6. Existe un cableado de fibra óptica multimodo de uso rudo desde el edificio 6 hasta el edificio 12 con lo que el anillo en cuanto a trayectorias de fibra está completo, sin embargo esta sección no se utiliza por el momento ya que el enlace del edificio 12 al edificio 4 (centro de la estrella), se hace mediante una tarjeta FDDI, formando un pequeño anillo de transmisión recepción entre ambos edificios. Inicialmente se tenía contemplada una instalación similar a la de los demás edificios, es decir, usando un solo par de fibras para unir ambos edificios, sin embargo dado que en el edificio 12 se encuentran los servidores principales a los que recurre la mayor parte de la comunidad, se optó por el enlace de FDDI (1 par de fibra para la transmisión y 1 para la recepción, formando los anillos redundantes) para proveer rápidamente los servicios de Internet, ftp, correo electrónico, etc., disminuyendo el tiempo de espera y mejorando el tráfico en la red local. Los servicios que provee REDII actualmente, serán descritos con detalle más adelante.

Con respecto a la conexión hacia RedUNAM solamente hay dos pares de fibra. De los cuales, uno permanece como redundante, es decir como medida de seguridad.

Cabe señalar que el Instituto de Ingeniería actualmente cuenta con 5 subredes para uso local que le fueron proporcionadas a través de la Dirección General de Servicios de Cómputo Académico (DGSCA), las subredes son las siguientes: 132.248.53.XXX, 132.248.153.XXX, 132.248.154.XXX, 132.248.155.XXX y la subred 132.248.156.XXX. Además se cuenta con algunas direcciones de la subred 132.248.189.XXX para uno de los edificios externos al campo universitario y otras 8 direcciones de la subred 132.248.126.XXX para el edificio conocido como la mesa vibradora, también del Instituto.

3.1.2 Estado de la red en el edificio 1

En este edificio hay alrededor de 110 nodos de red activos, que se proveen a través de 5 concentradores Hub STACK 10BASE-T de Cabletron Systems. El concentrador principal es un SEHI-24 de 24 puertos en RJ45, tiene una entrada para AUI (DB15) coaxial delgado y una más para fibra óptica; a este concentrador se conectan 3 SEH-24 en cascada, también de 24 puertos en RJ45 cada uno y por último se conecta en cascada, un SEH-34 de 24 puertos a base de telcos, usa dos telcos de 12 puertos.

Potencialmente se tienen 120 nodos de red que pueden estar activos en este edificio, además de que en caso de crecimiento en el número de los nodos de red, el equipo es apilable, y sólo se necesitaría implementar los concentradores necesarios para cubrir la expansión de la red. En este edificio están distribuidos nodos correspondientes a la subred 132.248.153.XXX, de la manera más adecuada para cubrir las necesidades de los usuarios así como para la administración de la red.

El equipo principal en este edificio es una estación de trabajo SUN modelo Sunserver 360 en la que se desarrollan trabajos de investigación sobre instrumentos de medición para sismos, los equipos restantes son PCs en su mayoría y algunas impresoras.

3.1.3 Estado de la red en los edificios 2, 3 y 8

Dado que estos 3 edificios tienen direcciones IP pertenecientes a la subred 132.248.154.XXX y que su ubicación física es muy próxima unos de otros, se decidió mencionarlos en un mismo subtema del presente trabajo.

El equipo principal de esta sección de red se encuentra ubicado en el primer entrepiso del edificio 2, es decir, entre los niveles de la planta baja y el primer piso. Ahí tenemos un equipo MMAC-M5FNB de Cabletron Systems, el cuál cuenta con 2 fuentes de poder redundantes M5PSM, para ofrecer una mayor seguridad ante posibles fallas en el suministro de energía del equipo. También cuenta con 5 tarjetas, de las cuales, 4 son TPMIM-34 y una IRBM con una entrada AUI y una para fibra. Las tarjetas TPMIM-34 proporcionan 24 puertos de red mediante 2 telcos de 12 puertos cada uno, mientras que la tarjeta IRBM provee las posibilidades para la interconexión entre diversos medios de transmisión y también proporciona la opción de monitorear directamente el equipo a través de un puerto serial similar al COM1 de las computadoras. De la tarjeta IRBM de este equipo principal, se lanza un cable coaxial delgado hacia un transceiver (acoplador de medios) para obtener un par de fibras que alimentan el equipo de la parte frontal del edificio 3 (Nave), este equipo de red es un concentrador SEHI-34 de 24 puertos a base de telcos (2 de 12 puertos cada uno), este concentrador proporciona red al primer piso del edificio 3 en la parte frontal y también a una parte del área de ingeniería sismológica (planta baja del edificio 2), de este equipo sale un par de fibras que llevan red a la parte posterior del edificio 3, en esta área se tiene un concentrador SuperSatck II de 3Com de 24 puertos en RJ45, este equipo proporciona, por el momento, 20 nodos de red para esa área.

Por su parte el edificio 8 conocido también como laboratorio de enrocamiento, tiene solamente 3 nodos de red los cuales se proveen mediante una conexión de UTP a través de una tubería directa de las regletas del edificio 2. En cuanto a los equipos principales de esta sección de red, podemos decir que se encuentran concentrados en el edificio 2, y son una estación de trabajo HP9000 (modelo 720) y una IBM RS6000, así como dos estaciones menores SUN SPARC classic, los demás equipos son PCs e impresoras. Los servicios proporcionados por la red en estos edificios se mencionarán más adelante.

3.1.4 Estado de la red en el edificio 4

El edificio 4 es actualmente el más importante dado que en él se encuentra ubicado nuestro equipo principal, que es el centro de la estrella y que proporciona conexión hacia el exterior mediante RedUNAM.

En este edificio contamos con un equipo MMAC-M5FNB, que tiene integrada una tarjeta ESXMIM-F2 que proporciona los enlaces de fibra tanto hacia RedUNAM como hacia todos los edificios del Instituto conectados en red, este equipo funciona como un switch para distribuir la señal que le llega de RedUNAM a través de un par de fibras ópticas, las cuales se conectan a un ruteador ubicado en el edificio IIMAS. Por otra parte tenemos el equipo local para el edificio 4, éste es un concentrador MMAC-3 que mediante 2 tarjetas TPMIM-34 de 24 puertos cada una (2 telcos de 12 puertos cada

uno), proporciona 48 salidas potenciales de red de las cuales 40 están ya instaladas, distribuidas en las dos plantas que conforman este edificio

La subred que corresponde a esta sección es la 132.248.153.XXX, la cual, se comparte con el edificio 1. El equipo de cómputo principal son 2 estaciones de trabajo HP9000 (modelos 720 y 710), servidores locales de geotecnia: BLUES y JAZZ, y una estación de trabajo Silicon Graphics modelo Octane 8, servidor local TLALLI. El equipo restante lo conforman PCs e impresoras. Cabe señalar que dado a que este edificio fue uno de los primeros en los que se implementó la red de cómputo, hay una combinación en el cableado, ya que éste es en algunas zonas de categoría 3 y en otras de categoría 5.

3.1.5 Estado de la red en el edificio 5.

El edificio 5 es el que cuenta con más nodos de red por el momento, ya que tiene 7 concentradores.

En primer lugar tenemos un equipo MRXI de Cabletron Systems que proporciona 12 puertos a través de un telco; a este concentrador, llega la acometida de fibra proveniente del edificio 4. Este equipo se conecta en cascada a un MMAC-3FNB que cuenta con dos tarjetas TPMIM-34 de 24 puertos cada una (a base de telcos).

También cuenta con una tarjeta IRBM que proporciona un enlace de fibra óptica para el edificio 6, un enlace mediante cable de 9 hilos blindado a un transceiver TMS-3 y la posibilidad de monitoreo del equipo a través de un puerto serial. El transceiver TMS-3 se conecta usando un cable coaxial delgado a un concentrador HPJ2602A de Hewlett-Packard con 48 puertos. Este concentrador cuenta con 4 telcos de 12 puertos cada uno, cabe hacer mención de que 4 de estos puertos no funcionan, por lo que en realidad sólo suministra 44 nodos. Hasta aquí tenemos una sección de red dentro del mismo edificio, la siguiente sección de red depende de 4 equipos de Cabletron Systems.

El principal equipo es un concentrador SEHI-24 que tiene 24 puertos para RJ45, la señal de red que lo alimenta es a través de un puerto EPIM1 (RJ45). A éste se conectan en cascada 3 equipos SEH-24 de 24 puertos cada uno, con salidas para conectores RJ45. Con esta infraestructura se pueden tener 204 nodos de red (considerando los puertos descompuestos) potenciales, de los cuales ya hay instalados 195 y tenemos algunos de holgura, es decir aún sin instalar. Cabe señalar, que la asignación actual de las direcciones IP es la que se generó a raíz de una reasignación de direcciones llevada a cabo el mes de junio de 1998, a este edificio le corresponde la subred 132.248.155.XXX.

Los equipos de cómputo principales en el edificio son 2 estaciones de trabajo HP9000 (modelos 750 y 720), servidores: VORTEX y QUETZAL, así como algunas estaciones de trabajo menores, que sirven para resolver problemas de ingeniería hidráulica e ingeniería ambiental. Los demás equipos son PCs y algunas impresoras que están en red.

3.1.6 Estado de la red en los edificios 6 y 12.

En el edificio 12 que es donde se encuentra la coordinación de Sistemas de Cómputo, tenemos un concentrador de Cabletron Systems, modelo MMAC-M8FNB con 8 tarjetas de las cuales, una es FDMMIM-24 que nos proporciona el enlace de FDDI hacia el edificio 4 mediante un pequeño anillo redundante, además de 4 servicios en RJ45, donde conectamos los principales equipos de la Coordinación, mediante un CDDI. También tenemos 6 tarjetas TPMIM-34 de 24 puertos cada una, a base de telcos (2 de 12 puertos cada uno), los cuales nos proporcionan 144 nodos potenciales de red para este edificio. Por último tenemos una tarjeta IRBM para el monitoreo del equipo. La distribución de direcciones IP se hizo recientemente mediante una reasignación hecha el mes de octubre de 1998.

Por lo que respecta al edificio 6, tenemos un equipo de red MRXI de Cabletron, con 12 puertos a base de un telco, en este edificio solo se usan 9 de los 12 nodos potenciales, este equipo recibe un par de fibras provenientes del edificio 5.

Los principales equipos de cómputo ubicados en estos edificios son: en el edificio 12 hay 3 servidores generales (son 3 estaciones de trabajo de la marca Sun, modelos, Sparcserver 20, Sparcstation 20 y Ultrasparc), además se cuenta con una estación de trabajo para monitorear la red, dicho equipo es un SparcClassic de Sun que cuenta con el software de red SunNetManager y por último con una estación Sun SparcClassic que funciona como el DNS (Servidor de Nombres) local. Además de ello contamos con un servidor con sistema operativo Windows NT (ALTAIR) que provee muchos servicios como: antivirus, software de aplicación, sistemas operativos, etc.; para todas las PCs conectadas en red dentro del Instituto. Así mismo tenemos algunas estaciones de trabajo menores que sirven como servidores locales. La mayoría del equipo restante son PCs y algunas impresoras conectadas en red.

Por su parte el edificio 6 dado que por el momento tiene baja densidad de equipos de cómputo, sólo cuenta con un servidor local a base de Windows NT y algunas PCs.

3.1.7 Estado de la red en los edificios externos al campo universitario.

Además de la infraestructura de red antes mencionada, el Instituto de Ingeniería también se encarga de administrar y dar soporte a dos instalaciones de red que podríamos catalogar fuera del campo universitario. Una de esas instalaciones la conforma el piso 6 del edificio que se encuentra ubicado en la calle de Esparza Oteo #144, ésta calle es paralela a Insurgentes (a la altura de Plaza Inn). El piso con instalación de red, da cabida a 24 nodos mediante un concentrador SuperStack II de 3Com, de 24 puertos en RJ45.

El equipo principal de cómputo es un servidor local con sistema Windows NT, el cual provee diversos servicios a las PCs ubicadas en el área. Las direcciones IP asignadas para estos nodos de red pertenecen a la subred 132.248.189.XXX.

El otro edificio que cuenta con infraestructura de red es el conocido como la "Mesa Vibradora", ubicado a un costado del jardín botánico. Este edificio, a pesar de encontrarse en CU, se incluyó en este apartado porque la administración de los nodos así como el mantenimiento de la infraestructura de red con que cuenta, no se centraliza en la Coordinación de Cómputo del Instituto.

En este edificio hay solamente ocho nodos de red y actualmente sólo dos de ellos están siendo utilizados. Las direcciones IP que pertenecen a la mesa vibradora son de la 132.248.126.180 a la 132.248.126.187. En este edificio el equipo de cómputo es escaso ya que se tiene un servidor con Windows NT (conectado a la red) y algunas computadoras, de las cuales sólo una de ellas está en red. La administración de estos nodos depende de las personas que trabajan en ese edificio. Los servicios de red con que cuentan éstas máquinas son los mismos que se tienen en todos los edificios pertenecientes a REDII y se describen con detalle en el punto correspondiente.

A continuación veremos, algunos ejemplos de la manera general de asignación de las direcciones IP en los edificios antes mencionados, cabe señalar que dicha asignación se llevó a cabo de la mejor manera posible, tomando en cuanta tanto la capacidad de nuestros equipos de red, asi como la manera más adecuada de administrar nuestras subredes, los planos de ejemplo son los del edificio 3 (figuras 3.5 y 3.6) y los de Esparza Oteo (figura 3.7)

DISTRIBUCIÓN DE PUNTOS DE RED DEL **EDIFICIO 3, SUBRED 132.248.154.xxx.**

. DIRECCIÓN IP ASIGNADA
▌ CONCENTRADORES

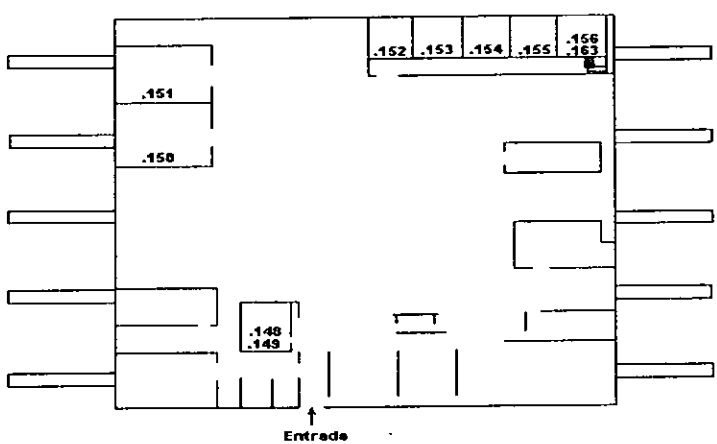
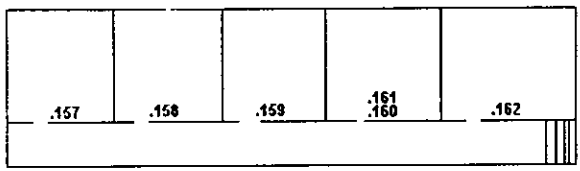
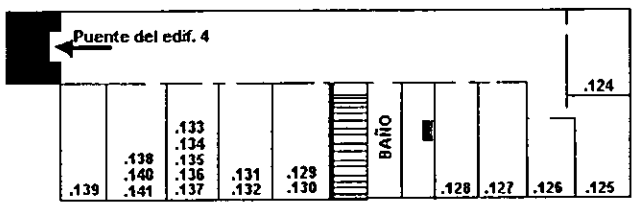


Figura 3.5. Planta baja (PB)

ESTA AREA ESTA EXACTAMENTE ARRIBA DE LOS CUBICULOS DE LA PARTE POSTERIOR DE LA PB DE LA NAVE.



Este concentrador alimenta esta sección y algunos puntos de Ing. Sismológica



ESTA AREA ES EL PISO 1 DE LA NAVE EN SU PARTE FRONTAL

Figura 3.6. Piso 1

DISTRIBUCIÓN DE PUNTOS DE RED DEL **EDIFICIO DE ESPARZA OTEO, SUBRED 132.248.189.xxx**

. DIRECCIÓN IP ASIGNADA
▮ CONCENTRADORES

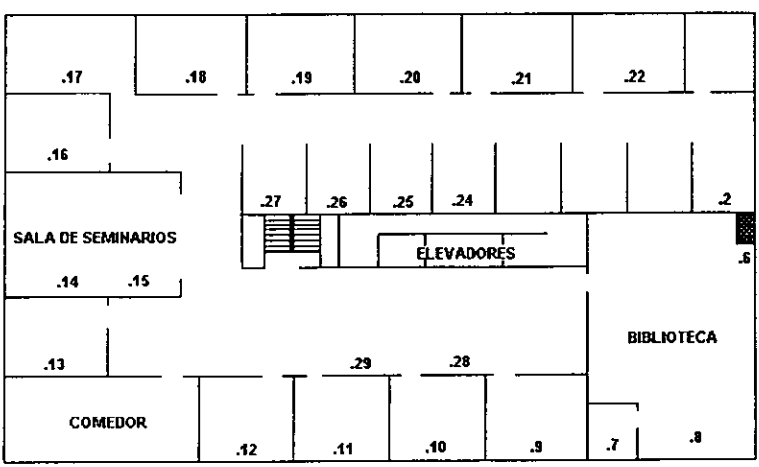


Figura 3.7

3.1.8 Observaciones sobre el cableado actual de la red

Actualmente el cableado interno en cada uno de los edificios mantiene un esquema centralizado, esto impide una distribución adecuada del número de nodos para cada piso, ya que a cada closet de telecomunicaciones llegan demasiados cables de UTP, que en ocasiones impiden llevar a cabo labores de mantenimiento del equipo de red debido a que el espacio para desempeñarse es reducido. Si bien es cierto, el problema se presenta principalmente en edificios con grandes concentraciones de nodos, como son el 5, el 1 y el 12, sin embargo el problema también se presentará en un futuro en los edificios restantes a medida que se vayan instalando más salidas de red. Para evitar esta saturación en los closets, proponemos descentralizar el cableado a lo largo del edificio, para lo cuál es necesario construir algunos closets de telecomunicaciones además de los ya existentes y distribuir en cada uno de ellos el cableado correspondiente. Nuestra propuesta de cableado consiste básicamente en lo siguiente:

1. Instalar por piso y en cada uno de los edificios un closet de telecomunicaciones con un rack estándar. El closet deberá estar lo más centrado posible con relación a la longitud del edificio, esto con la finalidad de cablear hacia ambos extremos del mismo y evitar gastar más cable del necesario.

2. En cada closet, debe de instalarse el cableado requerido única y exclusivamente para esa planta y no de otros pisos.

3. El enlace vertical entre cada closet de telecomunicaciones podrá hacerse mediante fibra óptica o cable UTP categoría 5, dependiendo de las necesidades particulares de cada caso. Sugerimos un cableado vertical basado en fibra óptica multimodo.

4. El cableado horizontal deber ser a base de cable par trenzado (UTP) categoría 5. En algunos casos el cableado ya existente podrá reutilizarse, para ello bastará redireccionarlo a través de ductería o canaleta. En los otros casos se requerirá un cableado completamente nuevo.

5. La remodelación del cableado deberá cumplir con las especificaciones de la norma EIA/TIA 568, descrita en el capítulo 1 del presente trabajo.

Por otra parte tenemos la estructura del cableado del backbone, como se describió anteriormente tenemos un anillo a través de 3 pares de fibra. Para brindar redundancia recomendamos establecer un anillo alterno para permitir, en caso de una falla muy severa en el anillo principal, la interconexión de nuestros edificios y RedUNAM. Es conveniente que se utilice nuevamente fibra multimodo y que se instale un cable de al menos 6 hilos. Un plano que muestra la ruta propuesta para llevar a cabo la redundancia es el que se presenta en la figura 3.8.

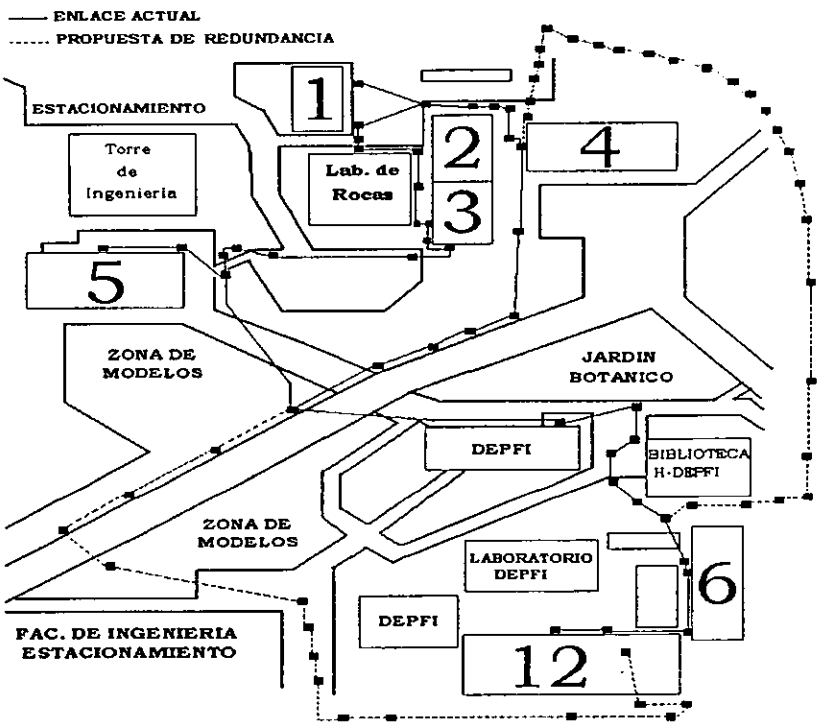


Figura 3.8

La propuesta de redundancia se presenta en el plano con línea punteada, mientras que la trayectoria de fibra ya existente es la línea continua. Como vemos en la propuesta se establecen dos posibles maneras de proporcionar el enlace de todos los edificios del backbone. Así por ejemplo la ruta de la derecha, plantea una ruta del edificio 4 al 12 por la cuál se podrían traer los edificios 1, 2, 3, 4, 5, 6 y 8 (laboratorio de enrocamiento). El registro cercano al edificio 6 sería la ruta por la que se alcanzaría el edificio 12 (actual centro de la estrella), esta ruta se usaría en caso de una fisura en el cable de fibra ya sea en la trayectoria central o bien en la trayectoria de la izquierda. Así mismo la trayectoria del lado izquierdo (zona de modelos) se usaría en caso de una ruptura en la parte central o derecha del backbone en funcionamiento. Con estas rutas redundantes se asegura la interconectividad de los edificios del Instituto en caso de cualquier daño en las trayectorias centrales del backbone.

3.2 SERVICIOS PROPORCIONADOS ACTUALMENTE POR LA RED DEL INSTITUTO DE INGENIERÍA.

Los servicios que proporciona REDII, a todos los edificios que hacen uso de ella, se pueden generar gracias a que la red del Instituto puede utilizar como protocolos de comunicación: TCP/IP (Internet), IPX/SPX (Novell Netware) y NetBEUI (Microsoft).

Actualmente, sin embargo, se está tratando de generalizar el uso únicamente del protocolo TCP/IP por su mayor estandarización, y para poder llevar a cabo una completa compatibilidad en nuestros equipos de red y servidores, así como la detección y corrección de posibles fallas.

A continuación se realiza una breve explicación de los servicios de red que más se utilizan en el Instituto de Ingeniería.

3.2.1 Servicios básicos

Sesión remota

Las sesiones remotas se efectúan mediante emulaciones de terminales que proveen al usuario un mecanismo de enlace remoto con la mayoría de los equipos con que cuenta el Instituto (las estaciones de trabajo que se encuentran conectadas a la REDII) o aquellas máquinas localizadas en el mundo o red Internet.

Dada la gran aceptación que ha tenido TCP/IP como un estándar en las comunicaciones a nivel mundial, el servicio de sesión remota mejor referido como **telnet** se ha convertido en la herramienta más empleada para efectuar sesiones remotas en Internet y redes que trabajan con esta familia de protocolos. Telnet permite al usuario acceder a una computadora remota desde su computadora local, una vez conectado el usuario al equipo remoto, puede introducir datos, ejecutar programas y llevar a cabo todas aquellas tareas que desee como si estuviese trabajando directamente en el equipo remoto.

Comunicaciones electrónicas

Las comunicaciones electrónicas aprovechan las herramientas de comunicación en línea y de transferencia de mensajes, para entablar, en forma confiable y de manera eficiente la comunicación con otros usuarios dentro de la misma institución o con personas en otras organizaciones nacionales o extranjeras que se encuentren integradas a una red mundial (como la Internet) y que cuenten con los mismos servicios.

La aplicación más utilizada dentro de los servicios de comunicación electrónica entre los usuarios es el **correo electrónico** (e-mail), que se utiliza para intercambiar mensajes con una o varias personas, y se considera la herramienta de comunicación que más se utiliza en el mundo. La mayoría de los mensajes contienen sólo texto, pero también es posible enviar archivos conteniendo imágenes, sonido y hasta animaciones.

El conjunto de protocolos TCP/IP especifica un estándar para el intercambio de correo electrónico entre anfitriones, este es referido como el **Protocolo de Transferencia de Correo Simple** (SMTP: Simple Mail Transfer Protocol), que describe las características bajo las cuales el correo electrónico debe ser implantado.

Los sistemas basados en la plataforma Unix usan el programa **sendmail,** el cuál utiliza el protocolo SMTP, este programa es capaz de comunicarse con otros servicios de

correo basados en el SMTP, así mismo, puede operar como un intérprete o gateway entre diferentes sistemas de correo.

Todas las estaciones de trabajo del Instituto de Ingeniería utilizan el programa sendmail como servicio para el correo electrónico, de esta manera, se encuentran configuradas para la recepción y envío de mensajes a cualquier punto del mundo a través de la red Internet y otras redes. Otros servicios adicionales dentro del servicio de correo electrónico son soportados, tal es el caso del protocolo de servicio referido como POP (Post Office Protocol), el cuál es el encargado de atender a los clientes de POP instalados en las computadoras personales (PC's). Es importante señalar que fue necesario utilizar estos servicios adicionales ya que permiten que el servidor de correo electrónico (sendmail) también pueda entregar y recibir mensajes hacia/desde computadoras personales (cliente) que utilizan el POP.

