UNIVERSIDAD LA SALLE

ESCUELA DE INGENIERIA

INCORPORADA A LA U. N. A. M.

CONSIDERACIONES DE DISEÑO PARA REDES

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

AREA: INGENIERIA ELECTRONICA Y COMUNICACIONES

P R E S E N T A N :

GERARDO MONTER DE LA VEGA

GONZALO MONTER DE LA VEGA

ALFREDO TOMAS WYDLER OBERSTADT

SERGIO NAVARRO BARRIENTOS

MARIO FRANCO BAUTISTA

ASESOR DE TESIS: ING. EDUARDO RUIZ RIVERA

MEXICO, D. F. 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

LA SALLE

Gerardo Monter de la Vega
Gonzalo Monter de la Vega
Alfredo Tomás Wydler Oberstadt
Sergio Navarro Barrientos
Mario Franco Bautista

[illegible] solicitud relativa, me es grato transcribir a usted la autorización del tema que aprobado por este [illegible], para que sea presentado como tesis en el examen profesional de [illegible] Ingeniero Electricista, de [illegible] en Ingeniería Electrónica.

"CONSIDERACIONES DE DISEÑO PARA REDES"

[illegible]

INTRODUCCION
ANTECEDENTES
CAPITULO I.- GENERALIDADES DE REDES LAN Y WAN
CAPITULO II.- INTEGRACION LAN-WAN
CAPITULO III.- GENERALIDADES DEL PROCESO PARA DISEÑO DE REDES
CAPITULO IV.- OPCIONES DE ARQUITECTURA
CAPITULO V.- CASOS REALES
CAPITULO VI.- ADMINISTRACION DE REDES
CONCLUSIONES
GLOSARIO
BIBLIOGRAFIA

[illegible] cabal cumplimiento de que el [illegible] en la Ley de Profesiones, deberá prestar Servicio [illegible] requisito indispensable para sustentar examen profesional, así como de la obligación de la Dirección General de Servicios Escolares, en el sentido de que se imprima en lugar visible de los ejemplares de la tesis, el título del trabajo realizado.

A T E N T A M E N T E
"INDIVISA MANENT"
ESCUELA DE INGENIERIA
México, D.F., a 25 de Enero de 1995

ING. EDUARDO RUIZ RIVERA
ASESOR DE TESIS

ING. EDMUNDO BARRERA MONSIVAIS
D I R E C T O R

UNIVERSIDAD LA SALLE
BENJAMIN FRANKLIN 47, TEL. 516-99-60 MEXICO 06140 D.F.

Ante todo gracias a Dios.

A nuestros Padres, Esposas y Hermanos, a quienes finalmente les debemos lo que somos.

A nuestros Hijos, por quienes seguiremos siendo.

A Eduardo Ruiz, por su apoyo.

A la Universidad La Salle, por todo lo que nos ha dado.

A los que creyeron en nosotros y nos impulsaron para que llegáramos hasta el fin de esta tesis.

Alfredo, Gerardo, Gonzalo, Mario y Sergio.

ÍNDICE

CAPITULO VI

INTRODUCCIÓN

INTRODUCCIÓN

Hoy en día toda entidad privada y gubernamental requiere un manejo de información en forma expedita y confiable, es por ello que las Redes de Área Local y de Área Amplia ocupan un lugar importante en la mente de los empresarios y los dirigentes en todo el mundo.

Nuestro país no se podía sustraer a esas tendencias, como todos sabemos, en los últimos diez años las empresas del área de telecomunicaciones e informática han presentado crecimientos importantes y entre éstas destacan fuertemente las que se dedican a la comercialización de soluciones de comunicación de datos.

Las firmas más importantes de equipo de redes a nivel mundial han visto en México un mercado potencial interesante, por lo cual en nuestro país ya es posible obtener equipo de tecnología de punta directamente del fabricante o de un representante autorizado.

Por otro lado con la firma del T.L.C. con Estados Unidos y Canadá se creó la necesidad de eficientar los procesos a fin de poder competir con nuestros nuevos socios comerciales.

Las redes en México habían estado conceptualizadas como sistemas que podían controlar la contabilidad y la administración de los negocios, los bancos las utilizaban para acelerar sus operaciones y poder extender sus servicios a muchos lados con la seguridad de que las decisiones estarían basadas en datos confiables y así se reducía el riesgo de manejo del dinero.

En la actualidad esta perspectiva es totalmente diferente, las empresas se han dado cuenta de que las redes y los sistemas les permitirán además de eficientar los procesos, manejar gran cantidad de información y tener incluso comunicación de voz e imagen a través de sus mismas redes de datos.

Con la velocidad en que se han venido presentando los cambios de tecnología en esta área, es difícil encontrar literatura formal sobre los temas de redes. La mayor parte de la información esta emergiendo de los propios fabricantes de equipo, y cada uno de ellos presenta sus opciones en forma muy seria, pero con frecuencia manejan tendencias a respaldar las posibilidades de sus productos y por otro lado justificar sus desarrollos y avances tecnológicos.

Por lo anteriormente expresado pensamos firmemente que al contar con una forma de adquirir las bases de conocimiento en redes, se puede facilitar el desarrollo de sistemas más confiables y permitir a la gente que diseña redes tener un medio de brindarle a sus clientes una herramienta de conocimiento con la cual les será más sencillo comprender sus recursos y sus necesidades.

Nuestra intención para este trabajo no fue el crear un manual de diseño paso a paso, sino mas bien una propuesta de planeación clara y estructurada sobre las posibles necesidades y las recomendaciones inherentes que pueden surgir al diseñar redes y para así lograr el mejor aprovechamiento de los recursos con que cuentan las empresas actualmente, lo cual es vital en la economía de nuestro país.

Somos partidarios de reutilizar la base de redes instalada actualmente y así mismo aprovechar lo mejor de la tecnología que nos brindan los fabricantes de equipo actualmente, la cual definitivamente está propugnando por un cambio en etapas. Esto queda de manifiesto al analizar sus soluciones, las cuales fuera de dejar desconectada a la

infraestructura actual están proponiendo conectarla transparentemente hacia los medios de alta velocidad que se manejarán en el futuro.
Luego entonces el presente trabajo brindará a quien lo lea una perspectiva global del estado que guardan las redes actualmente y le permitirá tener bases sólidas de juicio para la elección de soluciones acordes con nuestra problemática y nuestros recursos.
La forma en que se plantea la información permite a la gente que no tiene conocimientos en el tema entrar al mundo de las redes. Tratamos de usar un lenguaje claro con los tecnicismos necesarios, ya que finalmente es un documento técnico, pero teniendo en mente brindar algo más que solo información técnica.
Los capítulos I y II tratan de manera seria las tecnologías actuales en lo referente a redes LAN y WAN, se plantean así mismo los beneficios y carencias de los sistemas sin dejar de ofrecer las recomendaciones pertinentes para cada caso.
Estos capítulos nos presentarán las bases sólidas de comprensión, necesarias para entender las partes que conforman las redes, así como sus principios y normatividad para poder entrar de lleno a la conceptualización de una red y tener la capacidad de asimilar las recomendaciones planteadas a lo largo de todo el texto.
Para aquellos que ya conocen las estructuras básicas también ofrece una herramienta de actualización interesante, ya que tratamos con las tecnologías que actualmente se manejan y hablamos acerca de las posibilidades que nos puede deparar el futuro inmediato.
En los capítulos III a V ofrecemos nuestro plan para la organización de la información requerida para normar el criterio de diseño o expansión de redes actuales y/o redes a mediano plazo.
Así mismo mostramos una forma de analizar la información recibida, para estar en posibilidad de asignarle el peso específico e importancia que deberá tener dentro del proyecto de diseño. Esto sin dejar de mostrar ejemplos prácticos para clarificar de la mejor manera posible, los conceptos manejados.
Se analizan así mismo las nuevas tendencias en arquitecturas de red y las razones que han motivado el desarrollo de las mismas.
Buscando la mejor visualización de lo que implica una red, se tratan también temas de interés para el instalador de redes, como son los materiales utilizados para cableado y sus beneficios. Sin dejar de tocar el tan de moda tema del "Cableado Estructurado", que sin lugar a dudas esta ganando adeptos rápidamente por sus múltiples ventajas sobre el cableado convencional.
En el capítulo VI se trata el tema de la administración de las redes, haciendo énfasis en la importancia de que exista un buen control y seguridad, para con esto lograr realmente obtener el mejor desempeño de la red de datos.
A lo largo de todo el trabajo se tratan las consideraciones de diseño, motivo de esta tesis como partes integrales de la información manejada. Esto lo hicimos pensando que es mas sencillo captar el mensaje cuando tenemos la información que lo origina y entonces lo podemos relacionar, que si nos hubiésemos dedicado a concentrar todas las recomendaciones en un capítulo especial, donde tal vez no hubiese existido una secuencia lógica.

ANTECEDENTES

ANTECEDENTES

•Evolución de los sistemas de cómputo

Los sistemas de cómputo desde su inicio en los años 50's, han sido una de las áreas con mayor desarrollo tecnológico, y en los últimos 10 a 15 años se ha incrementado de forma acelerada en todas sus áreas. (Software, Hardware, Comunicaciones, etc.).

Grandes corporaciones, gobiernos, compañías pequeñas, y sobre todo la milicia, basan hoy día sus operaciones normales en el uso de equipo de computo y muchas de ellas en sistemas de información y comunicación extendidos a lo largo de todo el planeta.

Primero en los 50s nacen los sistemas concentradores de información, en los cuales un grupo de gentes se encargaba de recibir la información de las diferentes áreas de las empresas o entidades de gobierno, la cargaban en la computadora central (Captura) y entonces era procesada. Los resultados impresos los entregaban o bien los enviaban por correo o mensajería a los solicitantes.

Esta forma de trabajar presentaba problemas de tiempo, así como de confiabilidad, pues en muchos casos cuando se recibía la información había transcurrido demasiado tiempo y la misma no era tan útil. Es por ésto que nacen los sistemas compartidos (Redes), en los cuales las áreas tenían terminales tontas (No efectuaban ningún proceso propio) y podían ellos mismos capturar su información para ser procesada en la computadora central y en algunos casos hasta la podían imprimir.

Entonces se puede decir que las redes nacen por una necesidad en las empresas de compartir información hacia muchos lugares de manera confiable y expedita, y sobre todo a un costo razonable.

Debido a las cargas de trabajo en las computadoras centrales no fue posible manejar toda la información de todas las áreas, ya que conforme se añadían más terminales a la red, la velocidad de procesamiento bajaba y entonces se tenían nuevamente problemas con el desempeño, utilización, etc.

Por lo mismo, se comenzaron a crear núcleos de trabajo por áreas, en donde cada departamento o área funcional tenía su propia computadora central (Mainframe) y cada quien corría sus propios procesos.

Desgraciadamente la solución anterior sólo aplicaba en empresas muy grandes debido a los costos inherentes al equipo de cómputo.

A mediados de los 70s con la aparición de nuevos componentes a base de silicio y con grandes escalas de integración se abre la posibilidad de construir equipos compactos con mayor inteligencia. Con esta visión nace el concepto de las Computadoras Personales (PC), las cuales permiten tener procesamiento limitado pero a un costo muy atractivo en comparación con los mainframes.

Durante la década de los 70s se popularizó bastante el concepto de PC, hasta se le llamó la era del Floppy disk (Disco Flexible). Las compañías se llenaron con equipos de esta naturaleza, pero persistía el problema de compartir la información, ya que sólo se podía hacer transportando los diskettes de un lugar a otro, con problemas de capacidad y seguridad, lo cual no ocurría con los mainframes.

En base a esta problemática se comenzaron a dar soluciones alternativas mediante enlaces remotos o locales usando los puertos de comunicaciones de las computadoras y los

dispositivos de conexión llamados Modems (**Modulador-Demodulador**), los cuales se conectaban a través de redes telefónicas y permitían compartir información de un punto a otro en forma simultánea sin tener que usar los discos flexibles. También permitió la evolución de las tecnologías de discos duros para almacenar mayor información.
El uso de modems fue muy popular, incluso de forma interna en muchas empresas, pero tenía el inconveniente de no permitir transmisiones de grandes volúmenes de información, debido a que utilizaba el ancho de banda de un canal de voz (3 Khz), lo cual lo limitaba a utilizar en el mejor de los casos una velocidad de 19,200 bps.
A pesar de la popularización de los sistemas de computadoras personales y de las computadoras departamentales, se había retrocedido en una de las premisas iniciales, "Compartir la Información entre todas las Áreas".
Con el nacimiento de la tecnología Winchester para discos duros se abre una nueva puerta en el desarrollo de las PC, ya que se podía tener un medio de almacenamiento comparable al de una mainframe.
Así comienza el desarrollo de la Red de Área Local (LAN), en la cual se pueden compartir recursos entre muchos usuarios a un costo razonable.
Novell Inc. introduce las primeras redes locales (Arcnet y Ethernet) las cuales estaban basadas en una minicomputadora central llamada Servidor (Server en Inglés). Esta máquina se encarga de controlar la información y los recursos de impresión que podían ser accesados desde cualquier computadora conectada a la red.
La respuesta de IBM a esta tecnología fue su propia versión de red local llamada Token Ring.
Ya en los 80's fue muy demandada y aceptada la tecnología de LANs, lo cual relegó a las mainframes únicamente a las grandes corporaciones, que por costos difícilmente cambiaran su infraestructura.
Con las redes de Área Local se resolvió el problema de la comunicación entre áreas dentro de un edificio o incluso cerca de el (unos 2 Km. alrededor).
Ahora bien que sucedía entre tanto con los mainframes. Estos presentaban la posibilidad de interconectarse unos a otros incluso estando en diferentes ciudades y/o países y así enviar y recibir información. Lo anterior lo hacían mediante enlaces privados en Microondas, Satélite y otros medios.
Las redes locales sólo estaban posibilitadas para seguir enviando información en forma remota vía modems y/o multiplexores, pero esto seguía siendo información en lotes (Batch).

•*Redes de Comunicación*

Ahora bien, regresando al medio físico de envío de información tenemos que las redes telefónicas emplean tecnologías de conmutación de circuitos (Conexión y desconexión de enlaces físicos), las cuales permitían a los equipo hacer conexión física prácticamente a cualquier lugar del mundo, a menos de que tuvieran un enlace dedicado o línea privada que no es más que una conexión permanente entre dos puntos de la red telefónica.
Como ya dijimos anteriormente los primeros enlaces de datos se hacían vía telefónica con un módem.
Si se requería que los enlaces fueran permanentes la complejidad de conexiones era increíble, ya que se requería una línea privada de cada PC al punto central (Servidor) y peor aún si se requería intercambiar información entre todas las PC's de forma remota.
De aquí se desprenden dos conceptos para manejar las comunicaciones:

1. Sistemas centralizados — En donde una computadora se encarga de manejar toda la información y el tráfico de los datos.
2. Sistemas Distribuidos — En donde varias computadoras manejan procesos propios (Distribución) y existen equipos externos que se encargan de manejar el tráfico de los datos.