La mayoría de los usuarios nunca emplean el programa sendmail directamente, en su lugar utilizan aplicaciones de interfaz (referidos como front-end's) que proporcionan una forma más fácil de interacción con él, algunos ejemplos de estos programas son: PINE, elm, Mail; los cuales son ejecutados en las mismas estaciones de trabajo y por otro lado aplicaciones como Eudora, Minuet y Outlook Express instaladas en computadoras personales (por lo cuál son clientes del servicio POP).

Por otro lado, el Instituto de Ingeniería maneja otros servicios de comunicación electrónica a través de la red, como son los servicios: talk, finger, write, wall, IRC, etc.

Todos estos servicios de comunicación electrónica se proporcionan a todos los usuarios del Instituto que así lo requieran, y de manera implícita a todos aquellos usuarios que tengan cuenta en alguna estación de trabajo. Con estas herramientas se provee al personal del Instituto, el acceso a los más diversos servicios de comunicación electrónica a nivel local, nacional e internacional.

Transferencia de archivos (FTP)

Uno de los grandes beneficios que se tiene al contar con una red de cómputo, es la facilidad de transferir archivos entre computadoras, convirtiéndose ésta en una de las aplicaciones de uso principal que se tienen en la red. Los archivos a transferir pueden ser datos, imágenes, programas, texto o cualquier otro tipo de información. La aplicación estándar utilizada para transferir archivos en redes que emplean TCP/IP es el programa ftp (file transfer program) que se basa en el protocolo FTP (File Transfer Protocol).

Entre las características más relevantes del ftp se encuentran:

- Acceso interactivo: La mayoría de las implantaciones de ftp proveen una interfaz interactiva que permite al usuario interactuar fácilmente con servidores remotos. Entre las operaciones que se pueden efectuar en una sesión de ftp son: listar archivos, crear y eliminar directorios remotos, etc.
- Especificación de formato: ftp permite al cliente especificar el tipo de formato de los archivos a ser transferidos, es decir, el usuario puede emplear diferentes modalidades de transferencia (modo binario para formatos especiales o modo ascii para archivos de texto), con esta característica la transferencia de datos puede

hacerse incluso entre computadoras que empleen sistemas operativos diferentes o formatos de almacenamiento distintos.

- Control de autenticidad: ftp requiere que los clientes verifiquen su autenticidad enviando su nombre de usuario y su clave de acceso al servidor antes de iniciar una sesión de transferencia de archivos. El servidor niega el acceso a aquellos clientes que no cuenten con un nombre de usuario y una clave de acceso válida.

El programa ftp es una de las principales herramientas empleadas en el Instituto de Ingeniería ya que sirve para transferir información entre los diferentes equipos de cómputo conectados. Cada equipo conectado a la red del Instituto está provisto, de ésta herramienta, ya sea computadora personal o estación de trabajo. En lo que se refiere a computadoras personales se cuenta con diferentes versiones de clientes de ftp, mientras que para estaciones de trabajo cada una cuenta con una propia implantación del ftp tanto para el cliente como para el servidor.

También se ha implantado una cuenta pública en una estación de trabajo del Instituto para efectuar ftp de libre acceso, esta cuenta mantiene un conjunto de programas y documentos de interés general y que son de libre distribución, entre estos se encuentran manuales, programas antivirus, compactadores de información y diversas utilerías de dominio público. Este tipo de cuenta pública utilizada para efectuar la transferencia de archivos es conocida como ftp anónimo.

3.2.2 Servicios de recursos compartidos

Sistema de archivos en red (NFS)

El **Sistema de Archivos en Red** (NFS: Network File System), permite que directorios y archivos sean compartidos a través de una red. Esta herramienta fue inicialmente desarrollada por SUN Microsystems en los inicios de los años ochenta, sin embargo, ya ha sido adoptado como un estándar por otros fabricantes de software y actualmente forma parte del sistema operativo UNIX y otros sistemas operativos, existiendo incluso versiones de NFS para computadoras personales (como PC-NFS para el sistema operativo DOS y Windows 95).

Mediante NFS, usuarios y programas pueden acceder a sistemas de archivos localizados; en sistemas remotos y tratarlos como si fueran sistemas de archivos locales. Una vez implantado el ambiente de NFS, el usuario no conoce donde se encuentra su información y ni le interesa si esta guardada localmente (en el disco duro de su máquina) o si está en un disco duro de una máquina remota, es decir, la gestión de la información que hace NFS es completamente transparente desde el punto de vista del usuario e incluso de las aplicaciones.

Actualmente, todos los archivos pueden compartirse a través de la red en las computadoras personales, siempre y cuando cada usuario asigne permisos a los demás. Esta tarea de compartir archivos se ha enfocado principalmente a instalar software en algunas estaciones de trabajo (o en Altair), para que la comunidad del Instituto pueda acceder a esta paquetería, sin la necesidad usar los recursos de sus PCs.

Impresión remota

La impresión remota es uno de los mecanismos más empleados en ambientes de red para proporcionar a los usuarios de una organización el acceso a impresoras de características diferentes, tales como manejo de lenguajes de impresión (Postscript, HPCL, etc.), impresión a color o bien impresión de alta resolución; obteniéndose de esta forma un mejor uso y disponibilidad de estos periféricos. La impresión remota es efectuada por los usuarios como si ellos tuviesen conectada la impresora directamente al puerto paralelo de su computadora personal o estación de trabajo.

En ambientes de red, cuando un usuario desea imprimir un trabajo puede optar porque éste se lleve a cabo localmente (si cuenta con una impresora) o bien redireccionar su impresión hacia un equipo encargado de las tareas de impresión en la red, llamado servidor de impresión (print server). Este último se encarga de recibir cada una de las tareas de impresión de los diferentes usuarios de la red. Una vez que ha llegado un trabajo de impresión, el servidor verifica si existen trabajos esperando a ser procesados, en caso de que así sea, el nuevo trabajo será guardado en una cola de impresión (esta cola es realmente un archivo guardado bajo cierta estructura de subdirectorios que el propio servidor se encarga de crear) para esperar ser procesado y será almacenado ahí hasta que el servidor lo envíe a la impresora; en caso de que el servidor no este atendiendo otra impresión previa, el trabajo será enviado inmediatamente hacia la impresora. Cabe aclarar que la impresora puede encontrarse conectada directamente al servidor de impresión o bien puede hallarse conectada a la red como un nodo más de ella, sin que esto afecte su funcionamiento y disponibilidad. Esta última opción, de conectar la impresora a la red como un nodo más, presenta grandes ventajas ya que permite que una impresora se localice en lugares en donde los usuarios puedan acceder fácilmente y al mismo tiempo se evita que personal no autorizado tenga contacto con los servidores.

El servidor de impresión no solo se encarga de recibir trabajos provenientes de la red y enviarlos a impresión, éste efectúa otras tareas como: monitorear el estado de las colas de impresión, manipular el orden en que se encuentran los trabajos en las colas de impresión, cancelar trabajos y llevar un estricto control de trabajos de impresión efectuados para un determinado usuario o departamento.

El uso de impresión remota en el Instituto de Ingeniería se ha convertido en una tarea común, para ello se han implantado diferentes mecanismos que permiten llevar a cabo esta actividad. Uno de ellos se basa en el uso de servidores de impresión del sistema operativo Novell Netware versión 3.11, el cual actualmente solo se usa en el área de administración, ya prácticamente obsoleto; mientras que un segundo mecanismo emplea las facilidades de impresión en red que la plataforma Unix proporciona y un tercer mecanismo, el más usado hoy en día, es mediante tarjetas de red externas conectadas a cada una de las impresoras y controladas por el servidor Altair. Todos los mecanismos, antes mencionados llevan a cabo el control de tareas de impresión, y cada uno de estos servidores requiere que las siguientes tareas sean efectuadas antes de ponerlos en operación:

1. Determinar de forma estratégica la ubicación de impresoras dentro del Instituto, ya sea que estas se encuentren conectadas directamente a los servidores de impresión o bien sean conectadas a la red como un nodo más en lugares accesibles únicamente para los usuarios autorizados.
2. Establecer qué equipos se emplean como servidores de impresión remota.
3. Definir para cada servidor las colas de impresión, así cómo las impresoras que atenderán a cada una de éstas colas.
4. Especificar las características de operación de cada una de las impresoras que los servidores utilizarán para canalizar las tareas de impresión.
5. Finalmente, definir los usuarios a los que cada servidor atenderá.

3.2.3 Sistemas de Información Distribuida

Formalmente un sistema de información distribuida es una colección de módulos de software ejecutándose en varias computadoras interconectadas por una red, los cuales administran todos los datos distribuidos (archivos y bases de datos) y las transacciones asociadas. Básicamente estos sistemas incluyen la funcionalidad de un sistema de administración de base datos, un sistema de administración de archivos distribuidos y un sistema de administración de transacciones distribuidas.

En los últimos años, se han desarrollado diferentes protocolos y herramientas de obtención de información en Internet. A continuación se describen las principales herramientas de navegación y exploración que se utilizan el Instituto de Ingeniería.

Servicios interactivos de entrega de información

- World Wide Web

Desarrollado en Suiza, por el European Partide Physics Laboratory. El WWW, también referido como W3 o WEB, combina la obtención de información y uso de hipertextos para ser un simple pero poderoso sistema de información. Consta de documentos virtuales que pueden contener otros documentos con ligas a otros servidores WWW. Los servidores de WWW soportan documentos en una amplia variedad de formatos como por ejemplo, Postscript, audio, imágenes y video, o ligas a otros servidores WWW.

WWW utiliza el protocolo HTTP (Hyper Text Transport Protocol) como un programa de examinación que solicita documentos o búsquedas por medio de palabras claves de un servidor remoto. Estos programas son diseñados para acceder a datos usando el HTTP (conexión TCP utilizando el puerto lógico 80) y protocolos existentes como FTP y el NNTP usado en Usenet. Originalmente WWW incluía un cliente modo línea para utilizarse con el telnet y una interfaz gráfica limitada, actualmente la mayoría de los clientes WWW se encuentran basados en interfaces gráficas (GUI o navegadores) que pueden desplegar imágenes, video y agregar audio al hipertexto de calidad PostScript, los clientes GUI más destacados actualmente para WWW son el Mosaic, Netscape e Internet Explorer (Microsoft).

Actualmente y gracias al rápido crecimiento de Internet, este servicio es uno de los principales para buscar todo tipo de información en la red, en el Instituto contamos con el servidor PUMAS que entra dentro de esta categoría.

- Internet

El servicio de Internet es posible gracias a que se cuenta con la conexión a RedUNAM, por lo que además de los servicios anteriormente señalados, se incluyen todos los servicios públicos que provee la misma, sin embargo, sólo mencionaremos los aspectos principales de Internet, por ser el servicio con mayor demanda en nuestra comunidad.

Actualmente Internet es la red de datos más importante en el mundo. La adopción de los protocolos TCP/IP y el crecimiento de Internet no se ha limitado a proyectos con fondos del gobierno e instituciones educativas. Grandes corporaciones computacionales se han conectado a Internet, incluyendo: compañías petroleras, automovilísticas, empresas electrónicas, compañías farmacéuticas y de telecomunicaciones. Las compañías medianas y pequeñas se empezaron a conectar en los años noventa. Además, muchas compañías han utilizado los protocolos TCP/IP en sus redes corporativas (Intranets), aunque no han optado por ser parte de la Internet global.

Seguridad en Internet

La seguridad en un ambiente como Internet es algo muy delicado, pues la información es lo más importante y por tanto tiene un valor significativo y difícil de cuidar, debido a que implica entender cuándo y cómo pueden confiar los usuarios, las computadoras, los servicios y las redes, uno en otro, también implica entender los detalles técnicos del hardware y los protocolos de red. Algo muy importante, dado que TCP/IP soporta a una amplia diversidad de usuarios, servicios y redes, y debido a que Internet global puede abarcar muchas fronteras políticas y organizacionales, los individuos y las organizaciones participantes pueden no estar de acuerdo en lo que a un nivel de confiabilidad se refiere o bien en las políticas para el manejo de datos.

Los problemas de seguridad en Internet y los mecanismos de software que ayudan a que la comunicación en Internet sea segura, se pueden dividir en términos generales en tres conjuntos.

El primero, se enfoca a los problemas de autorización, autentificación e integridad. El segundo, se enfoca al problema de la privacia y el tercero, se orienta hacia el problema de la disponibilidad mediante el control de acceso.

- Mecanismo de autentificación

Los mecanismos de autentificación resuelven el problema de verificar la identificación. Muchos servidores, están configurados para rechazar una solicitud a menos que la origine un cliente autorizado. Para validar la autorización, un servidor debe conocer la identidad del cliente, por ejemplo, una forma débil de autentificación en Internet es utilizar la dirección IP. La autentificación de fuente IP es débil debido a que se puede romper fácilmente. En una red como Internet en la que los datagramas pasan a través de enrutadores y redes intermedias, la autentificación original puede ser atacada desde una máquina intermedia. Una forma más segura de saber si un cliente o un servidor se están comunicando o no, como un impostor, es utilizando un sistema de cifrado de clave pública.

- Mecanismo de privacia

El cifrado también puede manejar problemas de privacia. Por ejemplo, si un emisor y un receptor utilizan esquemas de cifrado de clave pública, el emisor puede garantizar que sólo el receptor involucrado pueda leer un mensaje. Si es así, el emisor utiliza la clave pública del receptor para codificar el mensaje y el receptor su clave privada para decodificar el mensaje. Dado que sólo el receptor involucrado tiene la clave privada necesaria, en ningún otra parte se puede decodificar el mensaje. Así, la privacia puede reforzarse aún cuando una tercera parte obtenga una copia de los datagramas conforme éstos pasan entre el emisor y el receptor.

Los mecanismos de cifrado de clave pública pueden utilizarse para ayudar a resolver los problemas de autentificación, autorización y privacia. Por otra parte, es necesario que tanto, el software del cliente como el del servidor sean modificados para poder usar estos mecanismos.

Antes de que una organización pueda elegir un mecanismo para reforzar la seguridad, es necesario establecer una política de información.

El mecanismo de **paredes de fuego** (fire wall) para la seguridad, se utiliza para controlar el acceso a Internet. Esto se lleva a cabo de la siguiente manera. Una organización coloca una pared de seguridad en cada enlace que realice la conexión de salida hacia el mundo exterior (a Internet global), esto es para garantizar que la red interna de la organización se mantenga libre de tráfico no autorizado. Una pared de seguridad consiste en dos barreras y una computadora o dispositivo seguro llamado *anfitrión baluarte*. Cada barrera utiliza un filtro para restringir el tráfico de datagramas. El anfitrión baluarte ofrece servicios visibles desde el exterior y corre clientes que acceden a servidores externos. La organización utiliza su información y sus propias políticas de acceso a Internet para determinar cómo configurar el filtro.

Por lo general, la pared de seguridad bloquea todos los datagramas que llegan desde el exterior, excepto los destinados al anfitrión baluarte en donde este verifica ciertos datos de información del datagrama y determina si le da acceso o no, a la red protegida.

Crecimiento y tendencias del futuro de Internet

Tanto la tecnología TCP/IP como Internet continúan evolucionando. Se siguen proponiendo nuevos protocolos y los más antiguos se están revisando. La NSF añadió una considerable complejidad al sistema al introducir una red de columna vertebral, redes regionales y cientos de redes, a nivel de campus. Otros grupos alrededor del mundo se conectan día con día a Internet. Sin embargo, el cambio más significativo no viene de la adición de conexiones de redes, sino del tráfico adicional. Cuando nuevos usuarios, se conectan a Internet y aparecen nuevas aplicaciones, los patrones de tráfico cambian. Cuando Internet se volvió más popular y los usuarios comenzaron a rastrear información utilizando servicios como gopher y World Wide Web, el tráfico se incremento de nuevo.

El crecimiento en las demandas para las redes no debe ser una sorpresa. La industria de la computación ha disfrutado por muchos años de una demanda continua de mayor poder de procesamiento y de mayor almacenamiento de datos. En el futuro podemos esperar incrementos continuos en la demanda de comunicaciones. Por lo tanto, se necesitarán tecnologías de comunicación con mayor capacidad para incorporar el crecimiento.

Necesidad de una nueva versión de los protocolos TCP/IP

La red Internet global ha tenido varios años de crecimiento exponencial, duplicando su tamaño cada nueve meses o menos. La evolución continúa conforme se conectan más columnas vertebrales de redes nacionales, produciendo un incremento complejo de políticas que regulen la interacción.

La versión 4 del Protocolo Internet (IPv4) proporciona los mecanismos de comunicación básicos del conjunto TCP/IP y la red global. Internet se ha mantenido casi sin cambio desde su inserción a fines de los años setenta. La antigüedad de la versión 4 muestra que el diseño es flexible y poderoso. Desde el momento en que se diseñó el IPv4, el desempeño de las computadoras se ha incrementado en magnitud y desempeño, las tecnologías LAN han emergido, y el número de anfitriones en Internet ha crecido hasta llegar a un total de más de 4 millones. Además, los cambios no ocurren de manera simultánea, el IP se ha adaptado a los cambios de una tecnología antes de adaptarse a los cambios de otras, es por esto, que a pesar de su diseño, el IPv4 también debe ser reemplazado, debido al inminente agotamiento del espacio de direcciones (32 bits). Actualmente, muchas organizaciones tienen varias redes LAN o incluso cuentan con una red WAN. En consecuencia, el espacio de 32 bits que se usa actualmente no puede adaptarse al crecimiento proyectado de la red Internet global.

Aún cuando la necesidad de un espacio de direcciones extenso está forzando un cambio inmediato en el IP, hay otros factores que también contribuyen. En particular, gran parte de éstos se refieren al soporte de nuevas aplicaciones. Por ejemplo, debido a que el audio y el video en tiempo real necesitan determinadas garantías en los retardos, una nueva versión del IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente pre-asignada. Además, como varias de las nuevas aplicaciones de Internet necesitan comunicaciones seguras, una nueva versión del IP deberá incluir capacidades que hagan posible autenticar al emisor. Es por esto que los grupos en el IETF han estado trabajando para formular una nueva versión del IP. La próxima generación se llamará IPv6, la cuál conservará muchas características que contribuyeron al éxito del IPv4 pero con unas cuantas modificaciones.

IPv6 tiene muchos aciertos, incluyendo los siguientes:

- **Incremento en el número de direcciones IP**. IPv6 incrementa las direcciones IP de un espacio de 32 a uno de 128 bits.
- **Configuración de dirección automática.** Esto permite asignar una dirección IP válida dinámicamente. La autoconfiguración hace más simples las cosas por la asignación automática y el proceso de detección de NICs a hubs, ruteadores y switches.

- **IPv6 define un encabezado de longitud alterada de 320 bits con 8 campos.** Aunque el nuevo encabezado es más largo que el usado con IPv4, este cambia un número de opciones entre encabezados separados. La extensión de los encabezados añade seguridad y opciones de destino, y también puede trabajarse para agregar comandos de control de paquetes acostumbrados. Bajo el estándar anterior, se almacenaban más opciones en el encabezado, y los ruteadores tenían que leer y procesar cada opción; con IPv6, los ruteadores leen y procesan sólo la información relevante.
- **Incluye características QoS.** El objetivo primario para QoS es multimedia. El nuevo protocolo de reservación de recursos (RSVP: Resource Reservation Protocol) permitirá a los administradores de la red, dedicar ancho de banda disponible a aplicaciones de multimedia. Tal vez este sea el beneficio prometido más grande sin ser tan caro.
- **Provee servicios móviles.** La IP móvil coordina el ruteo de IP entre redes de línea terrestre y de radio (sin hilos).
- **Autentificación y privacidad mejorados.** El IPSec (Seguridad IP) incluye ambos, autentificación de encabezados y el protocolo ESP (Encapsulating Security Payload); éste último encripta el datagrama IP entero, por ello permite la privacidad y la autentificación.

Nuevas aplicaciones

En un futuro se verán nuevas aplicaciones, algunas de ellas ni siquiera imaginables por la mayoría de los usuarios. Pero indudablemente el uso de multimedia y las bases de datos distribuidas serán algunas de las áreas que mayor atención tengan por parte de los desarrolladores. Por otro lado el objetivo de una red Internet, será acercar al usuario más alejado y al último dispositivo de la red de área amplia al escritorio de los administradores, de tal manera que sea transparente si se encuentra en la oficina de junto o al otro lado del mundo.

Las nuevas aplicaciones constituyen una de las áreas de mayor interés por parte del usuario de la red Internet, éstas nuevas aplicaciones cada vez más poderosas e interesantes requerirán un mayor número de recursos de los equipos y de las redes actuales, hoy en día existen importantes usos de Internet, que abarcan principalmente los campos siguientes:

- **Educación**

Actualmente se encuentran establecidas las posibilidades de la educación a distancia por medio de Internet. Este medio se presenta como una herramienta de gran valía en la educación a los usuarios de las redes institucionales educativas y corporativas, pues, si es correctamente utilizada, permite ahorros substanciales en la contratación de instructores y en el desplazamiento de los usuarios hacia los centros educativos (que muchas veces pueden estar incluso en otro país).

- **Comercio**

Con el auge comercial de Internet, cada vez es más frecuente el establecimiento de centros comerciales virtuales, incluso algunas compañías están vendiendo sus

productos directamente por medio de páginas web. Además de poder realizar compras se pueden realizar transacciones de diversos tipos, por tal motivo se requiere de un manejo muy eficaz sobre la seguridad del paso de información de alta confidencialidad. Por esto, en las aplicaciones presentes y futuras se deben incluir mecanismos con un alto grado de seguridad en el paso de la información a través de la Internet global.

Si bien es cierto, ya se ha avanzado en los aspectos antes descritos, sin embargo el crecimiento todavía puede ser mucho mayor tanto a niveles educativos, como comerciales e incluso de entretenimiento.

3.2.4 Otros servicios

Así mismo REDII presta servicios no tan visibles para los usuarios, pero que les son de gran utilidad, a la hora de trabajar en un ambiente de red; dichos servicios son:

Servicio de resolución de nombres

Este servicio se implementó ya que el método para encontrar nodos dentro de Internet se basa en un sistema de direccionamiento que involucra a las direcciones **IP**. Por facilidad para los usuarios a estos nodos se les da un nombre único asociado a la dirección IP, el cuál no es un número sino un conjunto de palabras comunes que identifican a este nodo como único en toda Internet.

Como ejemplo, tenemos que para acceder al servidor principal de la red del Instituto de Ingeniería tenemos dos caminos, la *dirección IP* y el *nombre del servidor*, así pues para hacer referencia al servidor cuyo nombre es: pumas.iingen.unam.mx, se puede hacer uso de su dirección IP, que es: 132.248.53.245 y viceversa.

En realidad la búsqueda del nodo se realiza por dirección IP no por el nombre de nodo, así es que se tiene la necesidad de contar con un sistema que sea capaz de buscar la dirección IP asociada a un nombre de nodo. El sistema que realiza la tarea antes mencionada es el **DNS** (Domain Name System).

El DNS tiene dos aspectos conceptualmente independientes. El primero es abstracto, especifica la sintaxis de los nombres asociados a las direcciones IP, y establece una jerarquía entre dichos nombres. El segundo es concreto, implanta un sistema cliente-servidor, que transforma eficazmente los nombres en direcciones IP.

Acceso vía módem

Investigadores en este Instituto requieren cada día más los servicios de REDII, ya que algunos de ellos tienen la necesidad de trabajar en el interior de la república o desde sus casas y necesitan acceso a todos los servicios de información de la red. Este servicio se proporciona con los protocolos **SLIP** y **PPP,** cabe aclarar que en el momento de escribir éstas líneas el acceso vía módem es restringido, ya que no se cuenta con un gran número de estos aparatos para dar servicio a toda la comunidad de investigadores, sin embargo se esta estructurando un plan para implementar un conjunto de módems para proveer este servicio al mayor número de usuarios posible.

3.3 ADMINISTRACIÓN, MONITOREO Y SEGURIDAD EN LA RED DEL INSTITUTO DE INGENIERÍA

3.3.1 Administración

Un sistema de administración de red es un conjunto de herramientas tanto de software como de hardware que permiten llevar a cabo el control de la red, su función principal es auxiliar al administrador a resolver cualquier tipo de problema que se le presente. De esta manera, podemos decir más formalmente que un sistema de administración de red es la integración de herramientas (tanto software como hardware) que controlan y monitorean la red para obtener el máximo de eficiencia en la misma.

El sistema de administración debe cubrir las siguientes áreas:

- **Administración de fallas.-** El objetivo de esta área es determinar lo más rápido posible el punto de la red donde se presenta una falla para que se corrija inmediatamente.
- **Administración de acceso.-** En esta área se ve el seguimiento de la utilización de los recursos de red por los usuarios. Este tipo de administración es necesaria ya que con ello el administrador puede darse cuenta de que usuarios están abusando de sus privilegios de acceso, que usuarios usan inadecuadamente la red, etc.
- **Administración de desempeño.-** Es el proceso de medición del desempeño de los dispositivos que conforman la red, los aspectos que reflejan el desempeño pueden ser: porcentaje de utilización de la red, capacidad de ancho de banda disponible, tiempo de respuesta en la transferencia de información, tráfico, cantidad de errores, etc.
- **Administración de configuración.-** Involucra la configuración de los elementos de la red, desde una terminal remota. Esta administración involucra los procesos de inicialización, mantenimiento, y paro de los elementos individuales de la red ya sean recursos físicos o lógicos.
- **Administración de la seguridad.-** Es el proceso de control y monitoreo sobre los accesos a la información dentro de la red. Es decir, prohibir el acceso a información restringida, a usuarios no autorizados.

De esta manera, el sistema de monitoreo actual de la red del Instituto de Ingeniería contempla los siguientes puntos:

- Provee una interfaz gráfica para producir una estructura jerárquica de la red.
- Contiene herramientas que permitan medir el desempeño de los nodos administrados.
- Incluye generadores de alarmas y reporte de eventos inusuales en la red.
- Incluye herramientas de análisis y decodificación de protocolos.
- El sistema se basa en protocolos de administración de red estándares y actuales.
- Incluye análisis de datos y herramientas de graficación.
- El sistema es fácil de implantar y de expandir.
- El sistema tiene capacidad para crear desarrollos hechos por el administrador y la posibilidad de integrarlos en el sistema.
- El sistema requiere de un mínimo de equipo adicional.