Durante los años 60's y los 70's en nuestro país se utilizó de forma extensiva la conmutación de circuitos en redes telefónicas para transferir datos de una computadora a otra.

En los años 80's el método más empleado para transmisión de tráfico de datos fue la conmutación de mensajes. La cual emplea un dispositivo basado en una PC y el cual se encarga de recibir los mensajes de todas las terminales y enviarlos a sus destinos que están conectados directamente o a través de líneas conmutadas o privadas.

Estos dispositivos de conmutación de mensajes se siguen empleando sobre todo para aplicaciones de correo electrónico. sin embargo presentaban el problema de ser un cuello de botella de las comunicaciones debido a la gran cantidad de información que tenían que manejar y debido a que actuaban de forma dependiente (Maestro-esclavo) uno de otro al estar enviando la información.

Paralelo a estos desarrollos se presentó de nueva cuenta en las redes LAN la problemática del crecimiento, debido a que los servidores no eran capaces de manejar las demandas de sus propias áreas locales, nuevamente era necesario dividir o seccionar las máquinas de acuerdo a sus aplicaciones.

Una alternativa que se presentó fue gracias a los nuevos dispositivos creados para extender la cobertura de las LANs y que permitían empaquetar la información usando un protocolo propietario de la red local. Así se desarrollaron los Puentes (Bridge), los cuales permiten dividir una red local en segmentos funcionales y pueden tener incluso varios servidores compartidos entre diversos usuarios.

Los puentes abrieron un nuevo camino para el envío de información entre redes y mainframes de manera remota a través de canales dedicados, de esta forma nacen las Redes de Área Amplia (WAN).

La conexión de redes vía puentes es muy efectiva si los puntos de destino no son variables, en cuyo caso se hace demasiado costosa, debido a que no puede utilizar los medios convencionales de transmisión (Línea telefónica o privada) porque la densidad de información requiere mayor ancho de banda. Esto nos lleva a la contratación de enlaces satelitales directos o compartidos o algún otro medio de transmisión (Fibra Óptica, Microondas, etc.) con posibilidad de manejar el ancho de banda requerido.

Para resolver dicha problemática se desarrollaron nuevas tecnologías para el envío de información a través de redes públicas, las cuales empaquetan la información y la distribuyen hacia todos los usuarios de la red usando protocolos especiales para ser entregada y descifrada la información.

Esta nueva tecnología presenta las ventajas de distribuir de forma más económica la información además de distribuir la carga de trabajo entre varios procesadores a fin de que si uno falla existen otras rutas para entregar la información

En este punto prácticamente ya estaban resueltos los problemas de envío de información y de compartir la misma de forma segura. Sin embargo y debido a la propia evolución de los sistemas y diversidad de fabricantes se presentaron nuevas problemáticas:

1. Nacieron redes de conmutación de paquetes en cada país industrializado, sin embargo la mayor parte de ellas usaban tecnologías distintas entre sí para la conectividad.
2. Los fabricantes de redes de área local no utilizaban un formato único, por lo cual existían varias tecnologías y no eran compatibles en la mayor parte de los casos.
3. Las demandas de tráfico hicieron que los proveedores de servicios de transporte de datos tasaran en diferentes precios la utilización de los canales de acuerdo al tiempo y horario en que fueran utilizados.

En efecto nuevamente se buscó otra alternativa para la conectividad, muchas empresas prefirieron hacer sus propias redes privadas de comunicación usando Satélites, Fibra Óptica, Microondas y otras tecnologías de enlace.
Sin embargo esto no era lo deseable para la mayor parte de los usuarios que no utilizan constantemente todos los canales y a su máxima capacidad.
Nace entonces una nueva tecnología de equipos de conexión, capaces de elegir la mejor forma de enviar la información sin tener pérdidas de tiempo y desempeño de las redes de área amplia, estos son los ruteadores.
Con esta nueva alternativa podemos programar el medio a utilizar y dar prioridades de uso a los diferentes medios de enlace que posea la empresa.
Además son capaces de conectarse con gran variedad de medios mediante el uso de concentradores, los cuales reciben tarjetas o interfaces de conexión de varios protocolos y/o redes y permiten interconectarlos a través de un solo medio en un solo lugar.
Los ruteadores entonces proveen la solución para la coexistencia de redes LAN en un solo entorno de forma transparente y costeable.

•*Actualidad.*

Con la complejidad de las redes actuales se hace necesario el controlar el funcionamiento de las mismas de forma confiable, y la mayor parte de las veces centralizada.

Así nace el concepto de Administrador de Redes (Internetwork Management) cuyas responsabilidades principales son:

- Configurar.
- Monitorear
- Controlar
- Diagnosticar
- Administrar

Debido a la importancia de este punto se presenta un capitulo dedicado a la administración de todas las conexiones de la red.
Las fuerzas que actualmente impulsan la evolución de los sistemas son:

Demandas de Negocios:	Incrementar la productividad.
	Poder abarcar mercados globales.
	Reingeniería de las empresas.
	Redimensionamiento de las empresas.
Cambios tecnológicos:	Mayor densidad de información (Software Nuevo)
	Mayor Intercambio de información entre puntos distantes.(Mayor ancho de Banda)

Tecnología Asíncrona (Redes Virtuales)
Nuevas aplicaciones: Voz y Video simultáneos con datos,
Multimedia y programas interactivos.

En base a lo aprendido a través de los años ahora los fabricantes de equipo de conectividad y comunicación tratan de ofrecer la solución más rentable y que permita emigrar a tecnología futura con costos razonables.

Así vemos que en las diferentes áreas se comienzan a ofrecer soluciones que permitan prever estos posibles cambios.

- A nivel conexión local "Cableados Estructurados".
- A nivel software "Plataformas de protocolo Abierto como ATM".
- A nivel Hardware "Concentradores o Hubs, modulares".
- A nivel redes de transporte de datos "Posiblemente SDH y SONET".
- A nivel de enlaces locales digitales "RDI".

CAPÍTULO I

GENERALIDADES DE REDES LAN Y WAN.

CAPÍTULO I

GENERALIDADES DE REDES LAN Y WAN

1.1 Redes Locales

Una red local o LAN (Local Area Network) está compuesta por una serie de estaciones de trabajo y servidores conectados entre sí para compartir información y recursos.
Las LAN son medios de comunicación estructurados para distribuir sistemas de procesamiento de datos, dentro de un área máxima aproximada a un campus universitario. Por ende sus características deben ser similares a aquellos sistemas distribuidos (Sistemas de comunicación telefónica) en el área misma, como son capacidad de servicio a usuario dentro de la distancia establecida y servicio local e inmediato, situaciones que no deben presentar mayor problema.

1.1.1 Características de LAN

Las LAN difieren una de otra por sus características técnicas:

Servicios suministrados a una Organización
Velocidad de transferencia de información
Costo y facilidad de conectividad e interoperatividad
Mantenimiento y
Capacidad de crecimiento

1.1.1.1 Velocidades de LAN

De acuerdo con su velocidad se pueden dividir en tres:

1.-LANs de alta velocidad conectadas a computadoras centrales o grandes servidores (servers) con velocidades mayores a 50 Mbps.
2.- LANs de media velocidad de naturaleza interdepartamental interconectando minicomputadoras o servidores pequeños con velocidades en una rango de 10 a 50 Mbps
3.- LANs de baja velocidad que interconectan estaciones de trabajo o computadoras personales dentro de una organización con velocidades de hasta 10 Mbps.