Así mismo, el sistema de administración y monitoreo se basa en un software conocido como SUNET MANAGER y la versión que actualmente se tiene instalada es la 2.2.2. A continuación hablaremos un poco de este software.

El SunNet Manager (SNM) cuenta con herramientas que pueden proveer tareas de administración de red sobre las siguientes áreas: administración de fallas, de configuración, de acceso, de desempeño, y de la seguridad. SNM está basado en la familia SNMP (Simple Network Management Protocol) para proveer monitoreo y control sobre recursos conectados a través de redes TCP/IP básicamente.

Las características más importantes de SNM son:

1. **Herramientas de usuario.-** Estas herramientas, habilitan operaciones de monitoreo y control de red, y de sus recursos. Las interfaces gráficas son sencillas de usar reduciendo así los requerimientos de capacitación de uso del producto.
2. **Arquitectura distribuida.-** SNM, está basado en una arquitectura de sistema de administración de red distribuida, la cuál proporciona a los usuarios la habilidad de administrar redes que integren elementos de diferentes fabricantes, y que varían en tamaño y complejidad, SNM, puede administrar desde muy pocos nodos hasta miles de ellos.
3. **Interfaces de programación de aplicación API.-** SNM, provee herramientas de desarrollo para construir poderosas herramientas que permitan al administrador complementar la funcionalidad de SNM mediante la creación de herramientas que estén orientadas a resolver problemas específicos.

Se eligió SunNet Manager de entre otros sistemas de monitoreo debido a que cuenta con las características adecuadas para la red que se tiene actualmente en el Instituto, además porque no necesita de una gran cantidad de recursos para su implantación. Otro aspecto importante para la elección de SNM es que la mayoría de las estaciones de trabajo con las que cuenta el Instituto de Ingeniería son de la marca SUN MICROSYSTEMS, de esta manera se pueden aprovechar muchas de las aplicaciones que SunNet incluye, que son específicas para servidores Sun, además de poder implantar dichas aplicaciones a los demás servidores. Otro aspecto que también influyó para la elección de este software fue el costo, ya que es menor al de otros sistemas de administración. Por otra parte SunNet Manager es un sistema robusto que cubre todas las tareas de administración de una forma amigable y sencilla de aprender. La característica más importante para REDII que se encontró en SNM es que provee un ambiente para el desarrollo de herramientas propias, lo cual permite incrementar la funcionalidad del sistema de administración de la red.

Además del SNM, se tienen otras herramientas que funcionan gracias a las características de TCP/IP, permitiendo administrar y monitorear el estado de la red y el comportamiento de las aplicaciones. Algunas de estas herramientas se incluyen con los sistemas operativos y otras más son software de dominio público. Una relación de estas herramientas y su función de detección y corrección de fallas, es la siguiente:

Ifconfig (Interface configuration). Provee información acerca de la configuración básica de la interfaz, es utilizado para detectar direcciones IP, máscaras de subred y direcciones de envío de mensajes de broadcast incorrectas. Esta herramienta es provista con el sistema operativo Unix.

Arp (address resolution protocol). Permite efectuar traducciones de direcciones IP a direcciones Ethernet. Es utilizado para detectar sistemas en una red local que se encuentren configurados con una dirección IP incorrecta o repetida. Arp es considerado como parte de Unix, sin embargo también esta disponible en otros sistemas operativos.

Netstat. Provee varios tipos de información, es utilizado comúnmente para desplegar estadísticas detalladas acerca de cada interfaz de red, sockets y tablas de enrutamiento. Forma parte de los servicios de red que provee Unix.

Ping (Internet control message protocol). Indica cuando un anfitrión remoto puede ser accedido, también es útil para verificar la comunicación con otros dispositivos de red como puentes, compuertas y enrutadores. Despliega algunas estadísticas como son los paquetes perdidos y el tiempo de envío. Es parte de Unix, aunque también está disponible en otros sistemas operativos como VMS, MS-DOS y System 7.

Nslookup. Provee información acerca del Servidor de Nombres (DNS). Permite hacer consultas sobre dominios, anfitriones, registros MX, etc. Forma parte del software BIND de Unix.

Traceroute. Indica que rutas toman los paquetes de información desde el sistema origen hasta el sistema destino. Despliega la información acerca de cada salto (hop). Es de gran utilidad para trazar rutas o detectar fallas en redes remotas. Además es una herramienta de dominio público.

Etherfind (Analizador de protocolos). Esta herramienta, analiza los paquetes individuales que se intercambian entre anfitriones en la red. Etherfind es un protocolo TCP/IP que puede examinar el contenido de los paquetes incluyendo sus cabeceras de información, es muy útil para analizar problemas relacionados con la implantación de protocolos. Otros analizadores de protocolos son el **tcpdump** (para sistemas Unix) y el **lanwatch** (para sistemas MS-DOS).

3.3.2 Monitoreo

El servicio de monitoreo es una de las tareas más importantes dentro de las actividades de administración de toda red de cómputo, sus funciones engloban la extracción e interpretación de datos relacionados con el estado de los dispositivos conectados a la red. El operador de la red deberá siempre tener cuidado en llevar a cabo correcciones rápidas de fallas en la red, manteniendo un alto desempeño de ésta, sin olvidar el aspecto de la seguridad.

El desarrollo de una buena función de monitoreo permitirá llevar a cabo una planeación de posibles crecimientos de la red, de la manera más adecuada, basándose en un buen diseño.

Los tipos de monitoreo se pueden agrupar en dos clases:

Monitoreo de red físico: Este tipo abarca los elementos físicos de la red, como son interfaces de comunicación, puertos, canales, etc. Se basa en que todos los cambios de estado (cambios de voltaje por ejemplo) pueden ser medidos y comparados con umbrales de operación. Las funciones de monitoreo de la red física son capaces de analizar los tres primeros niveles del modelo OSI.

Monitoreo de red lógico: En éste se analizan los estados lógicos de los elementos de la red para garantizar el buen funcionamiento de todo el equipo como son: colas, uso de procesador, utilización de puertos, utilización de enlaces, memorias, tráficos, etc.

Dependiendo del tipo de monitoreo se deben considerar otros criterios más específicos como protocolos soportados, etc.

Para facilitar las tareas de administración y monitoreo de la red del Instituto de Ingeniería, ha sido necesaria la adquisición de dos sistemas de administración de redes: el SunNet Manager y el LANVIEW (presenta las mismas ventajas que el SNM, sólo que éste corre en una PC, por lo cuál no se describió a detalle como el SNM), los cuales permiten ambos tipos de monitoreo. Los dos sistemas utilizan el protocolo SNMP como protocolo de administración, de esta manera, los dos permiten una oportuna detección de fallas, adecuada configuración de los equipos y de los dispositivos, asi como un constante monitoreo del desempeño de la red. Todos los resultados arrojados por este sistema permiten efectuar cambios y considerar modificaciones, en la infraestructura de la red.

Como ya se dijo, las características principales que se tienen con estos sistemas de administración es que se puede tener un despliegue de una vista jerárquica de la red del Instituto. Además de que aprovechan la compatibilidad que tienen los equipos con el protocolo de administración SNMP, para monitorear todos los dispositivos sin importar sobre que protocolo de comunicación se desempeñe siempre que éstos tengan habilitado el protocolo SNMP. De esta forma se pueden monitorear sobrecargas en los segmentos, fallas en los servicios y parámetros como porcentajes de errores, colisiones, etc., esto ha permitido un monitoreo completo y confiable del estado de estos dispositivos, además de que se han logrado minimizar los tiempos en el monitoreo de desempeño, detección y corrección de fallas en la red.

3.3.3 Implantación de herramientas de seguridad en el Instituto de Ingeniería

En los ambientes de cómputo distribuido y sobre todo en aquellos que tienen conexión hacia redes externas como la red Internet, se deben tener en cuenta dentro de sus políticas, medidas de seguridad aplicadas a dispositivos de conexión, equipos que brindan soporte de servicios públicos (ftp, sesión remota, finger, correo electrónico, etc.) o que mantienen información crítica para la organización. Por esto deben ser provistos de medidas de seguridad muy rigurosas con la finalidad de mantener su buen funcionamiento y evitar daños o intromisiones no deseadas de personal no autorizado.

En el Instituto de Ingeniería se está llevando a cabo el establecimiento de nuevas políticas de uso y prioridades en los equipos conectados. Además se están instalando herramientas que realicen el monitoreo y control de ciertos aspectos del sistema.

Cabe aclarar que la seguridad a la que nos referimos en este apartado es sobre la información y su translado entre los dispositivos de la red, tales como switches, concentradores y ruteadores, mas no se refiere a la seguridad propia de los equipos ni a la transferencia de información cuando se usa internet.

Estas herramientas cubren en la medida de lo posible, los puntos principales que pueden ser automatizados en la seguridad de los anfitriones. De acuerdo a las necesidades básicas del Instituto, se decidió instalar y configurar herramientas de seguridad, algunas de ellas serán descritas a continuación.

1. **NPASSWD.** Es un programa que forza a que las claves secretas (passwords) de los usuarios cumplan ciertas reglas de seguridad, antes de que estos sean dados de alta. Npasswd no es un generador aleatorio de claves secretas, el usuario es libre de elegir su clave, pero debe de cumplir con ciertos criterios como son que la clave contenga un número mínimo de caracteres, que no contenga caractères ilegales, que sea una combinación de letras mayúsculas y minúsculas, que no este formada por información personal, etc.

2. **COPS (Computer Oracle and Passwd System).** Es una herramienta de seguridad que permite el diagnóstico y reporta el estado de una máquina Unix. El sistema es básicamente un programa de intérprete de comandos (shell script) que ejecuta varios subprogramas, en general analiza los permisos de los archivos, directorios, dispositivos, claves, grupos de archivos, el contenido del archivo /etc/rc y archivos cron. Además cambia el estado SUID, los permisos de escritura de los directorios (home), archivos de inicialización de los usuarios (profile, .cshrc), etc. Cabe mencionar que COPS no corrige ningún problema que encuentra y no es necesario tener la clave del administrador del sistema para correrlo.

3. **TCP-Wrapper.** Una de las técnicas más utilizadas para limitar el acceso entre sistemas conectados a la red es el **control de acceso**, esta técnica consiste en verificar la dirección IP del anfitrión que solicita un servicio, contra una lista de control de acceso. Si la lista indica que el anfitrión visitante puede utilizar el servicio solicitado entonces su acceso es permitido, en caso contrario el acceso al anfitrión es denegado. En sistemas Unix el control de acceso más utilizado es el llamado TCP-Wrapper, cuya principal característica es el acceso a servicios de red tales como FTP, Telnet, Finger, etc. TCP-Wrapper realiza dos funciones básicas: registrar las peticiones de servicios (independientemente de si tienen acceso o no), y proveer un mecanismo de control de acceso a servicios de red. El registro de peticiones de servicio es una excelente herramienta para monitorear el uso de los servicios de red, de gran ayuda para la detección de actividades ilegales (personal no autorizado), pero su poder real es su habilidad para controlar el acceso a los servicios de red.

Es importante destacar que aunque estas herramientas ayudan a mejorar la seguridad del Instituto, se siguen probando otros esquemas y herramientas de seguridad para implementarlos a futuro.

3.4 ANÁLISIS DE RENDIMIENTO DE LA RED ACTUAL

3.4.1 Elaboración de pruebas de desempeño

Para llevar a cabo el análisis de rendimiento de la red, se prepararon dos tipos de pruebas cuyo esquema se basa en la transferencia de paquetes a través de la red. Las pruebas se aplicaron durante dos semanas, 3 veces al día, dichas pruebas fueron:

- **Prueba de Transferencia de Archivos (FTP)**

Para llevar a cabo esta prueba se seleccionaron varias estaciones de trabajo (1 por edificio) con características similares, tales como; capacidad en memoria, velocidad en la tarjeta de red, carga de trabajo, etc. Para establecer las conexiones diariamente y a tres horas del día diferentes, las conexiones se establecieron a las 10:00 de la mañana a las 3:00 de la tarde y a las 8:00 de la noche, con el fin de tener diversas mediciones del tráfico de red ante diferentes circunstancias de carga de trabajo en la misma. Las pruebas consistieron en llevar a cabo un ftp con un archivo de tamaño fijo (1 MB), de una estación ubicada en el edificio 12 (atlas) a otras estaciones ubicadas en los otros edificios que conforman la red. Así mismo se llevo a cabo la prueba con una estación ubicada en la DGSCA. En la prueba, se hacía una transferencia manual o programada del archivo y se registraban tanto el tiempo de transferencia como la velocidad a la que se había llevado a cabo. Las estaciones elegidas fueron las siguientes:

- Atlas ubicada edificio 12, estación de la cual se mandaba el archivo.
- Gea ubicada en el edificio 1, estación que recibía el archivo.
- Gauss ubicada en el edificio 2, estación que recibía el archivo.
- Blues ubicada en el edificio 4, estación que recibía el archivo.
- Hidros ubicada en el edificio 5, estación que recibía el archivo.
- Donky ubicada en el edificio 6, estación que recibía el archivo.
- Titán ubicada en el edificio 12, estación que recibía el archivo.
- Servidor ubicada en DGSCA, estación que recibía el archivo.

Esta prueba se diseño con el fin de obtener datos sobre la eficiencia en la transferencia de información en la red, así como saber en donde se originaban los cuellos de botella, y determinar el segmento de red con mayor carga de trabajo para que al implementar la solución de la red ATM, sea posible distribuir las cargas de la manera más adecuada. Los resultados se muestran y analizan en el siguiente subtema.

- **Prueba de establecimiento de la conexión (PING)**

En este caso se utilizaron las mismas estaciones que en la prueba anterior, pero además se incluyeron 2 PCs ubicadas en los edificios 3 y 8. Cabe aclararse que en la prueba de ftp, no fue posible incluir máquinas de estos edificios ya que en ellos no hay estaciones de trabajo que cumplieran las características necesarias para llevar a cabo la prueba de manera uniforme. Esta prueba consistió en ejecutar desde Atlas un ping a cada una de las estaciones y PCs mencionadas, esperar 10 transmisiones y obtener el tiempo promedio de la transferencia. El paquete que se envió fue de 64 bytes en todos los casos. Esta prueba se llevó a cabo todos los días de las 2 semanas, inmediatamente después de los ftp´s. Esta prueba se diseño con la finalidad de obtener parámetros similares a los buscados en la prueba del ftp.

- **Prueba del nivel de tráfico por segmentos en la red**

Esta prueba consistió en llevar a cabo un monitoreo durante dos semanas de la situación del switch principal de nuestra red, para determinar en que segmento de la misma se está llevando a cabo una saturación del ancho de banda y poder establecer soluciones a futuro. Para llevar a cabo esta prueba fue necesario aplicar un reset a los contadores de nuestro equipo principal y registrar los datos de paquetes enviados por cada puerto. Con esta prueba sabremos que segmento de la red está siendo más utilizado y por consiguiente cuál de los segmentos requiere de una distribución de cargas más eficiente.

- **Prueba de nivel de colisiones**

Esta prueba consistió en llevar a cabo un registro durante 15 días de las colisiones producidas en nuestros concentradores principales ubicados en cada edificio, para esto también fue necesario reiniciar los equipos. Con esta prueba conoceremos que tan frecuentes son las colisiones en nuestra red, lo cuál es un parámetro de mal uso de la misma o bien, que existen, en un segmento determinado, equipos con problemas que hay que corregir ya que están haciendo un mal uso del canal de comunicación. Los resultados obtenidos en cada una de las pruebas antes mencionadas, se analizarán en el siguiente apartado.

3.4.2 Análisis de resultados y conclusiones

En las pruebas del FTP obtuvimos los datos de las velocidades de transferencia así como los tiempos en que se hacían las mismas; en base a esos datos se generaron dos gráficas de los promedios de velocidad (figura 3.10) y tiempo por edificio o estación de trabajo (figura 3.9).

Resultados de la prueba de FTP (Tiempo)

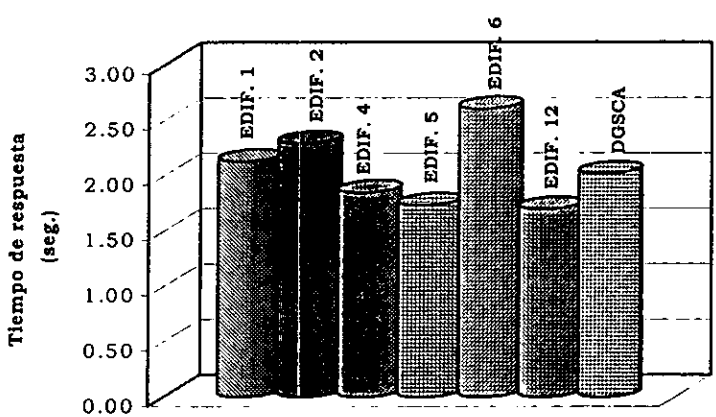


Figura 3.9

En la gráfica anterior, podemos observar los resultados del tiempo promedio que se obtuvieron al transferir un archivo entre el edificio 12 y cada uno de los servidores. Como se podrá observar el menor tiempo lo hizo el servidor Titan (edificio 12) lo cuál era de esperarse ya que este servidor se encuentra ubicado en el mismo segmento de red que el servidor atlas (del cual se llevaron a cabo las pruebas). Por otra parte, el mayor tiempo de respuesta fue registrado en el servidor Donky, ubicado en el edificio 6, de acuerdo a este resultado podemos concluir que el segmento de red más saturado, es el que va del edificio 12 al 6. Así mismo notamos que para el servidor Gauss (edificio 2) también hay un tiempo de respuesta considerablemente alto, lo que nos indica que el ancho de banda en este segmento está siendo insuficiente para descargar el número de paquetes que se producen. Un resultado importante de esta prueba es que, el segmento que nos enlaza con el servidor (DGSCA), está funcionando en niveles aceptables (alrededor de 1.95 segundos por cada MB de información), este resultado es de gran utilidad ya que antes de llevar a cabo esta prueba se creía que el principal cuello de botella se estaba originando entre nuestro switch principal y el segmento de enlace hacia DGSCA.

La siguiente gráfica nos muestra los resultados promedio de velocidad de transferencia por cada servidor, en ella simplemente se corrobora la saturación de los segmentos de la red, ya mencionada, de donde el segmento del edificio 12 al 6 representa la mayor lentitud en la transferencia de paquetes, siguiéndole el segmento de red que va del 12 al edificio 2. Por su parte el enlace local (del 12 al 12) resulto ser el más veloz. La gráfica es la siguiente:

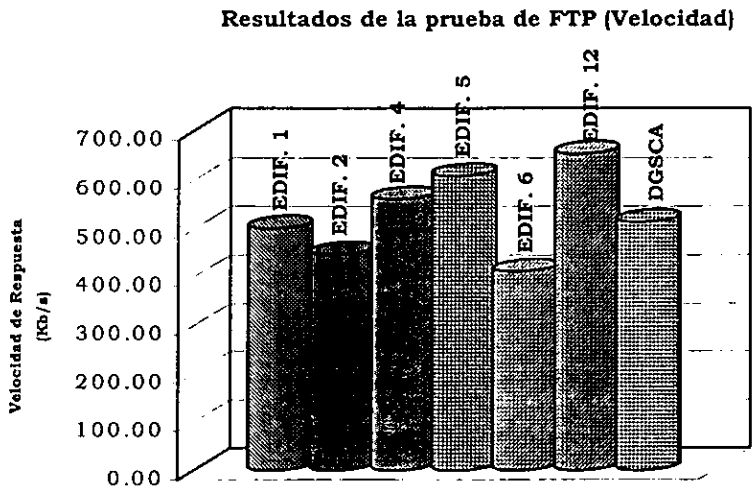


Figura 3.10

Una tabla resumen de los resultados de la prueba del FTP es la siguiente:

No. de segmento	Del edificio	Al edificio	Velocidad (Kbps)	Tiempo (segundos)
1	12	1	490	2.12
2	12	2	447	2.29
3	12	4	560	1.85
4	12	5	599	1.78
5	12	6	398	2.60
6	12	12	658	1.63
7	12	DGSCA	510	1.98

De igual manera, en la figura 3.11, mostramos la gráfica de los tiempos de respuesta promedio obtenidos en la prueba del ping.

Resultados de la prueba del PING

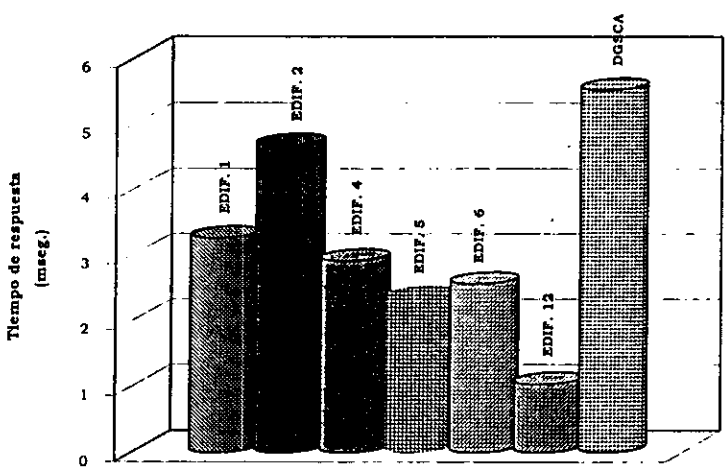


Figura 3.11

En este caso los tiempos de respuesta más altos fueron registrados por DGSCA y el edificio 2, y nuevamente el edificio 12 resultó ser el de menor tiempo de transferencia de paquetes. Comparando este resultado con el obtenido en la prueba de FTP podemos ver que el establecer la conexión es un poco tardado de aquí hacia DGSCA y hacia el edificio 2. Por otro lado, en esta prueba es comprensible que DGSCA registre un gran tiempo a la hora de llevar a cabo una conexión hacia un servidor ubicado allá debido a que se tienen que hacer las rutas lógicas de conexión para permitir el enlace, sin embargo también es posible que se esté originando un cuello de botella en el switch principal debido a que todos los paquetes de información concurren y el ancho de banda es insuficiente como para permitir una rápida velocidad de transmisión. Por otra parte el resultado que se generó en el edificio 2 nos indica que es necesario revisar la distribución del equipo en ese segmento, ya que existe un tiempo alto de gestiones entre equipos para poder llevar a cabo una conexión.

Para el caso de la prueba sobre el nivel de tráfico que presenta cada segmento de red, obtuvimos que el mayor nivel de tráfico se presenta en el segmento del edificio 5, esto es razonable ya que es ahí donde existe la mayor concentración de nodos, en segundo lugar tenemos al edificio 12.

Los demás edificios presentan un nivel aceptable de paquetes enviados, por lo que en este caso debemos de reorganizar la estructura de cargas en los edificios 5 y 12 para aprovechar otros segmentos y distribuir de manera uniforme los paquetes de información. En la figura 3.12, vemos las estadísticas de paquetes enviados por segmento, cabe aclarar que la barra del edificio 6 no se incluyó en este caso debido a que como ya mencionamos no tiene conexión directa al switch principal.

Paquetes Transmitidos (Switch)

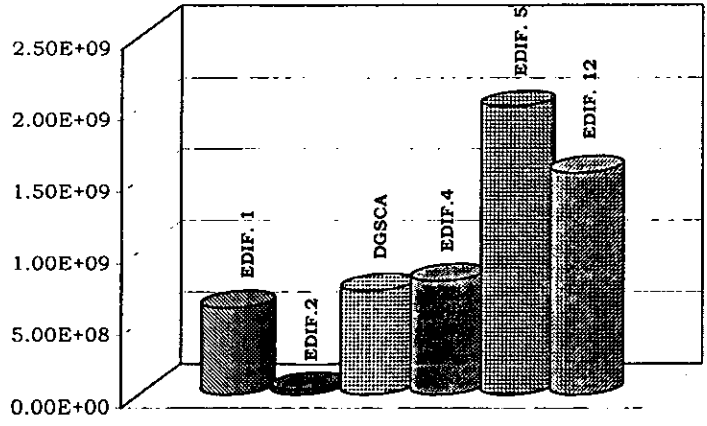


Figura 3.12

Esta prueba muestra que nuestro enlace con RedUNAM es eficiente, ya que no hay una gran carga de paquetes para ese segmento. Esto nos indica que los cuellos de botella que se están presentando en nuestra red, son en segmentos internos de la misma, específicamente en los edificios 5 y 12.

Los resultados de la última prueba, la del nivel de colisiones por edificio, nos muestra que existe un número considerable de ellas en los edificios 3 y 5, mientras que los edificios 1, 2, 4 y 6 presentan niveles menores a los dos millones de colisiones que con relación al número de paquetes que enviaron, es aceptable. El edificio 12 no presentó ninguna colisión, lo que quiere decir que las máquinas que en él se encuentran en cuanto a contendencia por el medio de comunicación, no presentan problemas. En la siguiente gráfica (figura 3.13) se muestran los resultados correspondientes a esta prueba.

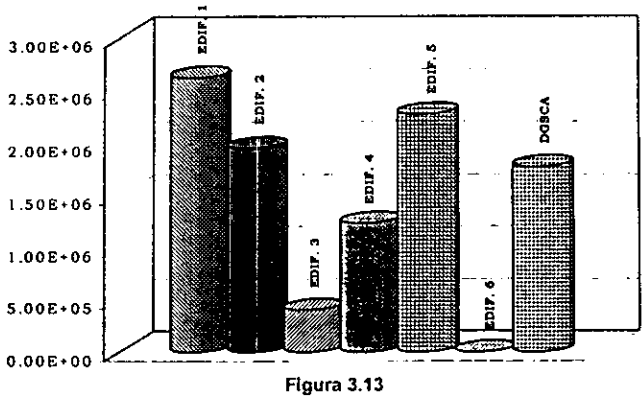


Figura 3.13

Como vemos en el edificio 1 es donde existen máquinas que constantemente envían simultáneamente sus paquetes de broadcast para accesar al medio de comunicación, este resultado no quiere decir que todas las máquinas de ese edificio estén presentando un problema de acceso, puede ser que solo algunas de ellas lo estén originando, de cualquier manera se tendrá que detectar la o las máquinas que están originando dichas colisiones para verificar sus dispositivos de conexión con el hardware de red correspondiente.