1.1.1.2 Costo y facilidad e interconectividad

Un punto a considerar en la construcción de una LAN es el costo de la conexión del usuario a la misma y por lo general deberá ser proporcional al costo del dispositivo que ejecuta la aplicación requerida por el usuario mismo.

1.1.1.3 Conectividad de LAN

Actualmente más y más organizaciones adquieren equipo de cómputo de diferentes proveedores. Esto es resultado de muchos factores como son disponibilidad de equipo especifico con funcionalidad única, calidad del mismo equipo o el mismo soporte ofrecido, capacidad de crecimiento modular del equipo y hasta fusiones de proveedores específicos y compañías relacionadas.

La conexión heterogénea es por tanto una característica importante cuando se habla del diseño de una LAN.
La solución a esta heterogeneidad de conexiones en las LAN se hace a través del uso y aplicación de normas. Estas normas permiten a las diferentes LANs retener sus características únicas e integrar componentes que cumplan con éstas mismas.

1.1.1.4 Confiabilidad de las LAN

Lo más importante en una LAN es su confiabilidad dado que una organización está dependiendo de ella para la transferencia de datos y comunicaciones, por tanto los sistemas de LAN deben contar con la capacidad de recuperación casi inmediata o al menos presentar alternativas en caso de que falle algún componente, hacemos énfasis de que el usuario final no pude darse el lujo de dudar de la integridad de los datos que maneje la LAN.

1.1.1.5 Capacidad de crecimiento, reconfiguración de mantenimiento.

Estos aspectos son importantes ya que las necesidades de las organizaciones están en constante cambio y optimización de recursos, por lo que las LAN deben tener la capacidad de adaptarse a las nuevas necesidades de negocio. Así mismo deben contar con mecanismos que permitan un fácil mantenimiento que contemple costos y tiempos de reparación.

1.1.2 La organización internacional de estándares (ISO) y el modelo de interconexión de sistemas abiertos (OSI).

La Organización Internacional de Estándares (ISO) es una asociación independiente localizada en Ginebra, Suiza que está encargada de la generación de estándares a nivel mundial. La ISO opera para coordinar los esfuerzos de otros organismos estandarizadores como el Instituto de Estándares Nacionales Americanos (ANSI) y la Institución Británica de Estándares (BSI).
Las recomendaciones de ISO en Interconexión de Sistemas Abiertos (OSI) tienen un peso muy grande en el mercado. La meta de los estándares OSI es que sea posible compartir e intercambiar información entre una computadora y una red de diferentes fabricantes.
El OSI es un modelo de 7 capas, que se muestra en la figura 1.1, que fue publicado en 1974. Cada capa realiza diferentes funciones. Cuando se aplica a redes todas las capas se toman en cuenta para constituir las piezas individuales para construir una red, como lo es una LAN, una WAN o una combinación de ambas. Este modelo define los estándares internacionales por los cuales un sistema abierto puede comunicarse con otro sistema abierto y también pone las reglas para aquellos estándares que se estén implementando.
Es importante notar que cada capa es totalmente independiente de las otras y más aún las capas OSI proveen servicios a las capas adyacentes a cada una. Por ejemplo, la capa de enlace de datos provee servicios a las capas física y de red pero opera independiente a estas.

Cada capa en el modelo participa con funciones específicas de comunicación de las computadoras.
1)FÍSICA: Esta capa es la menor y describe al medio físico de conexión, es decir las señales de transmisión a través de la conexión física del equipo terminal de datos y el equipo de comunicación de datos.

CAPA 7	APLICACIÓN
CAPA 6	PRESENTACIÓN
CAPA 5	SESIÓN
CAPA 4	TRANSPORTE
CAPA 3	COMUNICACIÓN DE RED
CAPA 2	ENLACE DE DATOS
CAPA 1	FÍSICA.

Figura 1.1. Las capas del modelo OSI.

La capa física transmite los bits que se mueven a lo largo del cable, esta es responsable de asegurarse que los bits viajen íntegramente de un lugar a otro sin importar que exista en medio. Esta capa trata de las características eléctricas y mecánicas del cable y de la conexión mecánica y eléctrica hacia la red.
Esta capa también especifica las características mecánicas de los conectores a ser usados en las terminales del cable, y controla las propiedades eléctricas de estos en cuanto a voltaje y frecuencia, técnicas de modulación o tipos de señales con las que deberán trabajar en la red.
Así mismo define el tiempo que deberá estar presente el voltaje en las terminales para poder reconocer un 0 o un 1 lógico como señales válidas.
El medio físico puede ser cable (Coaxial o par trenzado), inalámbrico (Microondas, radio o satélite) o bien óptico (Fibra o láser).
Se han normalizado gran cantidad de interfaces para este nivel y los más importantes son RS-232-C, V-24, X.21, V.35
Un ejemplo de equipo que opera en esta capa física sería el repetidor.
2)ENLACE DE DATOS: Esta es la segunda capa y trata con los medios de transmisión de datos entre dispositivos dentro de la misma red.
La misión de esta capa es permitir transferencias confiables de datos a través de la capa física; enviando bloques de datos con un flujo apropiado y tener el control de errores.
El protocolo HDLC (High-Level Data Link Control, Enlace de control de datos de alto nivel) define la operación e interfaces para esta capa. Actualmente se descompone en dos subcapas que son:
1)LLC (Logical Link Control)Control de enlace lógico
2)MAC (Medium Access Control) Control de acceso al medio.

1)Las funciones de los dispositivos que operan en esta subcapa son: Sincronización de la trama, Limitación de mensajes, Control de errores, Ordenamiento de datos, y Multiplexaje.

2)En esta subcapa se introduce el direccionamiento de los dispositivos, estas direcciones normalmente se conocen como dirección de máquina o dirección física y permiten tener un modo único de identificar a cada dispositivo dentro de la red.
Esta capa permite asegurar transferencias confiables a través de la capa física debido a que envía la información en bloques de datos con su sincronización apropiada, así como un control de flujo y de errores. tomando los bits de la capa física y transformando estos en una señal libre de errores para ser procesados por la capa de comunicación de red.
Las tecnologías de LAN como Ethernet, Token Ring y FDDI operan en esta capa.
Los puentes y los conmutadores son ejemplos de equipo para esta capa.