Una situación similar a la anterior se presenta en los edificios 2, 5 y 12. Los demás edificios presentan colisiones pero en un nivel mucho menor, de hecho las colisiones siempre existirán ya que son propias del método de acceso al medio que manejan las redes Ethernet, sin embargo el nivel de colisiones no debe sobrepasar el 10% con relación al total de paquetes enviados por cada segmento.

De todas las pruebas anteriormente mostradas, podemos concluir que los puntos a concretar al implementar la red ATM son:

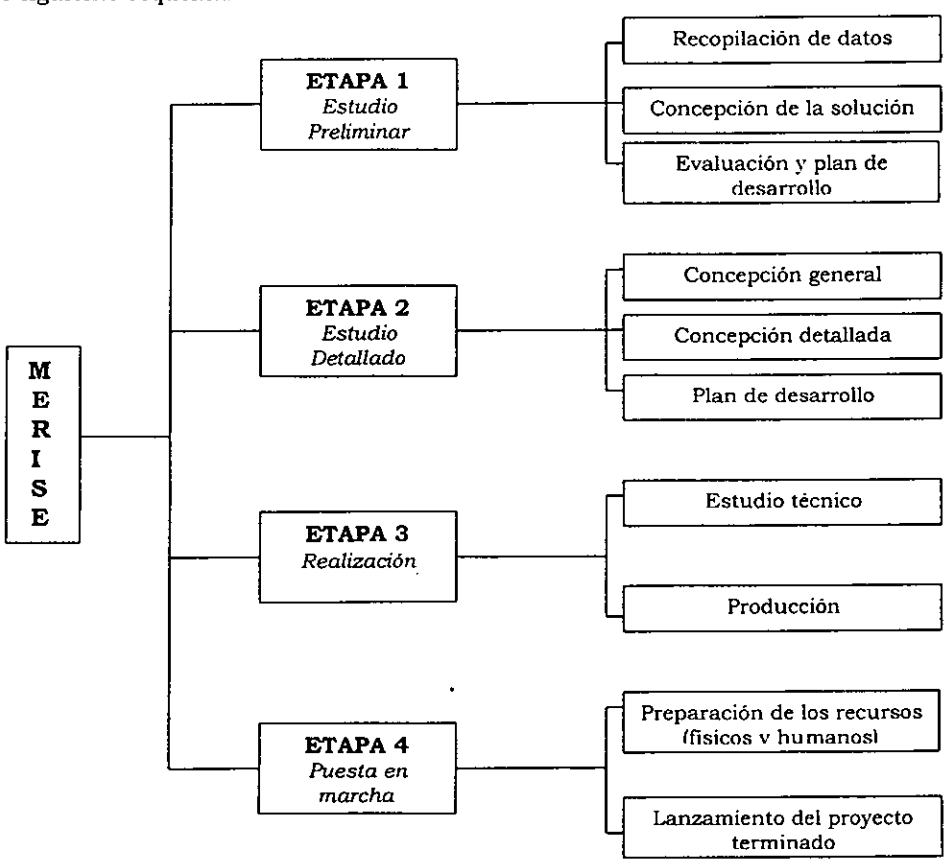
- Ampliar el ancho de banda total que se maneje en el backbone de la red.
- Distribuir cargas en los edificios de manera uniforme.
- Distribuir el tráfico de red lo más uniformemente posible sobre los segmentos disponibles.
- Revisar en cada segmento, las máquinas que presentan problemas de acceso y reparar su interfaz de red o cambiarla.

4.- ESTUDIO DE LA SOLUCIÓN ATM

4.1 METODOLOGÍA DE ANÁLISIS, PLANEACIÓN E IMPLEMENTACIÓN

La finalidad de elegir una metodología es tener una guía para planear, implementar y evaluar el desarrollo de una actividad, en este caso la implementación de la red ATM. De entre algunas metodologías ya existentes, tales como la de Merise, SSADM o la de Yourdon, las cuales tienen una serie de bloques generales similares y que deben sufrir algunos cambios para apegarse a un estudio particular, nosotros decidimos, tomando en cuenta los requerimientos de nuestro trabajo, aplicar un resumen de las ideas de la metodología de Merise, la cual propone en esencia, definir 4 etapas diferentes que son: *1) Estudio preliminar, 2) Estudio detallado, 3) Realización y 4) Puesta en marcha o implementación*

A su vez cada una de éstas etapas, consta de varias fases. Las cuales se muestran en el siguiente esquema:



Basándose en el método anterior y considerando nuestras necesidades, las etapas se aplican como sigue.

Parte de la etapa 1 que comprende el estudio preliminar, se abarca en el capítulo 3 del presente trabajo ya que ahí se recabó la información referente al estado actual de la red del Instituto y se establecieron datos importantes para poder concebir la reestructuración de la red. Este capítulo, así como la revisión de la propuesta original para llevar a cabo la migración, conforman la primera fase de ésta etapa. La segunda parte la integran las modificaciones hechas a la propuesta original y la relación con el proyecto de la torre de Ingeniería (fase 2), así como la planeación del método de instalación de la red ATM y el análisis del personal requerido para soportarla (fase 3).

Las etapas 2 y 3, es decir el estudio detallado y la realización, se tocan de lleno en el presente capítulo. A través de las descripciones teóricas de la estructura de la nueva red, por edificios y del backbone, se hace uso de las 2 primeras fases de la etapa 2. Por su parte la fase 3 (etapa 2), establece el plan a detalle para llevar a cabo la migración. La etapa 3 con sus dos fases va implícita en la elección del equipo definitivo para la migración y en la realización práctica del proyecto, así como en la descripción de la distribución final de cargas en la red.

La ultima etapa que es la puesta en marcha, se abarcará en el capítulo 5 del presente trabajo, ya que es ahí donde se hablará de los beneficios de la nueva estructura de red ya en funcionamiento, las pruebas de rendimiento que se aplicarán a la red ATM y el análisis de los resultados obtenidos.

Cabe mencionarse que algunas de las fases definidas en el método de Merise, pueden no verse claras en la descripción de la migración, sin embargo debemos considerar que la metodología se desarrollo en base a la implementación de un sistema computacional y no en base a la migración hacia una nueva tecnología de red, a pesar de ello es una de las metodologías más apegadas al desarrollo de un trabajo como éste.

A continuación se describirán las etapas posteriores al estudio preliminar, basándonos en el método de Merise.

4.2 ANÁLISIS DE LA SOLUCIÓN ATM (ETAPA 2)

Esta etapa abarca el estudio detallado, por tanto se describirán detenidamente los puntos que favorecieron a establecer la concepción de la red ATM.

4.2.1 Revisión de la propuesta ATM.

La propuesta original de la estructura de red ATM, que fue proporcionada como sugerencia por la compañía 3Com, con algunas modificaciones por parte del personal del Instituto, se muestra en la figura 4.1.

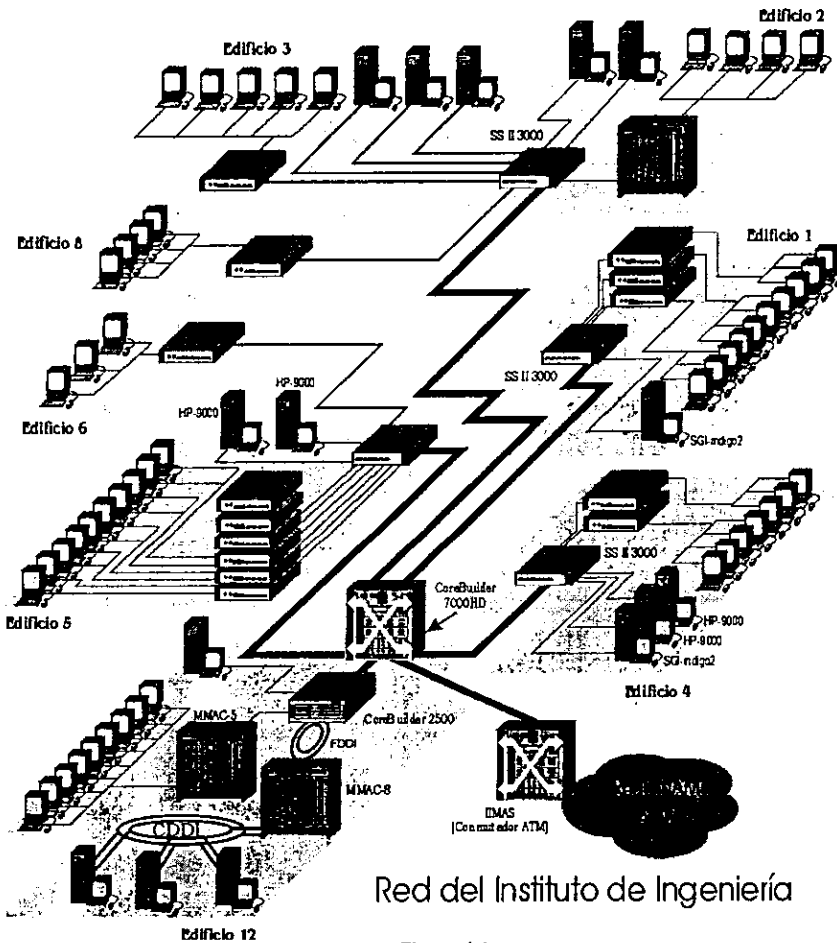


Figura 4.1

Como vemos la propuesta sugiere una distribución en estrella centralizada en el edificio 12, en ella se agrega un equipo CoreBuilder 2500 para proveer un enlace FDDI que soportará un CDDI al cual se conectarán los servidores principales ubicados en este mismo edificio. El switch principal es un CoreBuilder 7000 de 3Com, el cuál llevará a cabo la función de conmutador central del backbone ATM, por tanto a él se conectarán todos los equipos de red que se ubicarán en cada uno de los edificios. Otro aspecto de la propuesta es que se reubicó en el edificio 12 el equipo MMAC-5, que antes se encontraba en el edificio 4, en él se distribuye la carga de tráfico Ethernet. Por otra parte el equipo MMAC-8 se mantuvo en su ubicación original para dar la opción del CDDI. EL CoreBuilder 7000 se conectará mediante un enlace de fibra al backbone ATM de RedUNAM, con lo que se provee la comunicación del Instituto hacia el exterior. Así mismo vemos que para la conexión del FDDI al backbone ATM se instaló un conmutador/enrutador (CoreBuilder 2500) configurado en 2 enlaces, uno ATM y uno FDDI, mediante los cuales se llevará a cabo la integración.

Por otra parte vemos que para la conexión de los edificios restantes se propone instalar un conmutador apilable SuperStack II 3000 (se usará SS 3000 indistintamente para referirnos a éste con puertos Ethernet (auto sensibles 10/100); estos equipos se ubicarán en los edificios 1, 2, 4 y 5, y se configurarán con un enlace directo ATM para la conexión hacia el backbone. En cada SuperStack II 3000 se concentrará el equipo local por edificio. En este aspecto es importante hacer notar que los edificios 3, 6 y 8 no cuentan con un equipo propio SS 3000, ya que el número de usuarios en ellos es reducido, y no es justificable la inversión en un equipo de estas características, por tanto los enlaces se tomarán de equipos instalados en otros lugares y se harán usando fibra óptica para garantizar el mejor funcionamiento de los mismos.

Como vemos, esta propuesta, centraliza las funciones administrativas y de control de la red en el edificio 12, lo cuál representa una ventaja dado que el personal de la Coordinación de Cómputo encargado de la integridad de la red se encuentra en ese edificio. Aunque presenta una distribución de cargas en la red, dicha distribución no es adecuada en algunos edificios, por lo que en este aspecto se necesitarán cambios para permitir ocupar al máximo el equipo ATM y reutilizar adecuadamente todo el equipo de red actual.

4.2.2 Modificaciones hechas a la propuesta.

La propuesta original se modificó en algunos aspectos, principalmente en la distribución del equipo, así como en la marca del mismo ya que en lugar de instalar equipo 3Com se instalará equipo Cabletron y solamente se mantendrá el equipo CoreBuilder de 3Com, esto fue a causa de los resultados obtenidos en las licitaciones previas, correspondientes a la compra del equipo ATM. Cabe señalarse que estos cambios no afectarán la calidad de funcionamiento de la nueva estructura de red, ya que se consideró que los equipos sustituidos fueran de características muy similares a los adquiridos.

Entre los aspectos que quedaron sin cambio con relación a la propuesta antes mencionada, tenemos los siguientes:

- **Centralización del equipo principal en el edificio 12.** El equipo principal de la red ATM se instalará en el edificio 12, para tener un mejor control de administración y funcionamiento sobre el mismo, esto permitirá al personal encargado de la red solucionar cualquier falla en el menor tiempo posible ya que se evitarán traslados largos de un lugar a otro. Con esta ubicación del equipo se incrementará el aspecto de seguridad en el conmutador principal, que juega un papel critico en el esquema de la red ATM del Instituto. En este equipo contemplamos el conmutador principal (CoreBuilder 7000 o sustituto), el conmutador / enrutador CoreBuilder 2500, el equipo MMAC-8 (concentrador actual del edificio 12) y el equipo MMAC-5 (switch actual de la red ubicado en el edificio 4).

- **Carencia de conmutador SuperStack II 3000 en los edificios 3, 6 y 8.** Ya que el número de usuarios de red es reducido en estos edificios, no se instalarán equipos SS 3000 individuales, ya que no es justificado (económicamente hablando) el gasto

y además porque se prevee que el tráfico de red en estos lugares no será demasiado grande en el futuro. En estos casos el equipo de red local actualmente instalado, se enlazará a uno de los conmutadores ubicados en otro edificio; en este aspecto se acepta que el tráfico del edificio 3 sea manejado por el equipo del edificio 2; así mismo es comprensible que el tráfico del edificio 6 sea manejado por el SS 3000 que se ubicará en el edificio 5. Por lo que respecta al edificio 8, este no dependerá del SS 3000 ubicado en el edificio 2, pero la descripción de su conexión al backbone se mencionará más adelante.

- **Instalación de conmutador SuperStack II 3000 en los edificios 1, 2, 4 y 5.** En estos casos si es aceptable la instalación de estos equipos ya que existe un gran número de usuarios en cada uno de estos edificios y es justificable la compra, no sólo por la cantidad de usuarios que se verán beneficiados, sino porque la relación de costo-beneficio es equilibrada. Así pues se instalarán equipos SS 3000 en estos lugares, los cuales se conectarán con enlaces en línea al backbone principal ATM.

Por otra parte los aspectos que cambiamos son los siguientes:

- **Equipo:** En este aspecto observamos que el CoreBuilder 7000 de 3Com propuesto inicialmente como conmutador principal será sustituido por un SmartSwitch 6500 (usaremos SS 6500 para referirnos a él) de Cabletron Systems, con este equipo se da la posibilidad de establecer un ancho de banda para ATM OC-3 u OC-12, y permite la expansión hacia tecnología Gigabit Ethernet. Además de la velocidad, se obtienen beneficios adicionales como el poder integrar los servidores principales al backbone mismo, ahorrando costo de cableado. Otra sustitución importante, es que todos los SS 3000 contemplados como conmutadores por edificio serán cambiados por equipos SmartSwitch 2200 (abreviado en este trabajo como SS 2200) con puertos Ethernet a 10 Mbps, los cuales se conectarán con un enlace en línea ATM hacia el backbone principal

- **Integración del edificio 8 al backbone de la red ATM:** Para su integración se utilizará una conexión mediante fibra óptica, que se tenderá hasta el edificio 1. En el edificio 1 habrá un equipo SS 2200 el cual proporcionará servicio local, y uno de sus puertos proveerá la conexión de red al edificio 8. El SS 2200, está en un enlace directo al SS 6500 (ATM). Por otra parte se usará un concentrador de 24 puertos Ethernet a 10 Mbps para concentrar los nodos de red necesarios en este edificio, en este caso al igual que para el edificio 6 no es justificable la adquisición de un equipo como el SS 2200, por su baja densidad de nodos.

- **Distribución de las cargas del equipo actual con relación al equipo ATM:** En esta nueva propuesta planteamos una distribución diferente de los equipos conectados en la red para cada uno de los edificios, basada en la gran concentración de paquetes enviados y recibidos que existe en los edificios 1, 2, 5 y 12 principalmente. Para llevar a cabo esta nueva distribución nos ayudamos de los resultados obtenidos en las pruebas aplicadas a la red, descritos al final del capítulo anterior. En esta distribución tratamos de saturar lo menos posible cada uno de los puertos disponibles en los switches 2200, esto por ende nos llevó a distribuir uniformemente los equipos conectados actualmente en cada edificio.

Además de distribuir los equipos de red, se reordenaron los servidores principales de cada uno de los edificios para asegurar un canal de comunicación dedicado en el switch que se encargue exclusivamente de la carga de trabajo de estos servidores.

En general los puntos antes mencionados son los aspectos que se revisaron para establecer la nueva propuesta de implementación de la red ATM, esta nueva propuesta de estructuración de la red, se muestra en la figura 4.2.

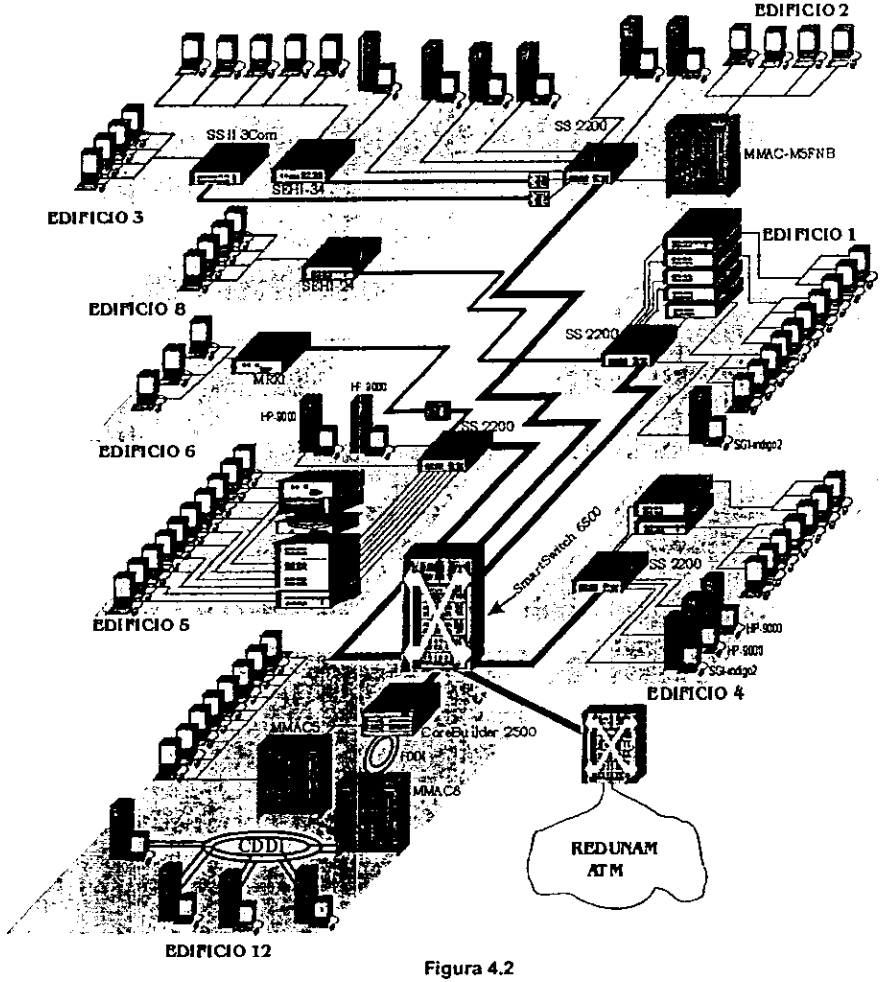


Figura 4.2

Observando el gráfico de la propuesta, vemos que existe una segmentación de la red ATM la cuál ofrece flexibilidad para cambios a futuro sobre todo en cuanto a integración de nuevo equipo, sin la necesidad de parar el funcionamiento de la red en su totalidad, ya que la segmentación nos permite realizar cambios por etapas.

Además de esto la propuesta ofrece una plataforma de red sólida para recibir a futuras tecnologías que podrán implementarse sin tener que realizar una reestructuración total del esquema de red. En subtemas posteriores, se describirá detalladamente el esquema de red ATM para cada edificio, así como el estado del backbone.

4.2.3 Relación con el proyecto de la torre de Ingeniería.

La torre de Ingeniería es un edificio que contará con grandes avances tecnológicos, en cuanto a su infraestructura, su red de comunicaciones deberá contar con la integración de voz, datos y video trabajando a alta velocidad. Es por ello, que la red del Instituto de Ingeniería deberá ser lo suficientemente robusta para soportar la interconexión con la torre y manejar de manera eficiente, el tráfico de red que de ella emane. Para lograr esto, el equipo ATM deberá soportar al menos un enlace que sea congruente con la tecnología de red instalada en la torre, de esta forma es como la red ATM del Instituto se encuentra relacionada al desarrollo del proyecto de la torre de Ingeniería.

Tomando en cuenta lo anterior podemos asegurar que con el switch 6500, (conmutador principal de la red del Instituto) se pueden proveer enlaces en tecnologías de alta velocidad tales como ATM, Fast Ethernet o Gigabit Ethernet, por lo que cualquiera que sea el esquema de red de la torre se podrá interconectar a la red ATM del Instituto con el mínimo de equipo adicional. Ahora bien, si el enlace no se provee directamente en el equipo SS 6500, contamos con los switches periféricos SS 2200 que también soportan tecnologías de alta velocidad con la simple implementación del módulo adecuado; por otro lado, si el enlace se provee de un equipo de DGSCA, nuestra red manejará el tráfico de información sin problemas de acoplamiento de medios y de cualquier manera se mantendrá un enlace eficiente con la red instalada en la torre asegurando su conexión a RedUNAM, independientemente del equipo físico.

4.2.4 Análisis del personal requerido para dar soporte a la red ATM.

A pesar de que la red ATM que se instalará en el Instituto no será muy extensa, es necesario establecer personal dedicado exclusivamente a mantenerla operando, para lo cual se necesitan distribuir tareas tales como: el monitoreo de la red, la administración de las direcciones IP, el mantenimiento preventivo y correctivo del equipo, el crecimiento de los nodos y la reparación de los mismos, y la conexión de equipo nuevo al existente entre otras. Para cubrir las actividades antes mencionadas, consideramos que el personal mínimo necesario debe ser de 5 encargados, los cuales se distribuyan el trabajo y puedan soportar adecuadamente cada tarea. Este esquema permite establecer 4 personas en servicio activo y una para coordinación. La persona que se encargue de coordinar debe de organizar a sus compañeros para atacar los problemas que se pudieran presentar en determinado momento, también debe servir como vínculo de comunicación entre el monitoreo de la red, el equipo principal y los equipos secundarios que serán revisados por los demás integrantes del equipo de trabajo.

Para mantener una comunicación constante sugerimos contar con mínimo 3 radios con un alcance mínimo de 5 km, los cuales se distribuirían de la siguiente manera: 1

radio para el coordinador, 1 para dos integrantes del equipo activo y el tercero para los otros dos integrantes del equipo activo, de esta manera se podrán resolver las fallas de 3 edificios simultáneamente o bien trabajar todos en una falla de red crítica estando en distintos lugares físicos, pero atacando la misma situación.

También sugerimos rolar las actividades entre todos ellos cada semana, para mantener un constante aprendizaje y un nivel de conocimientos similar. La toma de decisiones entre el grupo podrá hacerse en conjunto, sin embargo es conveniente que el coordinador dé el primer paso en la sugerencia de soluciones a los problemas que se presenten. En este aspecto también es importante considerar que las decisiones que pongan en riesgo el funcionamiento del equipo de red o la integridad de la misma, deberán ser compartidas con el Coordinador de cómputo del Instituto antes de ser llevadas a cabo.

4.3 INSTALACIÓN DE LA RED ATM (ETAPA 3)

La etapa 3 se enfoca de lleno a la realización del proyecto, dado que ésta abarca el aspecto práctico, nos enfocaremos a mencionar las distribuciones finales del equipo, y la estructura definitiva que tiene la red ATM implementada.

4.3.1 Descripción de la nueva estructura del backbone.

El nuevo backbone de la red del Instituto de Ingeniería trabaja en base a una tecnología ATM (OC-3) de 155 Mbps, con topología física de estrella, usando como centro de la estrella un equipo SmartSwitch 6500 que da cabida a todas las conexiones de fibra provenientes de los edificios enlazados en la red. El esquema de cableado de fibra sigue teniendo una configuración de anillo. Además de los 3 pares de fibras ópticas multimodo que se tenían originalmente, se agregó un cable de fibra multimodo de 12 hilos que enlaza directamente los edificios 4 y 12, por otra parte el edificio 8 se integró al backbone utilizando para ello un segmento de cable de fibra multimodo de 3 pares. La estructura del cableado se muestra esquemáticamente en la figura 4.3.

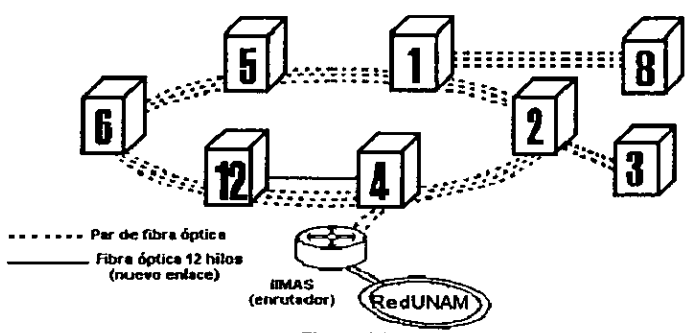


Figura 4.3

Como podemos ver en la figura, se cuenta con un enlace entre los edificios 1, 2, 4, 12, 6 y 5 quienes conforman el anillo principal. El servicio que se da al edificio 8 es mediante dos pares de fibra que se conectan al equipo ubicado en el edificio 1.