3)COMUNICACIÓN DE RED: Esta capa a diferencia de las dos anteriores trata con la transferencia de datos de dispositivos ubicados en *diferentes* redes.
Provee el medio para establecer, mantener y terminar las conexiones entre los sistemas. Trata con la conmutación y el enrutamiento de la información. Así mismo es la responsable de traducir las direcciones lógicas o nombres en direcciones físicas o conexiones.
Esta capa añade el concepto de dirección de red, usando un identificador único para cada red intermedia entre la fuente de datos y el destino o equipo terminal.
En este nivel se incluye X.25
Esta es la capa en la cual operan los ruteadores.
4)TRANSPORTE: La capa de transporte básicamente es el enlace entre las tres capas anteriores y las tres superiores, estableciendo el nivel de calidad.
Es responsable de asegurarse que los datos estén libres de errores antes de pasar a la capa 3, es decir se asegura de que los datos se envíen exitosamente entre las dos computadoras. En caso de existir un error en el envío es responsable de solicitar la retransmisión de los mismos.
Este nivel exige que el usuario defina a la red la calidad de servicio que desea, para así establecer el protocolo necesario en la comunicación con las capas superiores.
5)SESIÓN: Este nivel se encarga de controlar las sesiones entre dos computadoras mediante un mecanismo organizado para el intercambio de datos entre usuarios.
Aquí se coordina la comunicación entre dos o más aplicaciones, así se establece la administración y la decisión en comenzar o terminar una comunicación entre dos computadoras. Esta trata con los programas que se están corriendo en cada máquina para establecer conversaciones entre ellos.
Así pues permite que el usuario defina sus parámetros de comunicación; si va a ser bidireccional ó bien unidireccional, los puntos de sincronía para comprobar flujo de paquetes, así como recuperación de los mismos, abortar o arrancar comunicaciones y acelerar el flujo normal de datos.
6)PRESENTACIÓN: Este nivel asigna la sintaxis de los datos.
Aquí se convierten las aplicaciones en formato de datos a aplicaciones en forma legible (Ejemplo: ASCCI, SYLK, DIF). En otras palabras la sexta capa efectúa las conversiones de códigos y reformateo de los datos y viene a ser el traductor de la red, asegurándose de que la máquina está hablando en el lenguaje correcto hacia la red.
7)APLICACIÓN: En esta capa se encuentran las aplicaciones del usuario. Contiene los elementos necesarios para procesar la información que entrega el usuario a través de una terminal virtual.
Esta es la interface entre el software que corre en las computadoras y el de la red. Dicha capa permite aplicaciones en la computadora como correo electrónico o transferencia de archivos.
En esta y las dos capas anteriores trabajan los gateways.
En el modelo OSI el usuario presenta los datos en la capa superior. Los datos se pasan a través de todas las capas y se les va adicionando el direccionamiento y la información de control necesaria hasta llegar a la capa física donde es enviado al otro dispositivo y en donde se hacen las funciones inversas.

Finalmente se puede definir un protocolo como la colección de instrucciones que permiten gobernar la transferencia de datos entre capas iguales del modelo OSI.

1.1.3 El Modelo IEEE

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE en Inglés) propuso una variante del modelo OSI, la cual es ampliamente utilizada.
Para el equivalente de la capa de ENLACE DE DATOS maneja el MAC (Medium Acces Control), medio de control de acceso. Esta es una técnica de acceso específico la cual describe como un dispositivo es reconocido sobre el medio de transmisión.
Para las capas superiores presenta únicamente el LLC (Logical Link Control).

1.1.4 Topologías

La topología es la configuración física y lógica de una red. El término es usado para describir la distribución de la red .
Una topología es un diseño arquitectónico de una red, que muestra la estructura general de un sistema de comunicaciones. Las topologías son importantes; ya que no únicamente describen la red, sino que muestran el tipo específico de red. Son esquemas que deben mostrar la distribución de la red. Generalmente, no incluye dispositivos como PCs o impresoras, mostrando el método de acceso como lo son Ethernet, Token Ring, FDDI, etc. y nombres específicos y direcciones de redes que son usados para identificar los componentes de una red.
Hay 4 tipos principales de topologías: Estrella, Anillo, Bus y Árbol.

1.1.4.1 Topología en Estrella

Esta topología es probablemente la más antigua de las topologías usada en comunicaciones. Fue aplicada inicialmente en sistemas de telefonía.
En este tipo de topología todas las estaciones están unidas a un punto común mediante un cable, generalmente es un concentrador.
Cuando todas las estaciones están unidas punto a punto a un concentrador, es probable que el costo sea superior que al de otras topologías.
La ventaja de esta topología es que como el cubleado es a un punto, en caso de falla no se afectaría al resto de la red, sino solamente a la estación conectada por este cable.
La desventaja de esta topología es su concentrador central que puede ser el punto de falla único, que en caso de estar deshabilitado afectará a todas las conexiones. Actualmente los concentradores son más tolerantes a fallas con la llegada de dispositivos tales como fuentes de poder redundantes, cambio en línea (hot swap) que han reducido la posibilidad de que ocurran fallas.

1.1.4.2 Topología en Anillo

En esta topología todas las estaciones son consideradas como repetidoras y están contenidas en un anillo. No hay puntos terminales en esta topología. El repetidor, en este caso, es la tarjeta controladora en la estación que esta conectada a la LAN.
Cada estación recibirá una transmisión en un extremo del repetidor y se limitará a repetir la transmisión bit por bit sin almacenamiento, al otro extremo del repetidor. La transmisión de

datos es en una sola dirección y es recibida por el siguiente repetidor en el anillo. La transmisión de estaciones puede ser recibida por cualquier estación conectada al mismo cable; a esto se llama medio de transmisión.
Ya que cada controlador en una estación de la red es un repetidor cada estación repite cualquier señal que está en la red sin importar que la señal este destinada a una estación en particular. Esto podía tener implicaciones críticas para el anillo. Si por cualquier razón un repetidor se rompiera o dejara de repetir, podría ocasionar una falla general en la red. Aunque las posibilidades de que esto ocurra son remotas siempre existirá esta misma.
El controlador es capaz de manejar este problema y el repetidor defectuoso es capaz de aislarse del anillo permitiendo a éste que se estabilice y seguir funcionando.
La LAN que mejor representa a esta topología es la de Token Ring. Aunque el cableado físico de esta topología es una estrella, lógicamente Token Ring es una topología de anillo comúnmente referido comoun anillo cableado en estrella.

1.1.4.3 Topología de Bus

Esta topología también es conocida como topología de bus lineal. Es un diseño simple que usa un cable conocido también como medio para unir a las estaciones de trabajo. Todas las estaciones comparten este cable único. Las transmisiones de las estaciones pueden ser recibidas por cualquier estación conectada a este cable; a esto se le llama medio de transmisión. Hay puntos finales definidos en el segmento del cable utilizado, generalmente llamados terminadores.
Dada la simplicidad de esta topología el costo de su implementación es bajo. Sin embargo debido a su configuración física el cable puede ser un punto de falla, si esto sucede, ninguna estación estará habilitada para transmitir. Aunque el cable es un dispositivo pasivo, algo tan sencillo como un corte en el mismo podrá volver a la red inoperante.
La LAN más representativa de esta topología es la Ethernet,la cual tiene la capacidad de incorporar una amplia gama de cables.

1.1.4.4 Topología de Árbol

La topología de árbol es una generalización de la topología de bus lineal. El cableado es conocido como ramal, y todas las estaciones se conectan a él. La topología de árbol tiene un punto concentrador conocido como raíz. Esto es donde empieza el árbol. De aquí, el árbol dispersa sus ramales en diferentes direcciones desde la raíz. Estos ramales se extienden a puntos terminales de la red. Esto permite a una red crecer dinámicamente pero sólo habrá un camino para los datos activos entre cualquiera de dos puntos en la red. La red que mejor representa esta topología es la red que no utiliza anillos en su topología. Un ejemplo de esto es el algoritmo de Spannig tree para redes Ethernet. Este algoritmo deshabilita otros ramales hacia el mismo punto que pudiesen estar en anillo.

1.1.5 Ethernet

1.1.5.1 Antecedentes

La norma 802.3 nace del sistema ALOHA, desarrollado por Norman Abramson, en la Universidad de Hawai durante la década de los 70s. Utilizaba una difusión por radio con base terrestre, la idea básica consistía en un sistema conteniendo usuarios no coordinados

compitiendo por el uso de un solo canal. A esta primera versión, se le incluyó la detección de portadora, y la compañía Xerox construyó un sistema **CSMA/CD**(CARRIER SENSE MULTIPLE ACCES/COLLISION DETECTION) de 2.94 Mbps para conectar hasta 100 estaciones personales de trabajo en un cable de 1 km. de longitud. A este sistema se le llamó **ETHERNET**, en honor del éter lumífero, a través del cual se pensó alguna vez que se propagaban las ondas electromagnéticas. La Ethernet desarrollada por Xerox tuvo tanto éxito, que las compañías Xerox, DEC, e Intel propusieron una norma para la Ethernet de 10 Mbps; la cual constituyó la base para la 802.3. La norma que se publicó como la 802.3 difiere de la especificación correspondiente a la Ethernet en el sentido de que describe una familia completa de sistemas operando a velocidades que van de 1 a 10 Mbps, en varios medios físicos .
La norma inicial también da los parámetros para un sistema de banda base de 10 Mbps, utilizando un cable coaxial de 50 Ω.
La topología utilizada en Ethernet se muestra en la figura 1.2.

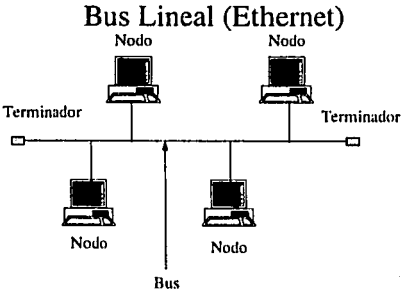


Figura 1.2. Bus Lineal Ethernet

1.1.5.2 Cableado para Ethernet

1.1.5.2.1 Cable Coaxial Grueso

Cuando por primera vez fue introducida la red Ethernet en 1980 como un producto de red comercial y normalizado, el esquema del cableado en bus conocido en ese momento era el cable coaxial grueso. Este cable es similar al comercialmente llamado RG-8 pero es exclusivo para cableados Ethernet. Fue especialmente fabricado y por ello muy caro, al mismo tiempo, era difícil de trabajar y requería de herramientas especiales para la conexión de estaciones, sin embargo permitió que un tramo de cable transportara la señal sin uso de repetidores hasta 500 metros. También estaba provisto de dos capas de blindaje para ser usado en diferentes ambientes de trabajo (fábricas, oficinas, escuelas, etc.).

1.1.5.2.2 Cable Coaxial Delgado

En 1984 se revisó la estructura del cableado Ethernet, ya que la experiencia demostró que el cable original era demasiado robusto, haciéndose difícil de trabajar y de implementar en las múltiples aplicaciones de Ethernet. Se utilizó un cable coaxial delgado el cual es comercialmente adquirido y es el tipo RG-58A/U. Éste es mucho más fácil de trabajar, de menor costo y su blindaje es adecuado para las instalaciones. De 1985 a 1990, el cable coaxial delgado fue el más comúnmente usado en el mercado comercial en redes de 2 a 10 estaciones. El tiempo de instalación de una estación al bus se redujo de 5 a 1 minuto.

1.1.5.2.3 Cable UTP (Unshielded Twisted Pair)

Al avanzar la tecnología el costo de algunos componentes se redujo de modo tal que el cable telefónico común, fácilmente se pudo adaptar para uso de la Ethernet. Este cable es muy barato ya que ha sido fabricado para uso telefónico por años. Los controladores para Ethernet fueron reconstruidos para poder manejar las ineficiencias de este tipo de cable. A diferencia de la topología de bus UTP permite también el cableado de sistemas en estrella que permiten la administración de la red por medio de una sola estación. Actualmente éste es el cableado más popular en redes Ethernet.

1.1.5.3 Nombres utilizados para los Cableados Ethernet

Al paso de los años, Ethernet ha cambiado sus esquemas de cableado para hacer esto más fácil de manejar y para obtener un mejor costo-beneficio. Desafortunadamente, cada tipo de cable adoptó más de un nombre por lo que queremos explicar a continuación el resumen de los tres tipos más usados para cableado en Ethernet, como se muestran en la figura 1.3.

Nombre	Coaxial Grueso	Coaxial Delgado	Par Trenzado Sin Blindaje
Tipo de Cable	RG-8	RG-58	22 - 26 AWG
Nombre IEEE	10BASE5	10BASE2	10BASET
Norma	IEEE 802.3	IEEE 802.3	IEEE 802.3

Figura 1.3. Tipos de cableado para Ethernet.

El primer renglón especifica el nombre comercial del tipo de cable.
El segundo renglón muestra el tipo de cable, en el caso de UTP se está especificando el calibre del mismo.
El tercer renglón representa un nombre codificado con las siguientes características:
<velocidad><tipo de señal><longitud máxima sin repetición de señal por 100 metros>.
Por ejemplo 10BASE5 es un cable con una velocidad de transmisión de 10 Mbps y señal de banda base (1V pico a pico de amplitud y 1 W de potencia) y con 500 metros de longitud. 10BASET es el nombre de la IEEE para el par trenzado sin blindaje (UTP) en donde la T significa par trenzado con una longitud de 100 metros.
El cuarto renglón, representa la norma para un tipo particular de cable.

1.1.5.4 Estructura del Cable coaxial Grueso

Este cable consiste de un conductor central hecho de cobre estañado, el cual es el conductor de la señal. Alrededor de éste lleva una capa aislante la cual a su vez esta cubierta por una delgada capa laminar.
Cubriendo todas esta capas existe un blindaje electromagnético.
La capa externa del cable coaxial grueso es de cloruro de polivinilo (PVC), generalmente de color amarillo. Lleva un tipo de cubierta de teflón para cumplir con normas de resistencia al fuego.

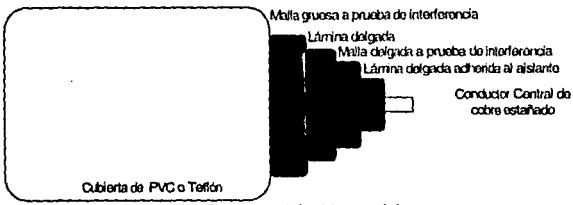


Figura 1.4. Estructura del cable coaxial grueso.

1.1.5.5 Conexión del Cable Coaxial Grueso.Los múltiples componentes de conexión son:

Tarjeta controladora de Ethernet (NIC)
Transceptor externo
Cable del Transceptor
Cable Coaxial Grueso

La tarjeta de interface controladora de Ethernet (NIC) se encarga del flujo de información entre la conexión a la red y el cable del bus central de la red, es decir, toma la información de la computadora y la transforma a un formato en la que el sistema Ethernet puede transmitir o recibir información. Se encuentra generalmente dentro de la computadora.
Los transceptores (transceivers) conectan el cable del bus al controlador. Debido al diseño del cable y a la densidad de componentes de la tarjeta controladora los transceptor son externos. Cada 2.5 metros habrá una marca en el cable coaxial grueso que indica la conexión propia para el transceptor. El transceptor puede conectarse aún en el caso de que la red este en funcionamiento. Entre el transceptor y la tarjeta controladora existe un cable que transporta la señal de comunicación entre ambos el cual no debe exceder 50 metros. Los conectores entre la tarjeta controladora y el transceptor externo son del tipo DB-15 o AUI.

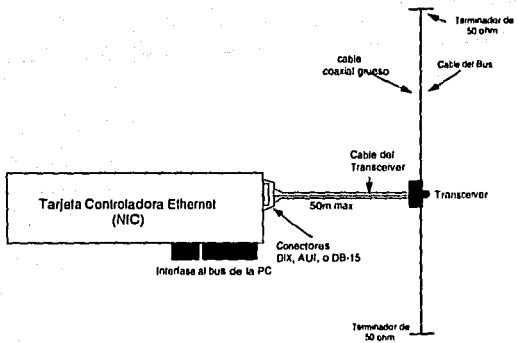


Figura 1.5. Conexión física del cable coaxial grueso.