Por su parte el ramal del edificio 3 se mantiene mediante 2 pares de fibra óptica multimodo que sale del edificio 2. Un par sirve para enlazar el equipo que habilita los nodos ubicados en el ala frontal de la nave y el otro par se usa para el equipo que se ubica en el ala posterior del mismo edificio.

El esquema de estrella une con un par de fibras, a cada uno de los edificios principales, así pues, en cada cuarto de telecomunicaciones de los edificios 1, 2, 3, 5, 6 y 8 hay un distribuidor de fibras, en donde hay 6 hilos de llegada y otros 6 de salida, en el distribuidor se toma un par de fibras para alimentar el equipo correspondiente y se realiza el puenteo de los 2 pares restantes para llevar la señal a los siguientes edificios. De esta manera y como lo plantea el esquema, todas las fibras parten del switch ubicado en el edificio 12 (centro de la estrella); de aquí se lanza una acometida de cable de fibra óptica de 12 hilos hasta llegar al edificio 4 de donde se usa un distribuidor para tomar un par y conectarlo al equipo local, en el mismo distribuidor se puentean 3 de los pares restantes para que se lance nuevamente una acometida de fibra, en cable rudo, hasta el edificio 2. En este edificio nuevamente se hace uso de un distribuidor para tomar un par de fibras para el servicio local y puentear otros 2 pares para que continúen su trayectoria. Estos últimos pares de fibras llegan al edificio 1 de donde uno de ellos se usa para el equipo local y el par restante se puentea para llegar al edificio 5 donde se conectará al switch local. En el switch del edificio 5 se conectan (mediante un transceiver) dos hilos de fibra que proveerán el enlace de red al edificio 6. Cabe destacar que por esta circunstancia, el equipo ubicado en el edificio 6 depende directamente del edificio 5, por lo que al fallar este último, ambos edificios pierden comunicación con el resto del Instituto.

Así mismo existe un cableado de fibra óptica multimodo de uso rudo desde el edificio 6 hasta el edificio 12 con lo que el anillo en cuanto a trayectorias está completo, sin embargo esta sección no se utiliza por el momento ya que se estableció para ofrecer redundancia en caso de que el enlace principal falle en alguno de sus segmentos.

Cabe señalarse que el Instituto de Ingeniería sigue contando con las 5 subredes para uso local que se mencionaron en el capítulo anterior.

4.3.2 Descripción de la estructura de red en los edificios 1 y 8.

En el edificio 1 mantuvimos los 5 concentradores con tecnología Ethernet 10Base-T que teníamos originalmente, todos estos equipos se conectaron al SmartSwitch 2200 que se instaló en ese edificio. Este switch cuenta con un enlace directo ATM, a través de fibra, al equipo principal ubicado en el edificio 12. El concentrador principal del segmento Ethernet del edificio 1 es un SEHI-24 de 24 puertos en RJ45, tiene una entrada para AUI (DB15) coaxial delgado y una más para fibra óptica; a este concentrador se conectan 3 SEH-24 en cascada también de 24 puertos en RJ45 cada uno y por último se conecta un SEH-34 de 24 puertos a base de telcos (dos con 12 puertos cada uno), este último también se conecta en cascada.

La conexión al SS 2200 se hizo mediante una interfaz EPIM 1 en RJ45, que se instaló en el SEHI-24; puesto que los SS 2200 tienen puertos RJ45, se hizo un crossover del switch al EPIM 1 del SEHI. Para evitar perder el monitoreo en base al módulo de Lan View que soportan los equipos Cabletron, se decidió mantener las conexiones en

cascada, y posteriormente se irán instalando más módulos EPIM a cada uno de los concentradores secundarios para hacer una distribución de cargas más elemental. Con esta configuración mantuvimos los 120 nodos que se tenían originalmente con opción a crecimiento, con el simple hecho de apilar más concentradores hasta cubrir las necesidades del personal del edificio. Es importante destacar que el crecimiento de la red a partir de este momento, puede ser sobre tecnología Ethernet o ATM, ya que la infraestructura permite implementar opciones modulares y paulatinas en cualquiera de las dos tecnologías antes mencionadas.

Por otra parte, la conexión del edificio 8 se hizo usando uno de los puertos del SS 2200 instalado en el edificio 1, dado que los medios eran fibra y UTP se necesito usar un transceiver para el acoplamiento, el enlace entre equipos se hizo mediante un par de fibras en los distribuidores y se utilizó un cable rudo de 3 pares de fibras multimodo para el enlace entre los edificios. El equipo local instalado en el edificio 8 es un SEHI-24 con puertos (Ethernet) RJ45, cabe señalarse que este equipo permite hacer una implementación en cascada con otros concentradores para permitir la ampliación de los nodos de red en caso de ser necesaria. La distribución de los equipos así como las conexiones del mismo se ven en el esquema correspondiente a la propuesta final de la implementación ATM (subtema 4.2.2).

En estos edificios se distribuyeron direcciones IP correspondientes a las subredes 132.248.153.XXX y 132.248.154.XXX de la manera más adecuada para cubrir las necesidades de los usuarios así como para la administración de la red. La distribución física de los nodos de red se mantuvo intacta de acuerdo a lo establecido en el subtema 3.1 del capítulo 3. El equipo principal del edificio 1 se conectó directamente a los puertos del SS 2200 para brindarles un canal de comunicación dedicado y minimizar el tiempo de transferencia de paquetes en la red.

4.3.3 Descripción de la estructura de red en los edificios 2, 3 y 4.

Dado que la ubicación física de estos 3 edificios es muy próxima unos de otros, se decidió mencionarlos en el mismo subtema. El equipo ATM que enlaza los edificios 2 y 3, también es un SS 2200 y se ubicó en el primer entrepiso del edificio 2, es decir, entre los niveles de la planta baja y el primer piso.

El SS 2200 mantiene un enlace directo ATM OC-3 al conmutador principal (SS 6500) del edificio 12, en el switch 2200 se conectó el equipo MMAC-M5FNB de Cabletron Systems, el cuál cuenta con 5 tarjetas, de las cuales, 4 son TPMIM-34 y una IRBM, que cuenta con una entrada AUI y una ST para fibra. Las tarjetas TPMIM-34 proporcionan 24 puertos de red Ethernet mediante 2 telcos, mientras que la tarjeta IRBM provee las posibilidades para la interconexión entre diversos medios de transmisión y también proporciona la opción de monitorear directamente el equipo a través de un puerto serial similar al COM1 de las PCs. De la tarjeta IRBM de este equipo principal, obtuvimos mediante un transceiver AUI a UTP un canal de enlace con el SS 2200, por otra parte, y mediante un transceiver de UTP a fibra fue posible enlazar el equipo de la parte frontal del edificio 3 (Nave), este equipo de red es un concentrador SEHI-34 de 24 puertos a base de telcos (2 de 12 puertos cada uno), este concentrador proporciona red al primer piso del edificio 3 en la parte frontal y también a una parte del área de ingeniería sismológica (planta baja del edificio 2).

Para conectar al backbone ATM el equipo 3Com, ubicado en la parte posterior de la nave, se hizo uso de un par de fibra óptica el cual llega a un transceiver (UTP/fibra) y de ahí se conecta a uno de los puertos del SS 2200. Como se mencionó en el capítulo anterior, el concentrador SuperStack II de 3Com, tiene 24 puertos (Ethernet) en RJ45 y proporciona 20 nodos de red a esta área.

La distribución de nodos de red en estos edificios, así como la distribución de direcciones IP, se mantuvo igual que como se definió en subtema 3.1 del capítulo 3.

Por lo que respecta al edificio 4, también se instaló un equipo SS 2200, que mantiene un enlace ATM con el switch principal del backbone, a este equipo se integró mediante un acoplador de medios AUI/UTP el equipo MMAC-3 que teníamos originalmente, en este equipo hay 2 tarjetas TPMIM-34 de 24 puertos cada una (mediante 2 telcos de 12 puertos cada uno) y proporciona 48 salidas de red las cuales se distribuyen en las dos plantas que conforman este edificio. Las direcciones IP distribuidas, pertenecen a la subred 132.248.153.XXX, la cual se comparte con el edificio 1.

El equipo de cómputo principal en este edificio, también se conectará directamente a los puertos del switch 2200. Cabe mencionarse que mientras DGSCA no nos proporcione un enlace ATM OC-3, nos enlazaremos a RedUNAM a través del switch ubicado en este edificio. Puesto que ésta es una medida temporal, no la especificamos en el diagrama de la propuesta final ATM.

4.3.4 Descripción de la estructura de red en los edificios 5 y 6.

El edificio 5 cuenta con una gran cantidad de nodos de red, por lo que en este edificio fue donde se hizo una distribución de cargas más minuciosa y se necesitaron de mayores recursos para implementar ATM.

En el rack de este edificio se instaló, al igual que en los demás casos, un switch 2200 que mantiene un enlace directo a través de fibra con el equipo principal de conmutación, en este caso se dividió el equipo Ethernet en 4 módulos, cada uno de ellos se conectó mediante transceivers a un puerto del switch local. Los módulos se construyeron como sigue:

El primer módulo, lo conforma un equipo MRXI de Cabletron Systems que proporciona 12 puertos a través de un telco; este equipo se conectó mediante un transceiver (UTP/fibra) a un puerto RJ45 del switch.

El segundo módulo consta de un equipo MMAC-3FNB que cuenta con dos tarjetas TPMIM-34 de 24 puertos cada una (a base de telcos). También cuenta con una tarjeta IRBM que proporciona un enlace mediante un AUI con el switch 2200, para este enlace se ocupó un transceiver AUI/UTP.

El tercer módulo es un concentrador HPJ2602A de Hewlett-Packard de 48 puertos (4 telcos de 12 puertos cada uno), en este caso nuevamente se hizo uso de un transceiver AUI/UTP para lograr el enlace con el SS 2200.

El cuarto módulo y el más importante, se compone de 4 equipos de Cabletron Systems. El equipo principal es un concentrador SEHI-24 que tiene 24 puertos para RJ45, la señal de red que lo alimenta es a través de un puerto EPIM1 (RJ45). A este se conectan en cascada 3 equipos SEH-24 de 24 puertos cada uno, las salidas son RJ45.

Al igual que en el edificio 1, fue necesario mantener las conexiones en cascada para evitar perder el monitoreo del módulo, como es obvio la conexión con el switch 2200 se hizo a través del puerto EPIM 1 instalado en el SEHI-24, en este caso será posible la separación de cada componente del módulo, únicamente si se instala en cada SEH-24 una tarjeta EPIM y se hace una conexión UTP/UTP con cada puerto del SS 2200, así se sigue manteniendo el monitoreo y mejora la distribución de cargas. Esta última solución debe ser gradual y a medida que la economía del Instituto lo permita, ya que el costo de los módulos EPIM es considerable.

Con esta infraestructura, se mantienen los 204 nodos de red Ethernet que se tenían originalmente, las direcciones IP de este edificio corresponden a la subred 132.248.155.XXX. Los equipos de cómputo principales del edificio 5 se conectaron directamente a puertos del switch con lo que la distribución de recursos de estos servidores se hizo más eficiente.

Por lo que respecta al edificio 6, se conecta al backbone ATM a través del equipo 2200 instalado en el edificio 5, este enlace es posible mediante un transceiver UTP/fibra, al cual se conectó el equipo MRXI del edificio 6. Este equipo tiene 12 puertos a base de un telco. En este edificio solo hay 12 nodos, la asignación de direcciones IP, es la misma que se tenía antes de llevar a cabo la migración, dichas direcciones pertenecen a la subred 132.248.156.XXX.

4.3.5 Descripción de la estructura de red en el edificio 12.

El edificio 12 ahora funciona como centro de la estrella, por esto, aquí se instalaron los equipos principales del backbone ATM. En este edificio tenemos al conmutador principal que es un SmartSwitch 6500 de Cabletron Systems, a este switch se enlazan todos los switches 2200 ubicados en cada uno de los edificios principales conectados a la red. El 6500 provee múltiples enlaces ATM a 155 Mbps y permite la creación de las ELANs en las que habitarán los clientes (switches 2200). Por simplicidad de administración se generó una sola ELAN la cual tiene varios LECs conectados a ella. Así mismo el switch 6500, permitirá el enlace ATM hacia RedUNAM, aunque por el momento no es posible hacer aquí la conexión ATM, ya que el módulo Fast Ethernet para el 6500 es mucho más costoso que uno para un SS 2200.

Otro equipo importante que se instaló en este edificio fue el conmutador/enrutador CoreBuilder 2500, este permite enlazar el doble anillo de FDDI con el resto de la red ATM. Como se describió en el capítulo 3, antes de la migración teníamos instalado un equipo MMAC-M8FNB con 8 tarjetas, una FDMMIM-24, seis TPMIM-34 y una IRBM. Actualmente la tarjeta FDMMIM-24 e la que proporciona el enlace FDDI hacia el CoreBuilder. Además de lo anterior, la misma tarjeta provee 4 servicios en RJ45, estos puertos proporcionan mediante un doble anillo en cobre (CDDI) las conexiones dedicadas a los principales equipos de la Coordinación de Cómputo. De las 6 tarjetas

TPMIM-34, sólo se mantuvieron 2 sobre este chasis y las 4 restantes se reubicaron en otro equipo. La tarjeta IRBM para el monitoreo directo del equipo se mantuvo intacta.

Además de lo ya mencionado, otro cambio importante en el esquema del edificio 12 fue la reubicación del equipo MMAC-M5FNB que antes funcionaba como switch principal de la red (ubicado en el edificio 4), en este chasis se instalaron 4 de las 6 tarjetas TPMIM-34 que estaban en el MMAC-M8FNB; esto se hizo con el fin de obtener una mejor distribución de cargas. De esta forma, el equipo MMAC-M8FNB quedó con el FDDI y 2 tarjetas TPMIM-34, mientras que el MMAC-M5FNB quedó con 4 tarjetas TPMIM-34.

La asignación de direcciones IP pertenecientes a la subred 132.248.156.XXX se mantuvo sin cambio, y al igual que en los demás edificios los equipos principales se conectaron directamente al equipo ATM, para ofrecerles un mayor ancho de banda y agilizar sus tareas como servidores.

4.3.6 Descripción de la estructura de red en los edificios externos al campo universitario.

Puesto que estos edificios no están físicamente dentro del backbone de la red del Instituto, y además cuentan con pocos usuarios, su infraestructura de red no cambio y se mantiene tal cual como se describió en el capítulo anterior (capítulo 3). Obviamente los beneficios de la red ATM favorecerán los niveles de transmisión de datos hacia estos sitios externos, en la medida que usen nuestro backbone para llevar a cabo la transferencia de información. Como ya se dijo, son dos las instalaciones de red que tenemos fuera del campo universitario. Una de esas instalaciones es el piso 6 del edificio que se encuentra ubicado en la calle de Esparza Oteo, la otra es la "Mesa Vibradora". La distribución de nodos de red no presentó cambios. Las direcciones IP asignadas para estos nodos de red pertenecen a las subredes 132.248.189.XXX y 132.248.126.XXX respectivamente.

4.3.7 Conexión a RedUNAM

En cuanto a la conexión del backbone del Instituto hacia RedUNAM, esta se hace actualmente mediante un par de fibras que se tienen disponibles en el edificio 4, contamos con otro par para proveer redundancia. Puesto que el enlace por el momento es con tecnología Fast Ethernet (100 Mbps), fue necesario instalar un módulo FE-100FX en el switch que se ubica en el edificio 4 para hacer posible la conexión.

Cabe mencionarse que esta situación es temporal, ya que el enlace con RedUNAM se pretende que sea ATM, y en este caso la conexión se realizará en el edificio 12 ya que es ahí, donde se encuentra nuestro conmutador principal de red (SS 6500). De esta manera tanto el backbone del Instituto así como el enlace hacia el exterior serán ATM puros a una velocidad de 155 Mbps. Con el enlace actual de 100 Mbps, tenemos un canal rápido y confiable para el acceso a Internet y a otras dependencias que se encuentran fuera del campus universitario, sin embargo el dispositivo que lo mantiene no tiene una capacidad de procesamiento tan grande como el switch principal por lo que pretendemos conseguir un enlace ATM-OC3 hacia DGSCA.

Con este enlace nuestro ancho de banda se incrementará considerablemente así como la velocidad en la transferencia. Como se indicó anteriormente la conexión hacia RedUNAM no se ilustra en el plano de la propuesta definitiva desde el edificio 4, sino desde el 12. Por su parte en el esquema del backbone si se nota la conexión desde el edificio 4, lo cual es correcto, ya que físicamente y debido a las trayectorias de la fibra el enlace a RedUNAM se lleva a cabo pasando por este edificio.

4.3.8 Descripción detallada del proceso de instalación

Para llegar a tener la red ATM, antes descrita, fue necesario realizar un plan de instalación que fuera lo más transparente posible para los usuarios. Esto implicó que el funcionamiento de la red de cómputo se suspendiera muy poco tiempo y además que el trabajo de conexiones finales se hiciera en días de poca utilización de la red (un fin de semana). Considerando estos aspectos como prioridades de la migración, realizamos la instalación del equipo ATM por partes, basándonos en un esquema de fechas bien estructurado, elaborando para ello un calendario de actividades y cumpliendo rigurosamente los tiempos destinados a cada actividad. El punto final de las actividades fue la conexión de los equipos Ethernet (ya existentes) al nuevo, y las pruebas iniciales de desempeño. El plan de instalación consistió básicamente en lo siguiente.

Antes de poner en marcha las actividades que planeamos en el calendario para la instalación, que fue de una semana aproximadamente, nos dedicamos a preparar todos los accesorios que se iban a requerir para llevar a cabo las conexiones físicas de los equipos. Los accesorios que conseguimos fueron: cables de fibra, acopladores, transceivers, módulos adicionales, conectores, etc. Así mismo estructuramos una pequeña red, con el equipo ATM con el fin de probarlo (pruebas de laboratorio) y llevar a cabo la configuración de éste. Estas pruebas nos permitieron verificar que el equipo funcionaba adecuadamente y también que la configuración que habíamos hecho era correcta. Previamente a la realización de las pruebas de laboratorio, tomamos un curso de capacitación con personal calificado de la empresa Cabletron Systems, quienes nos instruyeron en el desensamblaje, manejo de componentes, ensamblaje y configuración de los equipos de red a instalar. Por otra parte el esquema de configuración de la red ATM que manejamos fue bajo la estructura de una ELAN y varios clientes, de esta manera en el switch principal 6500 (se generó una red emulada mientras que en cada uno de los switches 2200 distribuidos, así como en el CoreBuilder 2500, se configuró un cliente de esa ELAN común. De esta manera todos residen en un mismo grupo y se provee la interconectividad entre todos los dispositivos conectados al switch 6500 y a los switches secundarios.

Una vez terminadas las pruebas de configuración y ya teniendo todos los accesorios, empezamos con la instalación del equipo nuevo en los racks de cada uno de los edificios, esta actividad se realizó en 2 días. El primer día instalamos el equipo en los edificios 1 y 12, al día siguiente instalamos en los edificios 2, 4 y 5. El tercer día lo ocupamos en preparar las conexiones del equipo nuevo, es decir, en verificar los accesorios y ponerlos en el equipo correspondiente. El cuarto día del calendario se dedicó a verificar e identificar los enlaces de la fibra entre edificios, y la etiquetación de los mismos para hacer las conexiones finales de manera más eficiente.

Los días 5, 6 y 7 se dedicaron a preparar los detalles de las conexiones finales, realizarlas y llevar a cabo las primeras pruebas de desempeño de la nueva red. Estas conexiones se llevaron a cabo mediante un esquema modular, es decir por edificios. En primer lugar conectamos el edificio 4 y DGSCA, verificando que los enlaces estuvieran funcionando adecuadamente, posteriormente llevamos a cabo la conexión del edificio 12, en este caso nuevamente probamos la interconexión de edificios y la salida a RedUNAM, posteriormente conectamos los edificios 2, 3, 1, 8, 5, y 6. En cada caso llevamos a cabo las pruebas de conectividad pertinentes.

La semana siguiente a la instalación mantuvimos a prueba y en monitoreo exhaustivo todos los dispositivos y enlaces para verificar el adecuado funcionamiento de la red. Después de ésta semana se establecieron las condiciones de monitoreo normales.

5.- EVALUACIÓN DE LA FUNCIONALIDAD DE LA RED ATM

5.1 DESEMPEÑO DE LA RED ATM (ETAPA 4)

Esta etapa cambia en relación con la definida en el método de Merise, ya que en nuestro caso particular existe un periodo de evaluación posterior a la implementación de la red. Es por ello que en este capítulo se mencionan los beneficios de tener una estructura de red basada en la tecnología ATM ya en funcionamiento, así como los resultados de las pruebas de desempeño aplicadas a la nueva red.

5.1.1 Aspectos importantes de ATM.

- **SEGURIDAD**

Para construir un sistema de seguridad ATM, lo primero que se debe hacer es identificar los requerimientos de seguridad sobre ATM.

Cuando se habla sobre seguridad de la red, se consideran los siguientes requerimientos:

- **Autentificación:** El usuario es el único que reclama serlo.
- **Confidencialidad:** Solo usuarios autorizados pueden accesar al contenido de los datos.
- **Integridad:** Los datos son alterados por los usuarios durante la transmisión.
- **Desconocimiento:** Un usuario no puede ocultar el hecho que ha accesado a un servicio o datos.

La seguridad viene de la encriptación/desencriptación. Si las llaves usadas en ésta pueden ser obtenidas fácilmente por un individuo, entonces el sistema de seguridad será afectado.

Estructura de la seguridad ATM

En el pasado, los servicios de seguridad se consideraban solo después de que el servicio de red estaba totalmente diseñado. El foro de ATM trata de abolir dichas dificultades considerando la seguridad como una parte integral de ATM.

La estructura de seguridad fue propuesta originalmente por Klasen, Munzert y Nauer en febrero de 1997. Basada en el análisis de los objetivos del cliente, del operador y de la comunidad pública, el proyecto identifica los siguientes objetivos de seguridad como los principales aspectos de la seguridad ATM:

- Confidencialidad
- Integridad de los datos
- Responsabilidad
- Disponibilidad

La confidencialidad y la integridad de los datos son obvias. La responsabilidad significa que todas las invocaciones y actividades de la red deben ser en forma responsable, es decir, que cualquier entidad debe responder por las acciones que inicia. La disponibilidad significa que todas las entidades válidas deben accesar a las facilidades ATM correctamente, no debe ocurrir negación de servicio. Esto es importante para la operación de QoS.

De acuerdo a estos objetivos principales, el proyecto propone las funciones básicas que un sistema de seguridad ATM debe proveer:

- Verificación de identificaciones: El sistema de seguridad debe establecer y verificar la identidad aclamada de cualquier usuario de una red ATM.
- Acceso controlado y Autorización: Los usuarios no deben obtener acceso a la información o recursos si no están autorizados.
- Protección de confidencialidad: Los datos almacenados y comunicados deben ser confidenciales.
- Protección de la integridad de datos: El sistema de seguridad debe garantizar la integridad de los datos almacenados y comunicados.
- Responsabilidad Obligada: Una entidad no puede negar la responsabilidad de sus acciones realizadas así como los efectos de las mismas.
- Actividades de "logging": El sistema de seguridad debe soportar la capacidad de recuperar la información acerca de las actividades de seguridad en los elementos de la red con la posibilidad de rastrear esta información a individuos o entidades.
- Reporte de alarma: El sistema de seguridad debe generar notificación de alarma sobre ciertos eventos ajustables y relacionados a la seguridad.
- Revisión (auditoria): Cuando ocurren violaciones de la seguridad, el sistema debe analizar los datos de "logeo" relevantes.
- Restablecimiento de la seguridad: El sistema de seguridad debe recuperarse de violaciones de la seguridad exitosas o de intentos de dichas violaciones.
- Manejo de la seguridad: El sistema de seguridad debe manejar los servicios de seguridad derivados de los requerimientos anteriores.

Ámbito de la seguridad ATM

Para identificar el ámbito de seguridad ATM, primero tenemos que observar la arquitectura de ATM. Ésta incluye 3 planos:

1. Plano de usuario.
2. Plano de control.
3. Plano de administración.

Un plano incluye entidades. Las entidades en el plano del usuario son usadas para transferir datos de usuario. Mientras las entidades en el plano de control tratarán con

el establecimiento de la conexión, liberación y otras funciones de la conexión, las entidades del plano de administración realizarán funciones de manejo y coordinación relacionadas con el plano de usuario y el plano de control. En particular, el plano de administración incluye las funciones de PNNI relacionadas al establecimiento de una infraestructura de ruteo. Además las entidades en estos 3 planos, son entidades de la capa ATM. Las entidades de la capa ATM realizan transferencia de datos ATM en nombre de las otras entidades en los 3 planos. La relación entre estos planos se muestra en la figura 5.1:

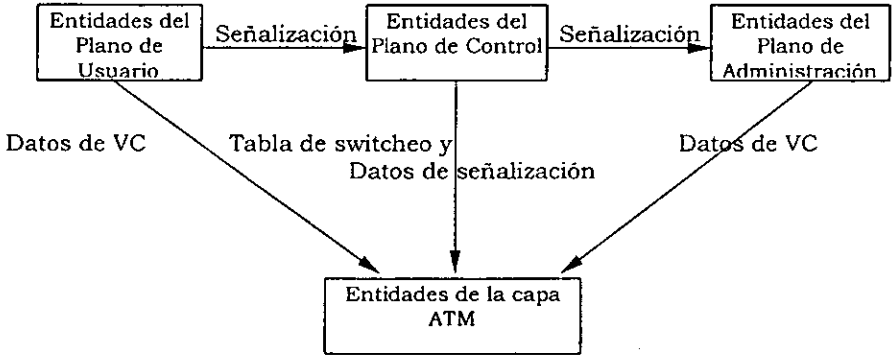


Figura 5.1

Para implementar los requerimientos de la seguridad en redes ATM, los 3 planos y la capa de ATM deben ser incluidos en el ámbito.