El cable del transceptor se conecta directamente al conector DB15 o AUI que se encuentra sobre la tarjeta controladora y el otro extremo del cable del transceptor DB15 o AUI se conecta la transceptor mismo.
Cabe aclarar que cada extremo del bus troncal o principal debe contar con un terminador que consiste en una resistencia de 50 Ω.
El segmento del bus de cable coaxial grueso entre el transceptor y la tarjeta controladora no debe exceder de 50 metros. Así mismo no puede tener más de 100 nodos o conexiones sobre el mismo segmento.
Cabe mencionar que el cable coaxial grueso es usado como backbone para instalaciones en fábricas por su longitud y capacidad de blindaje.

1.1.5.6 Transceptores (Transceivers)

Para poder transmitir o recibir información en una Ethernet es necesario el uso de un transceptor. Su función es la de acoplar la tarjeta controladora con el bus principal y proveer los medios de transmisión y recepción de señales. El transceptor también detecta errores y notifica a la tarjeta controladora de ese error para que tome la acción necesaria para corregir.
Solo en el caso de cable coaxial grueso los transceptores son externos a la tarjeta controladora.
La mayoría de los transceptores externos tienen LEDs indicadores de estado de ciertas condiciones como son:
Alimentación: Indica la presencia de alimentación de la tarjeta controladora.
Transmisión de datos: Si ha sido detectada transmisión de datos en el cable.
Colisión: Si dos estaciones de trabajo han trasmitido al mismo tiempo sobre el cable (Esta es una condición de error.

SQE(Signal Quality Error):Esta es una condición de la señal que indica el estado del transceptor a la tarjeta controladora de Ethernet.

1.1.5.7 Cable Coaxial Delgado

Después de la introducción de Ethernet se comprobó que el cable coaxial grueso era demasiado robusto difícil de trabajar y de costo elevado. La idea para que la LAN Ethernet fuera exitosa implicaba un análisis del tipo de cableado. Esta fue la razón por la que se introdujo el cable coaxial delgado, el cual utilizaba la misma topología y el mismo concepto. Este cambio se agregó a la IEEE 802.3 como IEEE 802.3a. La representación de la IEEE para este tipo de cable coaxial fue el llamado 10BASE2, ya que tenía una velocidad de transmisión de 10 Mbps., transmisión en banda base y un segmento de cable de 185 m máximo sin uso de repetidor.

La diferencia más notable entre ambos cables, es que el delgado tiene mucho menos blindaje. El cable coaxial delgado tiene una parte externa de plástico generalmente de color negro. Bajo esta cubierta plástica existe un recubrimiento muy delgado de malla que es el más adecuado para la mayoría de las instalaciones Ethernet, esta malla provee el blindaje necesario para evitar interferencias de señales electromagnéticas. Bajo la malla está la cubierta de polietileno y bajo la misma en el centro se localiza el cable rígido de cobre estañado.

Existen algunas restricciones para este tipo de cable, siendo la principal el hecho de que debe tener menos conexiones por segmento y el segmento es de menor longitud. Aún así el cable coaxial delgado se convirtió en el más usado para instalaciones Ethernet hasta 1990, cuando el par trenzado telefónico sin blindaje (UTP) apareció como una mejor opción en estas instalaciones.

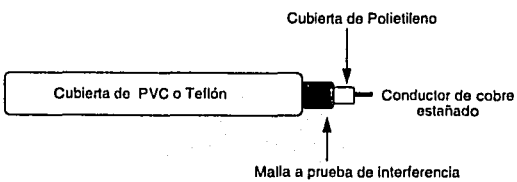


Figura 1.6. Estructura física del cable coaxial delgado.

1.1.5.8 Conexión del Cable Coaxial Delgado

Con la aparición de un sistema nuevo de cableado apareció también una manera de conectar las tarjetas controladoras Ethernet al cable. El cable coaxial delgado eliminó la necesidad de acorazar el cable del bus, de igual manera eliminó el transceptor externo y el cable del mismo. Introdujo dos nuevos conectores conocidos como BNC y conector T.

Un tramo de cable coaxial delgado corre entre cada uno de los dispositivos conectados. Este tramo de cable es pre-cortado a una longitud específica no menor a medio metro y a una longitud no mayor de 185 metros. Las tarjetas controladoras son ahora concatenadas una con otra a través del cable del bus común. El cable principal está conectado directamente a

las tarjetas controladoras por medio de un conector T. Existen 3 puntos de contacto en el conector T: un punto del conector T se conecta directamente a la tarjeta controladora y los otros 2 puntos directamente al cable principal.
Los extremos del cable siguen utilizando los terminadores de 50 Ω.
Este tipo de cableado tiene ciertas restricciones. No deben existir más de 30 conexiones al cable principal, las estaciones no deben estar más cerca de medio metro una de la otra, con la excepción de las tarjetas controladoras de red para lap top PCMCIA (Personal Computer Memory Card International Association) en las que los conectores T deberán estar conectados directamente al controlador de Ethernet.

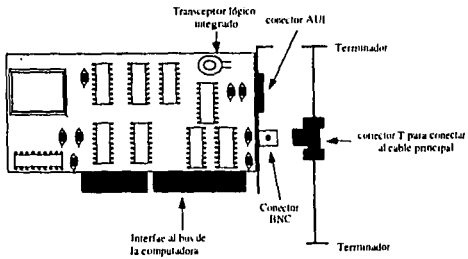


Figura 1.7. Conexión física del cable coaxial delgado.

Con la llegada del cable coaxial delgado los transceptores externos emigraron a las tarjetas controladoras de red como parte integral de las mismas, cumpliendo con las mismas funciones anteriores, ésto eliminó componentes costosos y permitió a la tarjeta controladora Ethernet reducir su costo en comparación a la anteriormente usada. Las tarjetas controladoras para cable coaxial delgado presentan los 2 tipos de conectores según sea el caso para cable coaxial grueso o delgado, es decir, conectores DB-15 (AUI) y conector BNC.
La tarjeta controladora de red puede escoger entre conectores para cable grueso o delgado por medio de software o conmutadores en el hardware, o puede ser autosensante. Cabe mencionar que únicamente se podrá usar un tipo de conector para cada tarjeta controladora de red.

1.1.5.9 Cableado con Par Trenzado sin Blindaje (UTP)

En octubre de 1990, la IEEE normalizó un nuevo tipo de cable conocido como UTP. Inicialmente, era el mismo tipo de cable utilizado en conexiones telefónicas. Era el 24 AWG (American Wiring Gauge), con 75-150 Ω de impedancia. Actualmente existe una gran diversidad de clasificaciones para este tipo de cable normalizado por la EIA (Electronic Industries Association) bajo la norma TIA568A. Esta norma incluye UTP para muchos tipos de cable UTP, pero para nuestro propósito es de interés el usado en redes.
UTP está definido para el grado de datos en categorías 3, 4 y 5.