Colocación de los servicios de la seguridad ATM

El plano del usuario es el que directamente interactúa con el mismo, por lo tanto para conocer los objetivos de la seguridad del usuario éste plano tiene que proveer servicios de seguridad como control de acceso, autentificación, confidencialidad de los datos e integridad. Otros servicios como el intercambio de clave (key), infraestructura de la certificación y negociación de las opciones de seguridad, podrían ser útiles para conocer la variedad de los requerimientos de los clientes. Las conexiones diferentes tienen diferentes requerimientos de seguridad. Los servicios de seguridad del plano de usuario tienen que proveer suficiente flexibilidad para conocer estos requerimientos.

En el plano de control se configurará la red para proveer el canal de comunicación para un usuario. El plano de control puede interactuar con la tabla de switcheo o manejar el canal virtual. Muchas cuestiones mencionadas anteriormente se relacionan con este plano, por lo que es muy importante el control de la seguridad. La clave para el control seguro puede ser proveer la autentificación y confidencialidad de la señal. Si el destinatario del mensaje o incluso el grupo de trabajo pueden verificar el origen de este mensaje, la negación del ataque del servicio no puede ocurrir. Y la autenticación del plano de control podría también ser usada para proveer información de auditoria (revisión).

La seguridad del plano de administración es también importante. En este plano, se deben considerar los siguientes puntos: "seguridad de escucha" (bootstrapping), descubrimiento del usuario autentificado, la seguridad de la Interfaz de la Administración Local Interina (Interim Local Management Interface) y seguridad permanente del circuito virtual. En la estructura de la seguridad, debemos proveer la recuperación de la seguridad y administración de la seguridad.

Ya que todos los datos han sido transmitidos a través de la capa ATM, la seguridad de esta capa a lo largo de todo el enlace es extremadamente importante. La autentificación, confidencialidad e integridad son también requerimientos de la capa ATM.

Una conexión en la capa ATM no es lo mismo que una conexión realizada en una capa más alta. Por lo tanto aunque una conexión ATM es autentificada y segura, la conexión de una capa más alta debe ser autentificada y protegida. Esto es especialmente necesario cuando una conexión se establece por una red heredada la cual está conectada a un switch ATM. Hoy en día, el tema de la seguridad sobre este caso no ha sido tratado con profundidad.

Avances sobre las especificaciones de seguridad para ATM

Para resolver el problema de la seguridad ATM, el grupo de trabajo sobre seguridad (del foro ATM), está trabajando en una nueva infraestructura de seguridad.

Actualmente el proyecto, en su fase I, detalla principalmente los mecanismos de la seguridad en el plano del usuario y una parte en el plano de control. Esta fase, incluye mecanismos de autentificación, confidencialidad, integridad de datos y control de acceso para el plano de usuario. También incluye mecanismos de autentificación para una parte del plano de control. El plano de administración y el resto del plano de control todavía no han sido estudiados. La especificación también trata algunos servicios de seguridad como son: la negociación de los servicios de seguridad y los parámetros de la misma. Cabe mencionarse, que sólo se especifican los mecanismos que pueden ser implementados en la capa ATM y/o AAL (capa de adaptación ATM).

El objetivo principal de esta fase es proveer una estructura suficientemente flexible, que permita acomodar diferentes algoritmos y longitudes de claves, para proporcionar interoperabilidad y compatibilidad entre dispositivos ATM, así mismo se busca obtener separabilidad de autentificación e integridad de la confidencialidad. La infraestructura también puede soportar un gran número de usuarios, y además es compatible con las versiones sucesivas de las especificaciones ATM.

Cabe señalarse que los mecanismos de seguridad para redes ATM siguen en desarrollo, así como las herramientas para implementarlos, sin embargo dado que nuestra red es híbrida, las herramientas de seguridad aplicadas por el usuario final siguen siendo las descritas para la red Ethernet, vistas en el capítulo 3. A medida que la red del Instituto vaya convirtiéndose en una red ATM pura, se tendrán que ir implementando herramientas nuevas de seguridad adecuadas a los requerimientos de ese momento.

- **ADMINISTRACIÓN**

Por la sofisticación y flexibilidad que presenta ATM, las soluciones que fueron adecuadas para otras tecnologías de administración de redes son insuficientes para el modo de transferencia asíncrono.

El problema de administración de red se debe principalmente al alto nivel de complejidad en las redes de hoy, ya que obligan al administrador a planear métodos sobre nuevos equipos, como son los switches ATM, incrementándose así la dificultad de las tareas.

Mientras las soluciones existentes pueden manejar varios aspectos del problema de la administración de redes competentemente, éstas carecen de sofisticación y utilidad necesarias para hacerlas suficientes para los ambientes ATM del mundo real. Por ejemplo, las herramientas existentes no soportan instalaciones ATM de vendedores diferentes, y los circuitos virtuales son comúnmente configurados sobre dispositivos ATM de vendedores diversos. La flexibilidad que ATM provee en el soporte de clases múltiples de tráfico da una carga más grande a los administradores de red, quienes deben ahora configurar y manejar no sólo una red de voz y datos, sino una red con voz, datos y video integrados. Añadiendo que las redes ATM operan a velocidades extremadamente altas, y que sus circuitos virtuales y velocidades altas poseen nuevos sistemas de seguridad.

Otro desafío es el hecho de que los swithes ATM generan un gran número de alarmas cuando fallan, y la mayoría de las soluciones de administración existentes son inadecuadas para procesarlas.

Por lo anterior, las herramientas de administración de red para este ambiente, deben tener la capacidad de soportar fallas y realizar administración en este ambiente de alta velocidad.

Algo que hay que cuidar en el aspecto de la administración es que debido a que ATM provee sofisticados servicios para usuarios finales, estos pueden también ser explotados por los "hachers", si no se implementan las medidas de seguridad adecuadas.

Estos nuevos requerimientos forman las bases de un nuevo modelo de administración de red para ATM, con una arquitectura sofisticada que es capaz de direccionar las complejidades de ATM. Este modelo tiene características como: un ambiente de conexión orientado, variación de clases de servicio, volúmenes más altos de tráfico, configuraciones de red virtual y tipos de tráfico múltiple.

Administración de fallas

Es un componente crítico del sistema de administración de una red ATM. La administración debe incorporar monitoreo de la red, detección, correlación, diagnósticos y resolución de fallas. Complicando estos requerimientos, está la gran cantidad de mensajes que pueden ser generados de una falla simple en una red ATM, esto hace virtualmente imposible para un administrador de red, el leer, analizar, y actuar apropiadamente en cada situación.

La filtración inteligente de la alarma y la correlación de alarmas es esencial para redes ATM. Los mecanismos de alarma deben permitir al administrador controlar fácilmente las alertas que aparecen en la consola principal. Los operadores deberán obtener diferentes vistas enfocadas al mismo problema. En adición, las alarmas de la red ATM deben estar correlacionadas de tal manera que sólo las alarmas críticas sean enviadas a la estación de trabajo del operador y las secundarias sean suprimidas. Los sistemas expertos deben ser los que guíen a los operadores en el diagnóstico y la resolución de un problema.

Administración de la configuración

Este aspecto debe soportar circuitos virtuales ATM y la administración de los servicios para los usuarios. El sistema de administración de redes debe tomar en cuenta la configuración de PVCs en respuesta a los requerimientos del usuario y de acuerdo a los parámetros QoS tales como el "troughput" y el "delay". Para la administración responsable y rápida las capacidades de configuración deben permitir búsqueda, cambio y borrado de PVCs fácilmente, usando reglas y procedimientos del sistema experto o a través de una Interfaz de Usuario Gráfica (GUI). Este sistema debe proveer las herramientas necesarias para definir tablas de ruteo que soporten los PVCs y aseguren que las tablas ubicadas en diferentes switches estén sincronizadas.

Administración de acceso

Este aspecto del sistema debe describir numerosas conexiones virtuales, identificadores de conexión virtual y rutas virtuales a través de la red y mantenerlas eficientemente. La actividad de ejecución debe ir más allá del monitoreo básico de la red y proveer administración constante para mantener al sistema corriendo en su nivel óptimo. La administración de la configuración, extiende las herramientas de este tipo de administración al soportar circuitos virtuales ATM así como, la administración de los servicios para usuarios tal como, la reconfiguración virtual automática.

Administración de la contabilidad

Para ayudar al consumo eficiente de los recursos disponibles en la red, los mecanismos de contabilidad deben estar integrados a través del sistema de administración de la red.

Administración de la seguridad

Este tipo de administración se refiere a las restricciones de acceso a estaciones de trabajo y aplicaciones de administración, basadas en privilegios asignados. Los mecanismos de revisión deben comunicar y accesar a los recursos. Un seguimiento de las auditorías de varios eventos debe ser un requerimiento de la organización para poder llevar a cabo un análisis posterior que sirva para detectar e investigar accesos no autorizados a los recursos.

La filtración inteligente de la alarma y la correlación de alarmas es esencial para redes ATM. Los mecanismos de alarma deben permitir al administrador controlar fácilmente las alertas que aparecen en la consola principal. Los operadores deberán obtener diferentes vistas enfocadas al mismo problema. En adición, las alarmas de la red ATM deben estar correlacionadas de tal manera que sólo las alarmas criticas sean enviadas a la estación de trabajo del operador y las secundarias sean suprimidas. Los sistemas expertos deben ser los que guíen a los operadores en el diagnóstico y la resolución de un problema.

Administración de la configuración

Este aspecto debe soportar circuitos virtuales ATM y la administración de los servicios para los usuarios. El sistema de administración de redes debe tomar en cuenta la configuración de PVCs en respuesta a los requerimientos del usuario y de acuerdo a los parámetros QoS tales como el "troughput" y el "delay". Para la administración responsable y rápida las capacidades de configuración deben permitir búsqueda, cambio y borrado de PVCs fácilmente, usando reglas y procedimientos del sistema experto o a través de una Interfaz de Usuario Gráfica (GUI). Este sistema debe proveer las herramientas necesarias para definir tablas de ruteo que soporten los PVCs y aseguren que las tablas ubicadas en diferentes switches estén sincronizadas.

Administración de acceso

Este aspecto del sistema debe describir numerosas conexiones virtuales, identificadores de conexión virtual y rutas virtuales a través de la red y mantenerlas eficientemente. La actividad de ejecución debe ir más allá del monitoreo básico de la red y proveer administración constante para mantener al sistema corriendo en su nivel óptimo. La administración de la configuración, extiende las herramientas de este tipo de administración al soportar circuitos virtuales ATM asi como, la administración de los servicios para usuarios tal como, la reconfiguración virtual automática.

Administración de la contabilidad

Para ayudar al consumo eficiente de los recursos disponibles en la red, los mecanismos de contabilidad deben estar integrados a través del sistema de administración de la red.

Administración de la seguridad

Este tipo de administración se refiere a las restricciones de acceso a estaciones de trabajo y aplicaciones de administración, basadas en privilegios asignados. Los mecanismos de revisión deben comunicar y accesar a los recursos. Un seguimiento de las auditorías de varios eventos debe ser un requerimiento de la organización para poder llevar a cabo un análisis posterior que sirva para detectar e investigar accesos no autorizados a los recursos.

Arquitectura

La arquitectura del sistema debe tomar en cuenta una vista integral de la red a través de una consola central, el sistema de administración de la red debe también utilizar una arquitectura de datos centralizada con un sistema de bases de datos flexible para asegurar la máxima eficiencia al accesar, manipular y mostrar datos sobre diversas aplicaciones necesarias para la administración. El definir una buena arquitectura de sistema también ayudará a visualizar los problemas mediante la presentación de un conjunto de mapas de red, desplegando ventanas y menús que ayudarán al administrador a realizar más fácilmente su trabajo.

Simulación y modelado

El papel del sistema de administración de la red puede ser ampliado a ejercicios de simulación y modelado basados en datos reales. Utilizando estos datos, tenemos un reflejo real y preciso del ambiente en el cuál la red está trabajando, con esta información pueden ser producidos mejores modelos para proveer una ayuda adecuada, en la administración de los recursos y al momento de llevar a cabo una reestructuración de la red. Estas herramientas permiten a los administradores de red experimentar con diferentes escenarios para mejorar los diseños alternativos.

Los aspectos antes mencionados sólo son las bases sobre las cuales se establece la administración fundamental de una red ATM, existen varios sistemas de software que permiten llevar a cabo las tareas administrativas, dichos sistemas deben elegirse basándose en el equipo de ATM que se instalará en la red. En nuestro caso, trabajaremos con el sistema SPECTRUM de Cabletron Systems y el TRANSCEND de 3Com, las características generales de estos, se describirán en el siguiente punto.

- **MONITOREO Y CONTROL**

El monitoreo y control de la red ATM, se llevará a cabo con la ayuda de dos sistemas de administración adquiridos basándose en el equipo instalado. Así pues y como ya se mencionó anteriormente se utilizará el SPECTRUM para todos los dispositivos Cabletron Systems y el TRANSCEND para los equipos 3Com. A continuación se describen las características principales de cada uno de estos sistemas.

Administrador de Servicios ATM SPECTRUM

El Manejador de Servicios ATM SPECTRUM, es un paquete de administración basado en estándares, dirigido a realizar la administración de un conjunto de switches ATM. Este paquete provee control centralizado, administración de la conexión, administración de la topología, administración del servicio, administración de la configuración, administración de fallas, administración del ancho de banda y las estadísticas sobre estos niveles administrativos. Esta nueva herramienta provee a los administradores un control total de la red, con lo que se reducen los costos de operación, permitiéndoles incrementar la eficiencia de la misma.

El control centralizado

El SPECTRUM provee una interfaz fácil de usar que satisface todas las necesidades de la administración en ATM.

El software SPECTRUM puede ser instalado en un servidor, un cliente, o bien en muchos clientes separados. Cada cliente puede tomar control de la red de acuerdo a sus privilegios de acceso. Además, para incrementar la facilidad de uso, la documentación del usuario está disponible en línea desde el panel de control, proporcionando a cada operador del sistema un fácil acceso a todos los manuales de usuario, notas sueltas (release notes) y guías de referencia rápida.

A través de la aplicaciones que presenta el SPECTRUM, los administradores pueden manejar la red entera, incluyendo los switches y los dispositivos terminales en una sola plataforma con lo que se reducen los requerimientos y el costo de mantenimiento de múltiples sistemas. Además, su facilidad reduce enormemente el número de técnicos especializados requeridos para manejar switches o dispositivos necesarios en un enlace o circuito (en este apartado se usan indistintamente estos dos términos).

Administración en la conexión

Se usa para el establecimiento de circuitos, monitoreando su estado, e incrementando la efectividad y la tolerancia de fallas en los mismos. De esta manera, una sola interfaz permite analizar elementos fin a fin con sólo seleccionarlos con el mouse; también permite incluir QoS, diferentes tipos de conexión y Servicios de Emulación de Circuitos (CES). Además de lo anterior, muestra el estado del circuito usando un código de colores, incluye detalles y rastreo del mismo, y proporciona una interfaz para la administración del segmento de red analizado.

Los elementos fin a fin establecen circuitos a través de la red entera. Cada circuito puede tener su propia calidad de servicio diseñado para cubrir las necesidades del cliente. El SPECTRUM provee plantillas por default para soportar circuitos de voz, video y datos. Los menús con que cuenta el software, permiten al administrador seleccionar los tipos de conexión y configurar circuitos CES en la red mediante una plataforma de administración simple, reduciendo enormemente los tiempos de configuración.

El SPECTRUM también permite que cada conexión sea configurada por **CBR** (Constant Bit Rate; estos servicios se usan en aplicaciones donde los datos de tiempo real son importantes y la perdida es alta. Es típico de circuitos de voz y video MPEG), **VBR** (Variable Bit Rate) es útil solo para tráfico que no pierde sensibilidad y varía lentamente. Se usa en WANs para voz y video donde no se requiere calidad perfecta), **ABR** (Availabe Bit Rate; típicamente usado para tráfico de datos donde la transmisión libre de error es importante pero no requiere ancho de banda reservado) o **UBR** (Unspecified Bit Rate; es un tipo de tráfico con QoS no garantizado). Se usa sólo para tráfico LAN) provistos por el hardware del switch que soporta a cada una de estas. Esto brinda flexibilidad para elegir el tipo de servicio que la aplicación particular requiera.

Las plantillas por default que maneja el software están basadas en las recomendaciones del Foro de ATM para QoS y parámetros de tipo de tráfico para voz, video o datos. Gracias a esto, proveen una guía general para administradores sin requerir gran habilidad técnica para proporcionar circuitos a través de la red. Un operador puede simplemente agregar un ID al circuito y el nombre del cliente, asignar un VPI o un VCI, seleccionar el tipo de servicio, introducir los nodos finales para el circuito y presionar "enter" para establecer la conexión. El operador también puede escoger ajustar el PCR, el MCR, el ancho de banda, y otras opciones provistas en la pantalla. Aunque éstas vienen por default, se pueden cambiar y salvar como plantillas diferentes, adecuadas a un equipo de red o cliente determinado.

Los tipos de conexiones que el SPECTRUM permite son **PVCs** (usados para conexiones que pueden ser establecidas punto a punto, o punto a multipunto. En caso de falla, el SPECTRUM puede volver a rutear el PVC), **PVPs** (para mayor ancho de banda entre las locaciones y uso de VCs múltiples, incluyendo PVCs, SPVCs y SVCs; Así mismo el SPECTRUM permite establecer PVPs de punto a punto, soportando arriba de 65,000 VCs por PVP) y **SPVCs** (Soft Permanent Virtual Circuits; habilitando un switch para re-rutear automáticamente un circuito en caso de falla).

Ya que **el código de colores relacionado con el estado del enlace** simplifican el monitoreo en la red. Este software ha implementado estos servicios; de esta forma el verde significa que el circuito está activo, el azul muestra cuando un enlace está administrativamente desactivado y el rojo cuando hay una falla a lo largo de la ruta que ha causado la caída del circuito.

Los detalles que SPECTRUM maneja sobre los circuitos, switches y puertos ayudan en el monitoreo y configuración de la red ATM. Estos detalles incluyen representaciones en texto y gráficas de la red. Los detalles del switch muestran su nombre, el nombre de la comunidad y el intervalo del registro de datos, los cuales son configurables por el administrador. Hay otros detalles que no son configurables, como dirección IP, número del puerto, número de usuarios y número de enlaces. Los detalles del puerto incluyen un campo (nombre del puerto) configurable y muchos campos de sólo lectura. Los campos no configurables proveen información útil para seguir la comunicación con cada puerto e incluyen datos sobre el ancho de banda máximo de los VPIs, máximo de los VCIs, así como el número provisto de circuitos por cada puerto.

Para la **selección de ruteo**, el SPECTRUM rutea automáticamente la conexión a lo largo de la mejor ruta. Esta ruta es determinada por contabilidad métrica del circuito para la distancia más corta (switch hops) entre dos puntos finales, contabilizando la congestión del enlace y del switch para proveer el máximo desempeño. En caso de que se desee que el circuito atraviese por un grupo particular de switches o dominios, se puede hacer una selección manual, de los mismos y SPECTRUM determinará la mejor ruta a través de éstos, proveyendo suficiente ancho de banda de acuerdo a los requerimientos del circuito. Los SPVCs se rutean automáticamente por medio del estándar SPVC provisto, el administrador no interfiere con este ruteo.

Administración de la topología

Para proveer este nivel de administración, el SPECTRUM usa el estándar industrial PNNI para manejar cualquier otro estándar (compatible con PNNI). La característica de

esta administración es proveer una vista jerárquica de la red, desplegando representaciones gráficas actualizables al click del mouse. Ambas pantallas, la de topología textual y la de las gráficas utilizan el código de colores para mostrar el estado de los enlaces, switches, puertos y conexiones.

Este aspecto de la administración provee información actualizada y oportuna que permite a los administradores conocer el estado red, lo qué necesita ser arreglado y arreglarlo de manera inmediata. La administración de la topología reduce el número de horas hombre requeridas para establecer un sistema de administración de la red ATM.

Administración de servicios del cliente

Este software provee herramientas, incluyendo las plantillas por default, para el servicio en línea a los clientes, así mismo, permite la creación de plantillas de cliente específicas para facilitar su uso al adicionar o cambiar servicios en un determinado momento.

Administración de la configuración

El SPECTRUM provee la administración de la configuración para redes compatibles con PNNI (actualmente PNNI 1.0). Incluye una herramienta sencilla de configuración para nodos y grupos PNNI en redes jerárquicas multi-nivel.

Administración de fallas

En este aspecto el SPECTRUM ofrece re-ruteo del circuito alrededor de secciones críticas de la red, así como herramientas (troubleshooting) para resolver anomalías de la red. El uso de esta herramienta también proporciona una notificación pertinente de los problemas encontrados en la red.

Como ya se dijo, el SPECTRUM tiene la capacidad de re-rutear circuitos cuando se presentan fallas en la red. Ante una falla del switch, del puerto o del enlace, SPECTRUM volverá a rutear los circuitos afectados por la falla si éstos son configurados para ello. Los circuitos serán re-ruteados basándose en una prioridad asignada. Esta asignación da a los proveedores del servicio de red mayor flexibilidad para niveles y clientes diferentes.

El módulo que maneja los problemas de conexión, provee soluciones a través del uso de pruebas cíclicas, probable origen, alarmas, eventos y aislamiento de fallas. Cada switch a lo largo de la ruta, la estará revisando automáticamente, para conocer el paso y la congestión de los datos. El SPECTRUM también es capaz de determinar la causa probable de cada falla y de reportarla al usuario.

Administración del ancho de banda

El SPECTRUM provee este tipo de administración, así como el monitoreo y la distribución de las cargas en la red para incrementar su desempeño. Esto ayuda a la planeación y predice problemas antes de que ocurran. Cuando la carga monitoreada muestra puntos de congestión, puede ser distribuida o bien se puede adicionar equipo a la red para mitigar la congestión. Cuando la distribución de cargas no se hace

manualmente, el software la distribuirá automáticamente, para esto toma en cuenta el ancho de banda disponible entre los enlaces, así como el disponible en los switches, así mismo observa los periodos de error en el hardware, para determinar la mejor ruta.

Estadísticas

El software de administración SPECTRUM ofrece estadísticas, incluyendo enlaces, switches y circuitos virtuales. También provee estadísticas generales de la red para saber como está trabajando y cuanta carga de trabajo hay en diversas partes de la red. Algunas de las estadísticas que se pueden obtener son:

- Las del switch que es el origen en la mayoría de los circuitos de la red.
- Las del switch que es el destino en la mayoría de los circuitos de la red.
- Las del switch en el que se producen más alarmas.
- Las del switch que es re-ruteado más veces.
- Las totales de los circuitos por tipo (VCs, SPVCs o VPs, punto a punto o punto a multipunto).

Como sabemos éstas estadísticas pueden ser usadas para monitorear el estado de cada enlace y dar información importante al administrador de la red.

Operatividad

SPECTRUM es una aplicación basada en las especificaciones de AToM MIB, PNNI 1.0, PNNI SPVCs, RFC 1483, y en un futuro de PNNI 2.0. Esto le permite observar y manejar cualquier red ATM conformada de dispositivos que soporten estos estándares. Para los casos en que los dispositivos de la red no soporten estos estándares, SPECTRUM puede ser adaptado para soportar otros que permitan llevar a cabo la configuración y el manejo de esos dispositivos.

SPECTRUM utiliza el **AToM** para suministrar circuitos ATM a través de la red. Esto incluye tanto PVCs como PVPs. AtoM también permite recoger estadísticas de los circuitos para cada segmento de la red.

PNNI 1.0 es utilizada por SPECTRUM para revelar la topología de la red, usando información almacenada en cada dispositivo a través de PNNI MIB. Este estándar también permite actualizar la topología, después de haber hechos cambios en la red.

PNNI SPVC permite crear PVCs a través de la red, los cuales automáticamente re-rutearán en caso de una falla en el estándar.

Por otra parte, el SPECTRUM soporta **RFC 1483** para la configuración de dispositivos extremos. Sin este soporte, sólo podría ser capaz de suministrar los circuitos a través de los switches, y los dispositivos externos necesitarían ser configurados manualmente para usar el PVC específico o circuito provisto en el switch.

Administrador de Servicios TRANSCEND

Por su parte el TRANSCEND es un software de administración, monitoreo y control de redes que trabaja sobre plataformas UNIX y que utiliza el protocolo SNMP. Este sistema integra monitoreo y control (fin a fin) exclusivamente en productos 3Com, tales como: adaptadores, concentradores, puentes ruteadores y switches. Esto se hace a través de una aplicación de administración gráfica que ayuda a consolidar las tareas sobre alguna de las siguientes plataformas:

- SunNet Manager
- HP OpenView
- IBM NetView para AIX

El TRANSCEND provee los siguientes beneficios:

Análisis y monitoreo de la red. Usa un monitor remoto de herramientas administrativas (RMON), combinado con el software SmartAgent para proporcionar beneficios tales como la auto calibración de las alarmas para la solución de problemas, esto incrementa las acciones correctivas sobre fallas en los equipos.

Administración sobre redes LAN virtuales. Permite llevar a cabo tareas administrativas sobre VLAN´s, usando LAN emulation y otras capacidades para redes ATM.

Integración sobre plataformas abiertas. Proporciona integración con las industrias que manejan plataformas estándares UNIX de administración de redes.

Fácil configuración. Permite llevar a cabo operaciones de configuración simultánea sobre múltiples dispositivos o puertos de un dispositivo. También permite realizar mediante el uso de sus herramientas de administración, el manejo de múltiples ruteadores.

Vista detallada de los dispositivos. Proporciona mediante operaciones sencillas de selección y ejecución, la interacción del usuario con la configuración detallada de un dispositivo o bien con la información estadística del mismo.

Documentación en línea. Proporciona un conjunto de ayudas relacionadas al hardware y al software que soporta, accesibles en cualquier momento que el usuario las requiera.

El sistema de administración manejado por el TRANSCEND se basa en una arquitectura de 3 capas:

1. Smart Agents de 3Com. Cada dispositivo usa un agente que recibe y responde a las instrucciones administrativas enviadas por la red. El tipo de agente depende del agente del dispositivo designado para administrarlo. Asi por ejemplo, las tarjetas adaptadoras tienen agentes proxy los cuales residen en la PC que usa la tarjeta; los concentradores tienen agentes que residen sobre el módulo de administración del concentrador y los ruteadores y switches tienes sus agentes integrados dentro de sus dispositivos de software. Para tareas simples de administración muchos

agentes soportan accesos directos usando una terminal conectada a través del puerto serial del dispositivo. Estas conexiones se pueden usar para cambiar parámetros de la configuración cuando la administración remota falle.

2. Plataforma de administración de redes. Las aplicaciones que maneja el TRANSCEND están diseñadas para correr en la parte más alta de las plataformas administrativas. Una plataforma de este tipo permite construir un mapa de red y ejecutar tareas de administración sobre los dispositivos contenidos en la misma, con lo que las tareas administrativas remotas se facilitan en gran medida.

3. Aplicaciones del TRANSCEND. Las aplicaciones del TRANSCEND realizan funciones específicas para varios dispositivos 3Com. Ejemplos de esas funciones son:

   - Administración de dispositivos. Permite configurar y administrar los dispositivos 3Com de la red. Cuando un dispositivo es seleccionado en el mapa de administración, la plataforma sobre la que corre, automáticamente habilita la aplicación de administración apropiada para el dispositivo.
   - Monitoreo y análisis. Permite monitorear los dispositivos, ver el estado de los mismos y recolectar estadísticas acerca de los datos que ellos generan.
   - Administración de alarmas. Permite llevar a cabo el control sobre las alertas recibidas de los dispositivos involucrados en la red.

Las aplicaciones a través de las cuales el TRANSCEND realiza el monitoreo y control de la red son:

- *Administración de acceso ATM.*
- *Inspección de dispositivos.*
- *Administración de puentes.*
- *Asistente LinkConverter.*
- *Administrador Oncore*
- *Administrador LANsentry.*
- *Inspección de estados.*
- *Administrador de alarmas.*
- *Administrador de inventario.*
- *Administración de ATM y VLAN's*

A continuación se hace una breve descripción de cada aplicación.

Administración de acceso ATM

Esta aplicación permite desplegar el estado de operación de un dispositivo ATM, configurarlo y obtener estadísticas del mismo. Esta aplicación cuenta con las siguientes características:

Visión de los dispositivos. Muestra una representación gráfica del dispositivo cuando éste es seleccionado.

Desplegado del estado mediante código de colores. Un código de colores indica el estado actual de los puertos y otros objetos desplegados en el dispositivo visto.

Objetos simplificados de administración. Permite seleccionar opciones administrativas de un menú y aplicarlas a los objetos seleccionados en la pantalla.

Inspección de dispositivos

Permite observar el estado de operación de un dispositivo seleccionado, configurarlo y obtener estadísticas acerca de él, esta aplicación es general para todos los dispositivos en la red (no sólo ATM) y presenta las mismas características que la aplicación anterior.

Administración de puentes

Permite controlar y operar los puentes usados en la red mediante una visión lógica y simple del dispositivo. Este punto proporciona los siguientes beneficios:

Simplificación de la configuración y el monitoreo. Haciendo click, sobre el icono de un puente o sobre algún puerto del mismo es posible configurar, monitorear, obtener el estado de las rutas y obtener datos del dispositivo.

Fácil Acceso. La aplicación se puede accesar desde cualquier pantalla de inspección de dispositivos, desde cualquier menú de administración de la red y desde la línea de comandos.

Asistente LinkConverter

Este asistente es una interfaz gráfica y manejador de opciones a través de menús que permite monitorear las unidades conectadas en línea al dispositivo, cuenta para ello con las siguientes características:

Configuración simplificada. Un menú de opciones de dispositivo es presentado, permitiendo así la fácil configuración de los dispositivos que están en línea al equipo principal de la red.

Desplegado del estado mediante código de colores. Usando un código de colores indica el estado de los puertos monitoreados.

Gráficas de estadísticas. Despliega e imprime estadísticas mediante gráficas de barras o circulares (pie).

Recabado de datos dinámico. Refresca el estado de los datos de los dispositivos en un intervalo de tiempo especificado por el usuario.

Unidad de control remoto. Permite habilitar y deshabilitar la configuración de los puertos, así como reiniciar el equipo remotamente.

Sesiones concurrentes. Permite establecer múltiples sesiones de acceso.

Acceso a la tabla de nombres comunes. Permite a usuarios, con privilegios adecuados, cambiar las 32 entradas de los posibles nombres de los dispositivos a monitorear.

Depósito de recuperación de archivos. Permite recobrar el contenido de los dispositivos de memoria utilizados para el análisis de un elemento determinado.

Administrador Oncore

Es una herramienta gráfica para el control de los concentradores multi-función, mediante ella se puede cambiar la asignación de puertos de red para balancear las cargas en la misma o para aislar un puerto o un módulo mientras se resuelve un problema determinado. Esta aplicación proporciona las siguientes características:

Distribución de software. Permite actualizar el software con el que opera el dispositivo, utilizando el protocolo trivial de transferencia de archivos (TFTP).

Desplegado dinámico y registro. Sirve para desplegar el estado del concentrador, así como el de cualquier módulo y ver la configuración del estado de los puertos; despliega y registra las estadísticas de tráfico; despliega y registra las condiciones de las alarmas y los mensajes enviados por ellas.

Reinicialización remota. Reinicializa el concentrador y todos sus módulos remotamente.

Configuración. Permite la reasignación de módulos, puertos u otros elementos de red; configura aspectos de seguridad para cada puerto previniendo así accesos no autorizados; a través de él se configura la operación tolerante a fallas de cada puerto y también permite llevar a cabo la configuración de parámetros específicos entre módulos y puertos.

Administrador LANsentry

Esta aplicación proporciona soporte completo para todos los dispositivos RMON. Consta de un grupo integrado de aplicaciones que se usan para desplegar y explorar ya sea en tiempo real o en una base de datos, los mensajes enviados por los dispositivos que cuentan con módulos de monitoreo remoto (RMON) en la red. También se puede usar para configurar dispositivos que manejen MIBS compatibles. Esta aplicación se puede usar para:

- Monitorear constantemente el desempeño de los segmentos de red.
- Detectar problemas de red comunes, como son: envío de paquetes irregulares, errores y colisiones.
- Configurar alarmas para el monitoreo de eventos específicos sobre un segmento.
- Capturar y desplegar paquetes, usando filtros y funciones de decodificación.

Así mismo el LANsentry presenta las siguientes características:

Comparación entre estadísticas de diversos segmentos. Permite probar y ver simultáneamente diversas interfaces en una misma gráfica, esta característica es muy útil cuando se comparan estadísticas generadas por dos o más interfaces estudiadas sobre un mismo tipo de prueba.

Interfaces ATM para emulación de LAN. Este tipo de interfaces permite monitorear redes virtuales.

Facilidad para detener momentáneamente las ventanas principales. Permite detener temporalmente las ventanas principales y prevenir un desplegado de datos excesivo. Si hay más de una ventana principal abierta, solo la ventana activa puede ser utilizada.

Inspección de estados

Esta aplicación administra dispositivos 3Com así como grupos de los mismos con el guardia de estados (Satus Watch) y el guardia MAC. El guardia de estados presenta las siguientes características:

- Monitorea el desempeño operacional de los componentes de la red.
- Detecta problemas operacionales en los dispositivos de red.
- Grafica o despliega los datos del estado de operación del dispositivo.
- Configura alarmas para que alerten de inmediato en caso de detectar problemas críticos en la red.

El guardia MAC presenta los siguientes beneficios:

- Visualiza todas las direcciones MAC asociadas con cada uno de los dispositivos de la red.
- Monitorea la actividad de las direcciones MAC para un grupo de dispositivos.
- Ejecuta la conversión de direcciones MAC a IP.
- Administra direcciones IP duplicadas.
- Localiza el sitio de la red donde se encuentran las estaciones finales (PCs o estaciones de trabajo) a través de su dirección IP o MAC.
- Deshabilita interfaces seleccionadas.
- Visualiza la conversión de direcciones IP a nombres de host.

Administrador de alarmas

Esta aplicación permite crear y configurar alarmas para los dispositivos 3Com que soportan el SmartAgent y las MIBS RMON. Gracias a ésta el administrador de la red puede darse cuenta de inmediato cuando una falla ha sucedido en algún dispositivo de la red.

Administrador de inventario

Permite definir grupos de dispositivos virtuales. Esta aplicación es el punto principal para muchas de las aplicaciones de red que maneja el TRANSCEND, ya que desempeña las siguientes tareas:

- Creación de clientes definidos basados en la información contenida dentro de la plataforma de administración de red y los mapas de red.

- Edición de grupos para combinar dispositivos individuales aplicándoles filtros, versiones de software y funciones predefinidas para cada tipo de dispositivo.

- Combinación de aplicaciones sobre uno o varios dispositivos.

Administración de ATM y VLANs

Esta aplicación permite configurar y administrar redes virtuales mediante el uso de estructuras ELAN o VLAN, también permite visualizar estadísticas sobre estas redes y visualizar todos los estados de los puertos de los dispositivos ATM. Esta aplicación cuenta con topología de mapas, herramientas de administración y un asistente administrativo.

- **SERVICIOS ADICIONALES**

Los servicios de red que pueden agregarse, gracias a la tecnología ATM, son básicamente 3:

- Videoconferencias.
- Redes Virtuales.
- Integración de datos, voz y video en un mismo canal.

A continuación describiremos en forma breve en que consiste cada uno de ellos.

Videoconferencias

La videoconferencia es un sistema de comunicación diseñado para llevar a cabo encuentros a distancia permitiéndonos la interacción visual, auditiva y verbal con personas de cualquier parte del mundo (siempre y cuando los sitios a distancia tengan equipos compatibles y un enlace de transmisión entre ellos). Con la videoconferencia podemos compartir información, intercambiar puntos de vista, mostrar y ver todo tipo de documentos, dibujos, gráficas, acetatos, fotografías, imágenes de computadora y videos, en el mismo momento, sin tener que trasladarse al lugar donde se encuentra la otra persona.

Conexiones entre equipos de videoconferencias

PUNTO A PUNTO. La conexión es directa y sólo se realiza entre dos equipos de videoconferencia.

MULTIPUNTO. Varios sitios participan en la reunión. Se requiere de un equipo especial adicional a los sistemas de videoconferencia llamado unidad multipunto, el cual permite la conexión de más de dos lugares durante la conferencia. Esta unidad multipunto es administrada por uno de los sitios, el que enlazará a los demás sitios.

Conforme cada grupo participante toma la palabra, su imagen y su audio se reproducen en uno de los monitores de los demás lugares.

Elementos que integran un sistema de videoconferencia

CODEC (COdificador/DECodificador o Compresor/DECompresor). Este dispositivo convierte las señales de video y audio en señales digitales, es considerado el corazón del sistema de videoconferencia.

DIPOSITIVO DE CONTROL. Puede ser una tableta de control, un teclado, un mouse, una pantalla sensible al tacto o un control remoto. Éste controla el CODEC y el equipo periférico del sistema.

CÁMARA ROBÓTICA. Es la cámara incluida en cualquier equipo, ésta es manejada a través de la tableta de control.

MICROFONOS. Capta el audio que se envía al otro sitio.

UNO O MÁS MONITORES. En ellos se puede observar a los participantes del sitio local y de los sitios a distancia, así como gráficas, fotografías, diapositivas, videos, etc.

SOFTWARE DEL SISTEMA DE VIDEOCONFERENCIA. Es el programa que permite la acción conjunta de los elementos que integran al sistema de videoconferencia.

DISPOSITIVO DE COMUNICACIÓN. Es el dispositivo (DCU/CSO) al que llega la señal digital desde el CODEC y la envía por el canal de transmisión (microondas, fibra óptica, etc.) lo que permite enviar y recibir la señal a los sitios remotos.

CANAL DE TRANSMISIÓN. Éste puede ser cable coaxial, microondas, fibra óptica, satélite, etc.; y sirve para transmitir la señal de audio y video a otro sitio.

ESPACIO. Es el área especialmente acondicionada tanto en acústica e iluminación para alojar el equipo y realizar las sesiones. El nivel de confort de la sala mejora la calidad del encuentro.

PERSONAL CALIFICADO. Es indispensable que cada sitio, cuente al menos con una persona que posea los conocimientos necesarios de telecomunicaciones y operación técnica del equipo.

Funcionamiento del sistema de videoconferencia

Las señales proporcionadas por las cámaras, micrófonos y equipos periféricos son enviadas al CODEC, dentro de éste se realiza un proceso complejo resumido como sigue:

1) El CODEC convierte las señales de audio y video a un código de computadora. A esto se le conoce como digitalizar. De esta forma se transmiten datos requiriendo menos espacio en el canal de comunicación.

2) Los datos se envían a otro dispositivo de comunicación, el cual los transmite al sitio remoto por un canal de transmisión por el que viajarán.

3) A través del canal, el otro sitio recibe los datos por medio del dispositivo de comunicación, el cual lo entrega al CODEC que se encarga de descifrar y decodificar las señales de audio y video, enviándolas a los monitores para que sean vistas y escuchadas por los participantes.

Redes Virtuales (VLANs)

Una red virtual de área local es un grupo de dispositivos que funcionan como un segmento de una red de área local (dominio de broadcast). Los dispositivos que forman una VLAN particular pueden estar separados por geografía y ubicación en la red. La creación de VLANs permite a los usuarios ubicados en áreas separadas o conectados a puertos separados, pertenecer aun mismo grupo VLAN. Los usuarios que son asignados en un grupo determinado podrán enviar mensajes de broadcast y multicast como si todos estuvieran conectados aun mismo segmento de red.

Cuando las estaciones de trabajo son asignadas a una VLAN, el desempeño de la conexión de la red no cambia. Las estaciones conectadas a puertos switcheados no sacrifican el desempeño de un enlace dedicado para participar en la VLAN. Como una VLAN no es un lugar físico, pero un miembro si, los switches de la red determinan a todos los miembros de una VLAN particular asociando dicha red a un número de puertos particular. La creación de VLANS, facilita las labores administrativas sobre clientes de diferentes coordinaciones. Para obtener mayor detalle acerca de las redes virtuales referirse al capítulo 2 del presente trabajo, en el apartado de ATM.

Integración de datos, voz y video.

Ya que ATM maneja celdas de longitud fija, nos permite llevar a cabo la descomposición y reordenación de señales de audio, voz y video de tal manera que sobre un mismo enlace se pueden enviar mezclados estos 3 tipos de señales, de ésta manera se pueden integrar servicios sobre un mismo equipo y no es necesario tener un equipo para recibir cada señal, además de esto se eliminan los problemas por el ancho de banda que requiere cada uno de ellos y la latencia de cada mensaje, ya que como sabemos el video ocupa mayor ancho de banda que la transmisión de voz y de datos, por su parte la voz se compone de pulsos constantes por lo que el retardo en la señal no debe existir, ya que el mensaje enviado perdería sentido. Con un switch ATM es posible elegir canales para cada tipo de señal, estableciendo en cada uno de ellos parámetros tales como el ancho de banda máximo que se les ha de proporcionar, esto se maneja en base a la clase del servicio que se proporciona a un enlace determinado. Con la integración antes mencionada es posible usar al máximo el ancho de banda disponible en la red así como los diferentes tipos de tráfico que por ella circulen.

Cabe mencionarse que además de estos servicios adicionales, la red ATM del Instituto conservará los servicios de red mencionados en el capítulo 3 del presente trabajo.

5.1.2 Rendimiento de la red ATM.

- **ELABORACIÓN DE PRUEBAS DE DESEMPEÑO**

Para llevar a cabo el análisis de rendimiento de la red ATM, se prepararon las mismas pruebas que se aplicaron a la red Ethernet. Las pruebas basadas en la transferencia de paquetes a través de la red se aplicaron nuevamente durante dos semanas, 3 veces al día, las pruebas realizadas consistieron en lo siguiente:

- **Prueba de Transferencia de Archivos (FTP)**

Para llevar a cabo esta prueba se seleccionaron algunas estaciones de trabajo (1 por edificio) con características similares, tales como capacidad en memoria, velocidad en la tarjeta de red, carga de trabajo, etc. Para establecer las conexiones diariamente y a tres horas del día diferentes, las conexiones se establecieron a las 10:00 de la mañana, a las 3:00 de la tarde y a las 8:00 de la noche, con el fin de tener diversas mediciones del tráfico de red ante diferentes circunstancias de carga de trabajo en la misma.

Las pruebas consistieron en llevar a cabo un ftp con un archivo de tamaño fijo (1 MB), de una estación ubicada en el edificio 12 (atlas) a otras estaciones ubicadas en los otros edificios que se conectaron al backbone ATM. Así mismo se llevo a cabo la prueba con una estación ubicada en la DGSCA. La prueba consistió en una transferencia manual o programada del archivo antes mencionado, llevando a cabo el registro tanto del tiempo de transferencia como de la velocidad a la que se había llevado a cabo. Las estaciones elegidas fueron las siguientes:

- Atlas ubicada edificio 12, estación de la cual se mandaba el archivo.
- Tonalli ubicada en el edificio 1, estación que recibía el archivo, estación con características muy similares a Gea, utilizada en las pruebas anteriores.
- Gauss ubicada en el edificio 2, estación que recibía el archivo.
- Blues ubicada en el edificio 4, estación que recibía el archivo.
- Hidros ubicada en el edificio 5, estación que recibía el archivo.
- Donky ubicada en el edificio 6, estación que recibía el archivo.
- Titán ubicada en el edificio 12, estación que recibía el archivo.
- Servidor ubicada en DGSCA, estación que recibía el archivo.

Esta prueba se diseñó con el fin de obtener datos sobre el incremento de la eficiencia en la transferencia de información en la red ATM, así como para saber en donde se originan, en caso de existir, los cuellos de botella y determinar si la distribución de la carga por segmentos de red implementada había sido la más adecuada. Los resultados de esta prueba se muestran y analizan en el siguiente subtema.

- **Prueba de establecimiento de la conexión (PING)**

En este caso, nuevamente se utilizaron las mismas estaciones que en la prueba anterior, pero además se incluyeron 2 PCs ubicadas en los edificios 3 y 8. Cabe

mencionarse que en el ftp, no fue posible incluir máquinas de estos edificios ya que en ellos no hay estaciones de trabajo que cumplieran las características necesarias para llevar a cabo las pruebas de manera uniforme. Como recordaremos, esta prueba consistió en llevar a cabo desde Atlas un ping a cada una de las estaciones y PCs mencionadas, esperar 10 transmisiones y obtener el tiempo promedio de la transferencia. El paquete que se envió fue de 64 bytes en todos los casos. Esta prueba se llevó a cabo todos los días de las 2 semanas, inmediatamente después de los ftp's. La prueba se diseño con la finalidad de detectar mejoras en los tiempos de transferencia con la implementación de ATM.

- **Prueba del nivel de tráfico por segmentos en la red**

Esta prueba consistió en llevar a cabo un monitoreo durante dos semanas de la situación de los switches principales de nuestra red ATM, para determinar en que segmento de la misma se estaba llevando a cabo una saturación del ancho de banda (en caso de haberlo) y poder establecer soluciones a futuro. Para llevar a cabo esta prueba fue necesario aplicar un reset a los contadores de nuestros equipos principales y registrar los datos de paquetes enviados para cada puerto. Con esta prueba se sabrá que segmento de la red está siendo más utilizado y por consiguiente cuál de los segmentos requiere de una nueva distribución de cargas, o bien saber si la distribución hecha al implementar el cambio a ATM fue eficiente.

- **Prueba de nivel de colisiones**

Como sabemos, esta prueba consistió en llevar a cabo un registro durante 15 días de las colisiones producidas en nuestros concentradores principales ubicados en cada edificio. Con esta prueba conoceremos que tan frecuentes son ahora las colisiones en nuestra red; las colisiones son un parámetro de mal uso del medio de transmisión en la red y así mismo un indicador de que existen, en un segmento determinado, equipos con problemas que hay que corregir ya que están haciendo un mal uso del canal de comunicación.

Los resultados obtenidos en cada una de las pruebas antes mencionadas se analizarán a continuación.

- **ANÁLISIS DE RESULTADOS Y CONCLUSIONES**

En las pruebas del FTP obtuvimos los datos de las velocidades de transferencia así como los tiempos que duraban; basándose en esos datos se generaron dos gráficas para cada edificio: una de los promedios de la velocidad de transferencia (figura 5.3) y otra del tiempo (figura 5.2) en que se había llevado a cabo la misma. Cabe señalarse que las gráficas de este apartado incluyen también los resultados de las pruebas hechas a la red Ethernet, esto se hizo con el fin de poder comparar rápidamente el rendimiento de la red en ambas tecnologías.

Resultados de la prueba de FTP (tiempo)

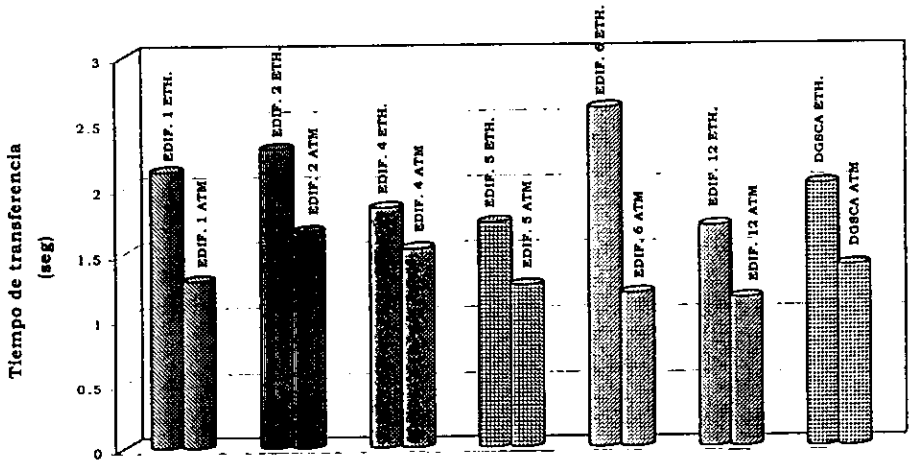


Figura 5.2

En la figura 5.2 podemos observar los resultados del tiempo promedio que se obtuvieron al transferir un archivo entre el edificio 12 y cada uno de los servidores. Como se podrá observar el menor tiempo lo hizo el servidor Titán (edificio 12). Por otra parte el mayor tiempo de respuesta fue registrado en el servidor Gauss, ubicado en el edificio 2, de acuerdo a este resultado podemos concluir que es el segmento de red más saturado. Sin embargo es importante notar que en general, los tiempos de transferencia, disminuyeron considerablemente, ya que en este caso apenas llegan a 1.66 segundos, mientras que en la red Ethernet rebasaban los 2.5 segundos, este cambio representa una importante disminución del tiempo; aproximadamente de 0.8 segundos, que equivalen al 32%. De esta manera se confirma el hecho de que el enlace hacia RedUNAM no es un problema para la transmisión de información desde el Instituto, ya que como vemos los tiempos registrados en este segmento de la red, son casi iguales a los registrados en los edificios 5, 6 y 12. De igual manera vemos que el ampliar el ancho de banda en la red sí mejoró el tiempo de transmisión de paquetes dentro de la misma.

La figura 5.3 nos muestra los resultados promedio de la velocidad de transferencia por cada servidor, en ella simplemente se corrobora la situación ya mencionada, de que el segmento del edificio 12 al 2 representa la mayor lentitud en la transferencia de paquetes. En este caso es importante mencionar que el aumento en la velocidad fue del 28.6 %. La gráfica obtenida se muestra enseguida.

Resultados de la prueba de FTP (velocidad)

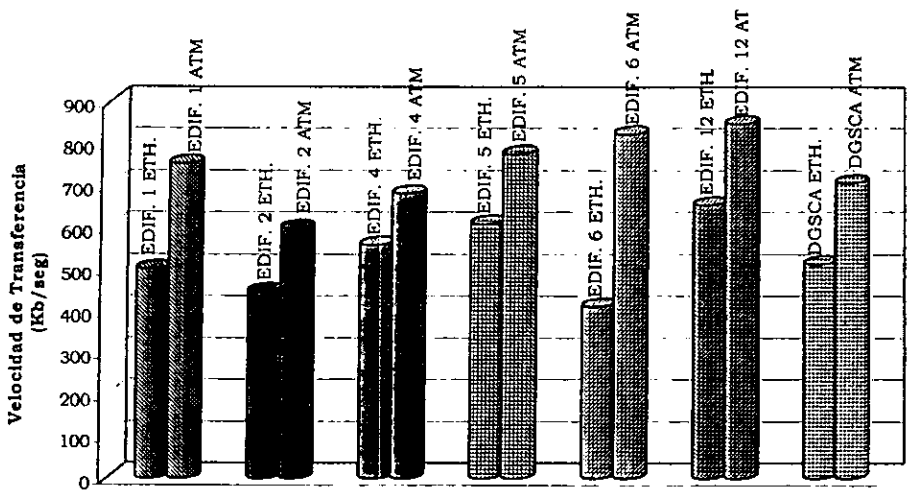


Figura 5.3

Una tabla resumen de los resultados de la prueba del FTP es la siguiente:

No. de segmento	Del edificio	Al edificio	Velocidad (Kbps)	Tiempo (segundos)
1	12	1	753	1.29
2	12	2	598	1.66
3	12	4	681	1.53
4	12	5	776	1.25
5	12	6	822	1.18
6	12	12	847	1.14
7	12	DGSCA	707	1.39

Así mismo a continuación presentamos la gráfica de los tiempos de respuesta promedio obtenidos en la prueba del ping (figura 5.4).

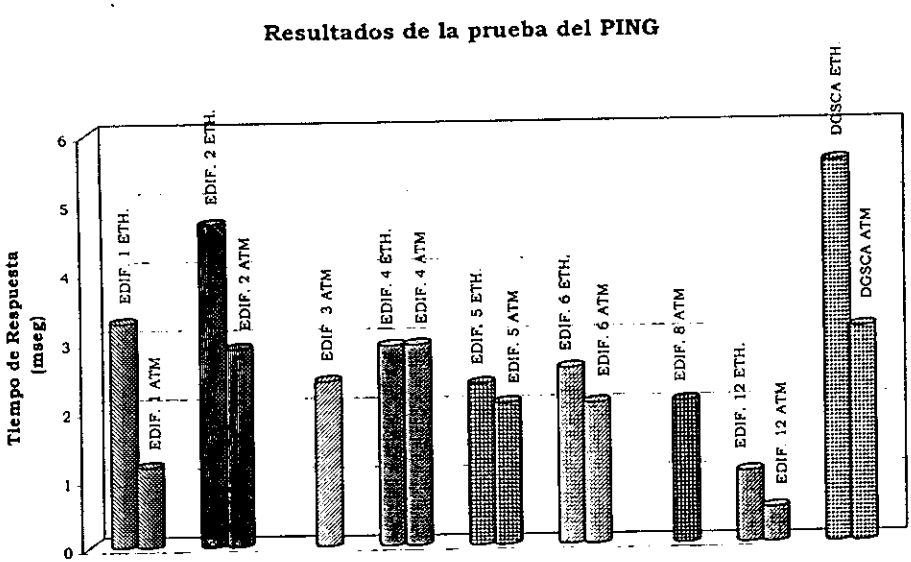


Figura 5.4

En este caso los tiempos de respuesta más altos fueron registrados por DGSCA y el edificio 4, por su parte el edificio 12 resultó ser el de menor tiempo de transferencia de paquetes. En esta prueba, también se registro una mejora notable en el tiempo de respuesta, ya que como recordamos, en las pruebas hechas sobre la red Ethernet obtuvimos tiempos de respuesta de hasta 5.84 milisegundos, mientras que en este caso el tiempo máximo fue de sólo 3.10 milisegundos, disminuyendo un 40.7 %. El tiempo mínimo alcanzó los 0.51 milisegundos, lo cuál también es una disminución notable en cuanto al tiempo de transferencia en los paquetes de prueba.

Para el caso de la prueba sobre el nivel de tráfico que se presenta en cada segmento de la red (figura 5.5), obtuvimos que después de la migración, el mayor nivel de tráfico se encuentra en el edificio 12, esto es aceptable ya que es ahí donde se concentran el mayor número de equipos que además son los utilizados con mayor frecuencia por toda la comunidad del Instituto. Como vemos comparativamente con la red Ethernet el número de paquetes, en este caso, se distribuyó lógicamente de acuerdo a la cantidad de equipo. En realidad esta prueba sólo nos indica que equipos tienen mayor flujo de paquetes, pero lo importante es la relación de estos con el número de colisiones, las cuales deben ser menores que el 10 % del total de paquetes enviados. Esta relación se corrobora con los resultados de las colisiones presentados más adelante.

En la figura 5.5 vemos las estadísticas de paquetes enviados desde cada edificio, los paquetes del edificio 8 se contabilizaron junto con los del edificio 1 ya que por el momento el switch del 1 da cabida a las conexiones del laboratorio de enrocamiento (edificio 8).

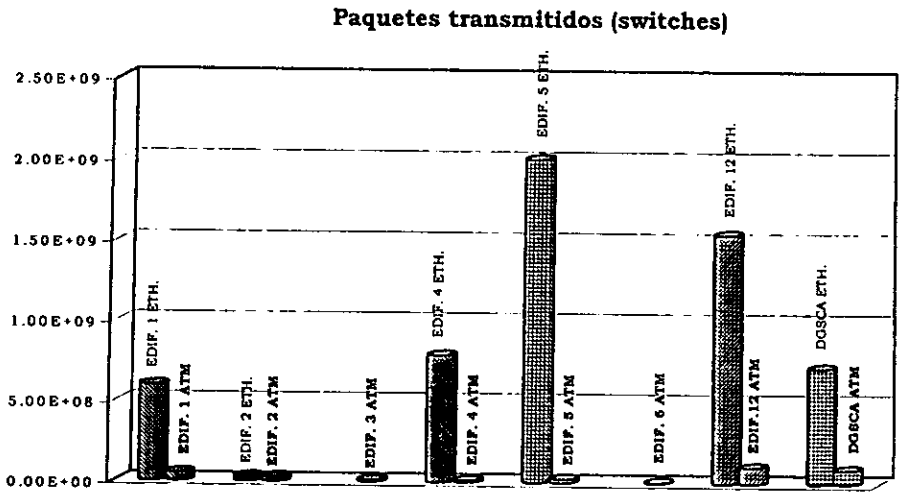


Figura 5.5

Los resultados de esta prueba del nivel de colisiones por edificio, nos muestra que se redujeron en gran cantidad en relación a lo obtenido anteriormente, como podemos observar el mayor número de ellas se presenta en el enlace hacia RedUNAM, sin embargo internamente las colisiones están muy por debajo del 10 % permitido, esto nos indica que la distribución de cargas hecha al llevar a cabo la migración a ATM fue correcta, y que los equipos que se revisaron mejoraron en cuanto a su manera de accesar al medio de comunicación. En la figura 5.6, tenemos los resultados correspondientes a esta prueba.

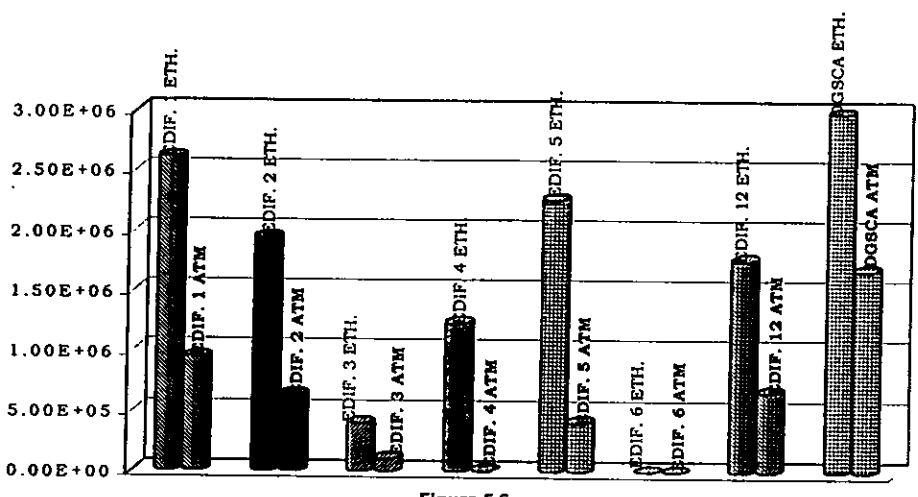


Figura 5.6

De todas las pruebas anteriormente mostradas, podemos concluir que:

- El backbone ATM con mayor ancho de banda realmente funcionó para incrementar la velocidad de transferencia en la red, así como el desempeño de las conexiones entre las computadoras hechas a través de la misma. En este aspecto aclaramos que si bien es cierto, el incremento presentado, que fue de aproximadamente 30 % en todas las pruebas realizadas, se obtuvo simplemente del backbone ATM. Este porcentaje de incremento en el desempeño, crecerá a medida que se vayan cambiando los dispositivos Ethernet que se heredaron de la red anterior por otros que funcionen bajo una tecnología más veloz. Como se comprenderá, el obtener mejoras de velocidad y desempeño de una red totalmente ATM, no fue posible en ésta etapa de migración de la red, debido a que dado que se adoptó una red con equipo que funciona a 10 Mbps, y dado que la limitante del proyecto de migración era no desechar ese equipo, se tuvieron que hacer acoplamientos de velocidad entre dispositivos ATM y Ethernet, lo cuál evidentemente baja el desempeño general de la red, sin embargo para solucionar este aspecto, proponemos que en una etapa posterior se decida llevar a cabo un estudio detallado que permita determinar qué equipo de red debe ser intercambiado por uno que funcione con una tecnología de red más actual y veloz (Fast Ethernet, o ATM). Así mismo y a nivel de los usuarios, también se debe llevar a cabo un sondeo para detectar qué equipos deben actualizarse en cuanto a su interfaz de red; con estos cambios graduales de los dispositivos Ethernet, se podrá mejorar mucho el desempeño de la red. Un primer acercamiento hacia esta mejora, puede ser el implementar en los servidores principales de cada coordinación o área un cambio parcial o total en cuanto a su hardware para integrarlos a una tecnología de red que funcione mínimo a 100 Mbps.

- La distribución de cargas efectuada con la migración está distribuyendo el tráfico de red en forma uniforme por lo que los puertos troncales de la red están menos congestionados ya que cada uno de ellos trabaja de acuerdo a la cantidad de usuarios que dependen del mismo, esto fue consecuencia directa de la conexión de los equipos en paralelo y no en cascada, que era como habían estado funcionando anteriormente. En este aspecto, también es conveniente mencionar que a medida que los dispositivos de red, así como las interfaces de las computadoras personales y estaciones de trabajo sean actualizados, y funcionen sobre tecnologías ATM o Fast Ethernet, los enlaces troncales se verán beneficiados, debido a que evitarán llevar a cabo conversiones de paquetes entre tecnologías, lo que disminuirá el tiempo de transferencia de los paquetes que circulen a través de la red.

- Las colisiones en la red disminuyeron considerablemente, por lo que se evitan problemas de acceso al medio, lo que repercute directamente en la velocidad de transferencia de la red. Cabe señalarse que las colisiones serán menores si se realizan los cambios establecidos en los puntos anteriores, y mejor aún de llegarse a establecer una red ATM pura, las colisiones desaparecerán por completo.

CONCLUSIONES

En este trabajo se engloban los cambios significativos que ha experimentado la red del Instituto de Ingeniería dados los requerimientos de la comunidad que lo conforma, de esta manera las conclusiones que hemos obtenido a lo largo de la planeación, diseño e implementación de la red ATM con que actualmente cuenta el Instituto, son las siguientes:

- La red ATM proporciona una arquitectura de red de alta velocidad, que es flexible y escalable a futuro, sin la necesidad de incluir grandes gastos en la compra e instalación de nuevo equipo, ya que con este trabajo se estableció una arquitectura ATM OC-3 de 155 Mbps para el backbone que conforma nuestra red. Con este aspecto se proporciona una ruta de migración gradual y transparente para nuevas tecnologías de red que pudieran surgir en el futuro dadas las necesidades en los servicios de red que requiera el Instituto en los próximos años.

- La red ATM implementada asegura la reducción de riesgos a fallas en la misma y por lo tanto una mínima interrupción del servicio prestado a los usuarios, así mismo proporciona el soporte para todo tipo de aplicaciones que requieran de un uso intensivo de ancho de banda, que sean sensibles al tiempo de transferencia y que requieran calidad de servicio. Con estas características se podrán proporcionar servicios tales como: videoconferencias, educación a distancia, aplicaciones de escritorio compartidas, correo de voz, reproducción de video, soporte para aplicaciones de procesamiento de imágenes y visualización, Internet 2, voz sobre IP, etc.

- La red ATM permite implementar servicios adicionales, tales como videoconferencias, redes virtuales, educación a distancia, o cualquier aplicación que requiera de gran ancho de banda o bien de cierta calidad de servicio. Estos servicios actualmente no se han implementado porque para hacerlo se requiere de equipo adicional que es costoso y que se adquirirá posteriormente, sin embargo, con la estructura de red establecida es posible ir agregándolos conforme se vayan requiriendo para lograr satisfacer las necesidades de la comunidad del Instituto de Ingeniería.

- La red ATM permite implementar un esquema de red con mayor seguridad ya que gracias a la implementación de redes virtuales se provee la posibilidad de evitar la visibilidad del tráfico de red, previniendo así que accesos no permitidos sean llevados a cabo, así mismo, el esquema de VLAN's evita que personal no autorizado haga uso de direcciones IP que sólo corresponden a nuestra Institución.

- La migración de una red hacia otra tecnología (en este caso ATM), es un proceso delicado el cuál implica una planeación minuciosa de cada etapa antes de desarrollar el proyecto, las etapas de la migración deben contemplar los siguientes objetivos:

1. Se debe otorgar transparencia a los usuarios, durante el proceso de la migración con el mínimo de interrupciones en el servicio de red.

2. Se debe proporcionar una base sólida para futuros cambios en la infraestructura de red, asegurando la funcionalidad de los nuevos componentes integrados a ella.

3. Se debe prevenir la compra de equipo innecesario.

4. Se deben establecer los métodos y requerimientos para la administración, el monitoreo y el control de la nueva infraestructura de red.

Por otra parte también concluimos que el llevar a cabo una migración total del equipo de red del Instituto de Ingeniería hacia tecnología ATM, era imposible debido a que para lograr esto se necesitaría de una gran cantidad de recursos económicos para adquirir todos los equipos necesarios. Así mismo sería necesario sugerir a cada usuario de red que cambiaran sus equipos de trabajo por otros con características que soportaran una estructura donde todos los equipos funcionarán bajo esta tecnología (ATM), al ver estos contratiempos, se estableció la migración del backbone, que proporciona las bases para llevar a cabo la migración de la red en cada edificio en la medida en que haya posibilidades de hacerlo, sin que estos cambios graduales afecten los servicios de red que se brindan a los usuarios que no cuenten con ATM. Para llevar a cabo una migración en cada edificio, primero es necesario organizar el cableado interno, de acuerdo a lo propuesto en el punto 3.1.8 del capítulo 3 del presente trabajo, con esto se provee una estructura de cableado estructurado que cumpla con las especificaciones establecidas en la norma correspondiente. De igual forma el cableado estructurado presenta grandes beneficios para llevar a cabo la administración y operación de la red, ya que mejora el rendimiento de la misma y facilita la solución de cualquier problema físico que en ella se pudiera presentar, reduciéndose así los costos de operación.

Por otra parte, sugerimos que para evitar pérdidas en el tiempo activo de funcionamiento de la red ante cualquier contingencia de ruptura en el canal de comunicación se establezcan rutas redundantes del anillo principal de fibra, de acuerdo a lo propuesto en el mismo apartado (3.1.8 del capítulo 3).

Los aspectos de cableado estructurado y redundancia, implican costos importantes para el Instituto de Ingeniería, sin embargo estamos seguros de que si se hace una inversión en estos aspectos, el rendimiento de la red, así como el aprovechamiento que tenga de ello la comunidad del Instituto, redituará completamente el esfuerzo.

Además de las conclusiones antes mencionadas, también es conveniente hacer notar que los tiempos establecidos para llevar a cabo el proyecto de migración en nuestro calendario de actividades se vieron afectados desfavorablemente, debido a que los procesos de compra de equipo y material realizados en nuestra dependencia son bastante lentos, aunado a esto, tuvimos que la asistencia por parte de nuestros proveedores también fue deficiente, éstas situaciones nos llevaron a un atraso en nuestro tiempo de entrega del proyecto de aproximadamente, dos meses, por lo que sería recomendable agilizar estos procesos y por otro lado buscar proveedores de servicio más comprometidos para futuros proyectos.

En cuanto a experiencias y conclusiones personales, mencionamos que es muy importante para nosotros el haber obtenido experiencia tanto en el manejo de equipo de red con tecnologías de punta, así como en la planeación, desarrollo y pruebas de desempeño de proyectos prácticos e importantes, así mismo es gratificante saber que el presente trabajo no sólo abarcó una parte teórica y un modelo de escritorio, sino que se llevó a la práctica, y lo que es mejor, actualmente la red ATM está en funcionando adecuadamente y dando servicio a la gran comunidad de investigadores y becarios del Instituto de Ingeniería. Por otra parte también adquirimos experiencia en el manejo de personal a pequeña escala, así como en el trato con múltiples proveedores de equipo de red, cableado y otros servicios.

En lo referente al Instituto de Ingeniería, podemos concluir que con la instalación de ATM, se convierte en la primera dependencia de la UNAM que cuenta con esta tecnología, igualando en velocidad a RedUNAM con 155 Mbps. Así mismo, podemos decir que el Instituto está a la vanguardia, ya que se pone al nivel de compañías comerciales que proporcionan servicios de red de datos de alta velocidad como Avantel, Intervan y otras.

Para finalizar diremos, que estamos convencidos de que el presente trabajo proporciona la documentación completa de la evolución y el estado actual de la red del Instituto de Ingeniería, que servirá como antecedente y base para modificaciones venideras, así como para el soporte, el control y la administración que se realicen sobre la arquitectura de red actualmente en funcionamiento.

GLOSARIO

Backbone o columna vertebral. Conjunto de nodos y vínculos que se conectan entre sí para formar una red, o los protocolos de capa superior usados en una red. Algunas veces el término se emplea para hacer referencia a los medios físicos de una red.

Baudio. Es el número de veces que una señal cambia de estado en un segundo.

Brouter. Dispositivo de red que combina las características del puente y el ruteador. Es puente cuando filtra protocolos y paquetes destinados a nodos de redes diferentes.

Cable rudo de fibra óptica. Cable que contiene los hilos de fibra óptica y que está recubierto por varias capas de protección. Se usa para el cableado entre edificios a través de ductos por el subsuelo.

Cables jumper o patch cords. Son cables pequeños de fibra óptica que se usan para llevar a cabo las conexiones de los distribuidores de fibra a los equipos de red terminales (como switches y concentadores).

Codec (Codificador/DECodificador o COmpresor/DECompresor). Este dispositivo convierte las señales de video y audio en señales digitales (ver capítulo 5 en la sección de servicios adicionales de ATM, punto 5.1.1).

Concentrador o **Centrador** (Hub). Dispositivo que sirve como punto central de conexión para los cables de los nodos que están puestos físicamente en topología estrella. Por lo general se encuentra en una red Ethernet 10BASE-T.

Contención. Estado que ocurre en algunas LANs donde la subcapa de control de Acceso a Medios (MAC), habilita a más de un nodo para transmisión simultánea arriesgándose a colisiones.

Datagrama. Unidad básica de datos usada en TCP/IP. Algunas veces llamado *Datagrama IP*, ya que en su encabezado contiene las direcciones IP de la fuente y el destino.

DQDB (Distributed Queue Dual Bus). Al igual que FDDI, es un protocolo para tráfico de circuitos conmutados especificado en la norma 802.6 del IEEE para redes de área metropolitana. (Ver capítulo 1, subtema 1.3.4.1 sobre los estándares del IEEE).

Emulación. Programa que simula otro dispositivo, enviando los mismos códigos que enviaría el dispositivo real.

Enrutador o **ruteador**. Dispositivo que conecta LANs en una interred y enruta tráfico entre éstas. Por lo general las redes que conecta usan la misma capa de protocolo de red (Capa 3) como TCP/IP o IPX. Tiene la capacidad de conectar redes que usan diferentes topologías lógicas, como Ethernet y Token Ring. También la palabra *encaminador* se refiere a éste.

FDDI-II. Nueva versión de FDDI que al igual que éste, corren a 100 Mbits/seg en fibra, pero además tiene un nuevo modo de operación llamado Modo Hibrido (Ver capítulo 2, subtema 2.2.11 sobre FDDI y FDDI-II).

Fragmentación. División de un programa en porciones más pequeñas, lo que se hace generalmente porque el datagrama original es demasiado grande para la red o el software.

Gigabyte. Mil millones de bytes, que corresponde al número decimal 1,073,741,824.

IETF (Internet Engineering Task Force; Fuerza de trabajo de ingeniería de Internet). Organismo encargado de proponer y establecer los estándares en Internet.

Infrarrojo. Tecnología que usa ondas electromagnéticas para LANs inalámbricas.

Interred. Varias redes con puentes y ruteadores, que permiten que nodos de diferentes redes se comuniquen entre sí.

Jam. Término Ethernet para comunicarse a todos los dispositivos de una red en la que haya ocurrido una colisión.

Jitter (fluctuación). Término que se usa generalmente en redes de 10BASE-T (Ethernet par trenzado), donde las señales estén fuera de fase entre sí.

Latencia. Es el tiempo que toma un conmutador para procesar un paquete. Se mide de diferentes formas dependiendo del método utilizado por el conmutador.

LLC (Logical Link Control). Subcapa homogenenizadora para permitir la interconectividad entre diferentes tipos de redes.

MAC (Media Access Control). Subcapa más relacionada con el medio físico, y que maneja el método de acceso para la transmisión.

Mbps. Notación equivalente a millones de bits por segundo (esta nomenclatura se utiliza a lo largo de todo el trabajo).

Módem (MOdulador DEModulador). Dispositivo que convierte las señales analógicas en digitales y viceversa. Se usa para conversión de señales para transmisión en líneas telefónicas.

Multiplexar. Cuando una sola conexión en la siguiente capa inferior soporta varias conexiones (de esta forma, tres conexiones de servicio de la capa de presentación se pueden multiplexar en una sola conexión de la capa de sesión).

Nodo. Termino genérico que se usa para referirse a los dispositivos de la red.

NSF. Es la Fundación Nacional de Ciencias, la cual tomó un papel activo al expandir el Internet TCP/IP, iniciando en 1985, con un programa para establecer redes de acceso distribuidas alrededor de sus 6 centros con supercomputadoras.

PBX (Private Branch Exchange). Es un sistema compuesto por un switch, un grupo de líneas de voz, un grupo de líneas de datos y varias unidades de control y servicios para proporcionar la interconexión de varios usuarios en los sistemas de telefonía pública.

PNNI. Es la interfaz red-red para redes privadas o P-NNI, es una de las nuevas interfaces para aseguren la compatibilidad entre equipos de las redes ATM. La P-NNI es todavía inestable y en gran manera sigue asociada a cada fabricante, encargándose del arbitrio de las conexiones virtuales, el control de congestión y gestión de la topología. (Ver capítulo 2, sección 2.6.8 sobre aspectos de la migración hacia ATM).

Protocolo. Reglas que rigen el comportamiento o el método de operación de algo.

Puente (Bridge). Dispositivo de red capaz de conectar redes que emplean protocolos similares. Primero revisa la dirección del paquete, luego si ésta corresponde al otro segmento de red, lo pasa a través del puente.

Repetidor o hub repetidor (nombrado así en el capítulo 2). Dispositivo de red que eleva la potencia de las señales de llegada para permitir que se extienda la longitud de una red. Al amplificar y retransmitir la señal de la red, permite segmentos de cable de red más largos.

RFC "XXXX" (Requests For Comments; Peticiones de comentarios). Propuestas de estándares plasmadas en documentos numerados sobre la creación y establecimiento de estándares en Internet, siendo *'xxxx'* el número identificativo de cada RFC. Cuando se propone un nuevo estándar, la IETF publica un RFC, el cual a su vez le hereda el nombre al estándar finalmente adoptado. Por ejemplo, para correo se tiene el RFC 822.

Round Trip Delay. Para saber si un bit ha llegado bien y no se tiene que retransmitir se ha de esperar un tiempo 2T, llamado **Round Trip Delay**. Donde T es el retardo de tránsito (tiempo en que se envía un bit y lo recibe el destino).

Switch. o **conmutador**. Aprovecha la topología en estrella y los diseños de concentradores para reducir la contención del canal sobre los segmentos de la red. Estos como los puentes, fueron diseñados para dividir una red local extensa en pequeños segmentos, aislando el tráfico de cada uno (tráfico local), de esta manera se aprovecha mejor el ancho de banda mientras permanece una completa conectividad de los segmentos. Además usan un esquema de reenvio basado en hardware, opuesto al de software usado en puentes y enruteadores.

Transceiver. Dispositivos de acoplamiento entre medios de transmisión diferentes (se menciona a lo largo de todo el trabajo).

Transceptor. Dispositivo de red requerido en redes de banda base, que toma una señal digital y la coloca en un medio de banda base analógico. Los transceptores pueden detectar colisiones. Algunas veces llamado **transductor**.

Troughput (Transferencia Real). Cantidad de trabajo que puede ser procesada en un tiempo dado. Es también, la cantidad de datos que son transmitidos a algún punto de la red.

REFERENCIAS

BIBLIOGRAFICAS.

Parne, Tere
GUIA DE REDES DE ALTA VELOCIDAD
McGraw-Hill . Madrid, España 1997

Parker, Tim
APRENDIDENDO TCP/IP EN 14 DIAS
Prentice Hall, 1995

Stalte, Kevin
TODO ACERCA DE LAS REDES DE COMPUTADORAS
Prentice Hall Hispanoamericana S. A., 1995

WWW

http://a01-unix.uc3m.es/~gmm/DOC1.HTM
http://www.cicese.mx/~aarmenta/frames/redes/fddi/fddi-ii/intro1/dang.html#p2
http://eantc.prz.tu-berlin.de/INFOSYS/fddi/cieberblick/FddiHistory.html
http://www.ora.com/reference/dictionary/terms/F/FDDI_Follow-On_LAN.htm
http://www.ora.com/reference/dictionary/terms/F/Fiber_Distributed_Data_Interface.htm
http://www.gigabit-ethernet.org
http://grouper.ieee.org/groups/802/3/z/public/index.html
http://www.gigabit-ethernet.org/technology/whitepapers/gige_97/papers97_toc.html#toc
http://www.cisco.com/warp/public/729/gigabit/
http://www.3com.com/technology/key_net/gig_ether/index.html
http://www.foundrynet.com
http://www.packetengines.com
http://www.prominet.com
http://www.rapid-city.com
http://www.bicsi.org/Gigabit/
http://www.scl.ameslab.gov/workshops/Talks/Payne/
http://wwwhost.ots.vtexas.edu/ethernet/descript-100quickref.html
http://distancia.dgsca.unam.mx/servicios/ques.html#1
http://www.atmforum.com/
http://www.trillium.com/whats-new/wp_ipqos.html
http://www.trillium.com/whats-new/wp_atmlane.html
http://www2.vnu.co.uk/logical_networks/esindex.htm
http://www.cis.ohio-state.edu/~jain/cis788-97/atm_security/index.htm
http://www.itr.unisa.edu.au/~dstowww/atm_security/
http://www-comm.itsi.disa.mil/atmf/sec.html
http://eantc.prz.tu-berlin.de/Documents/Standards/ATM-Forum/sec-pub.html
http://www.telematik.informatik.uni-karlsruhe.de/~wiltfang/projects/ManATM/
http://internet.net.com/repository/white_papers/atm_intro/

http://www.stel.com/stel/atmps/wpaper/wpaper.htm
http://internet.net.com/techtop/atm_intro/
http://www.cabletron.com/support/manuals/spel.html
http://www.cabletron.com/products/items/SPEL-MGR-2.00/
http://www.cabletron.com/white-papers/spectrum/atmserv-man.html
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm

REVISTA

RED
Núm. 94. Julio 1998

TESIS

Camacho Palacios, Gustavo
Ramírez Acevedo, Artemia
Septien Nava, Ricardo
ANÁLISIS Y DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA PARA LA RED DE ALTA VELOCIDAD DEL INSTITUTO DE INGENIERÍA.
Ciudad Universitaria, 1997.