La categoría 3 es usado en LANs con velocidades de hasta 10 Mbps.
La categoría 4 es usado en LANs con velocidades de hasta 16 Mbps.
La categoría 5 es usado en LANs con velocidades de hasta 100 Mbps.
La configuración física consta de 4 pares de cables trenzados. La cubierta de plástico encierra el cable de cobre y tiene un código de colores. Cada color del par debe estar trenzado por lo menos 2 vueltas por pie. A mayor categoría, mayor número de vueltas por pie, lo que permite mayores velocidades. Cada par de color está mezclado con el color blanco por ende el par 1 es azul con franjas blancas y blanco con franjas azules, así sucesivamente para naranja, verde y café. Ya que la impedancia de cada cable puede variar de 75 a 150 Ω, existen puentes en la tarjeta controladora de la LAN que permiten a la tarjeta acoplarse al tipo de impedancia del cable.
La configuración de pins para el Ethernet UTP (10BASET) es el par azul en pins 1 y 2 y el par naranja en pins 3 y 6. Un cable de la categoría 5 puede ser usado en cualquiera de la redes LAN utilizando la norma TIA568A mostrado en la figura 1.8. Los conectores para UTP están normalizados como RJ-45 para los 3 tipos de redes.

Par	*T568A*	*10BASET*	*Token Ring*	*FDDI*
Uno	**4 y 5**	**1 y 2**	**4 y 5**	**1 y 2**
Dos	**3 y 6**	**3 y 6**	**3 y 6**	**7 y 8**
Tres	**1 y 2**			
Cuatro	**7 y 8**			

Figura 1.8 Configuración de pins para cable UTP.

La primer compañía que promovió Ethernet por medio de cable telefónico fue Synoptics en 1985. Este tipo de cableado introdujo la topología de estrella. Al mismo tiempo, Ethernet estaba bajo presión por la introducción de Token Ring y su nueva norma de la compañía IBM, la cual se demoró en la implementación de Token Ring mediante UTP, sin embargo, Ethernet aprovechó esta circunstancia para implantar el cableado UTP.
Con el cableado coaxial grueso y delgado, la administración individual de estaciones de trabajo eran difíciles de implantar. Esta es una característica de la topología de bus. Con cable coaxial todas las estaciones están conectadas a un cable común, permitiendo un solo punto de falla. Si el cable principal se deshabilita, también todas las estaciones conectadas a él se deshabilitan. Además la administración individual de cada estación de trabajo era casi imposible.
Con la aparición de UTP no solo se presentó una nueva topología sino que también nuevos componentes. Con la topología en estrella, hay un componente central al que todas las estaciones se conectan. Este es el concentrador central conocido como *hub* (concentrador de cableado). Es el punto terminal de todas las estaciones de la red. Las estaciones pueden ser conectadas una con otra siendo esto válido solo para 2 estaciones.
Existe una relación uno a uno entre la tarjeta controladora Ethernet y el repetidor. El controlador conecta a puertos individuales en el concentrador.
Los conectores fueron cambiados a RG-45, este conector es de plástico tiene 8 pins y una pequeña pestaña que facilita su conexión y desconexión a la roseta. Los pins usados en este conector son la 1, 2, 3 y 6. El transceptor está localizado en la tarjeta controladora de red. El

transceptor fue modificado para aceptar el tipo de cable pero las funciones siguieron siendo las mismas que las anteriormente usadas con otros cables.

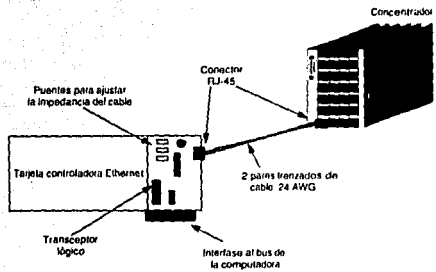


Figura 1.9. Interconexión Física entre tarjeta controladora y concentrador.

Un aspecto interesante de este tipo de cableado es que los terminadores de 50 Ω ya no se ocupan. Puesto que la impedancia del cable puede variar de 75-150 Ω hay unos puentes para igualar la impedancia de la tarjeta controladora y el cable. Antes de que el controlador sea conectado al cable, debe medirse la impedancia del mismo. Esto a través de un probador de cables. De esta forma se pueden posicionar correctamente los puentes de la tarjeta controladora.
La tarjeta controladora no debe estar a más de 100 metros del repetidor o concentrador
El punto central en el cableado con UTP son los concentradores o hubs. Todos los módulos de la red Ethernet son terminados en este módulo repetidor. A esto se le llama cableado punto a punto. Una vez que la señal entra en el repetidor, ésta es regenerada en cada puerto que se encuentre activo en el repetidor.

1.1.5.10 Concentradores de cableado o Hubs

Existen repetidores para cada tipo de cableado, sin embargo hay algunos que tienen la capacidad de aceptar a los tres diferentes tipos, todos dentro de un mismo dispositivo, llamado concentrador o hub. Todas las conexiones en este dispositivo tienen la habilidad de comunicarse con cualquier otra conexión. Esto es posible gracias a que el concentrador contiene también los dispositivos conocidos como módulos repetidores, cada módulo se desliza en una ranura encontrada dentro del concentrador y es un repetidor diferente y separado para cada tipo de cable. Los módulos se comunican uno con otro a través de la tarjeta madre, esto es, un receptáculo común, al que se conectan todos los módulos.
Este tipo de dispositivo mejoró la capacidad de Ethernet al ser posible una topología física de estrella dentro del concentrador y mejorar la administración de red
Un concentrador puede soportar diferentes tipos de cableado y de igual modo diferentes tipos de medios de acceso (Ethernet, Token Ring, etc.). Estos son mantenidos en tarjetas madres por separado y no pueden comunicarse entre sí, sin el uso de un puente o un ruteador. La ventaja es que están contenidas dentro de un mismo dispositivo que permite

una mejor administración de red. Las conexiones de 10BASET punto a punto llegan a uno de los módulos en el repetidor. Otro módulo en el repetidor permite conexiones a 10BASE2, finalmente, otro módulo permite la conexión a 10BASE5. No existe una configuración fija para el cableado de los módulos por lo que un concentrador puede contener todos los módulos en 10BASET o parte de ellos en 10BASE2 y así sucesivamente. Puede incluso contener módulos en fibra óptica que son recomendados en los casos en que las distancias sean hasta de 2 km. y para evitar el uso de repetidores. A este tipo de cableado se le conoce como 10BASEF. Esto también es recomendable cuando las instalaciones están propensas a grandes interferencias como puede ser el caso del sector Industrial. No existe ninguna restricción al número de módulos que pueden ser contenidos en el concentrador; esto lo especifica el fabricante.

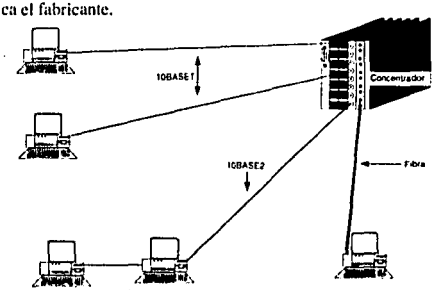


Figura 1.10. Cableado entre las estaciones y el concentrador.

1.1.5.11 Cableado por Fibra Óptica

La adición de 10BASE-F a la norma 802.3, la cual permite la utilización de fibra óptica, cambia la visión de la norma significativamente. Para aumentar la utilidad de esta nueva implementación en la capa física, se ha desarrollado un nuevo método de diseño y validación para grandes topologías.

Con 10BASE-F se permite tener hasta 5 repetidores conectados en cascada para redes que combinan 10BASET, 10BASE-F.

Existe otra norma para convertir un segmento de enlace de fibra óptica en UTP, llamado enlace entre repetidores de fibra óptica (FOIRL), el cual es utilizado en redes que requieren de enlaces no mayores de 2 km. de distancia.

Consecuentemente existe más flexibilidad para un futuro crecimiento de una Ethernet sin la adición de un puente, ruteador o conmutador.

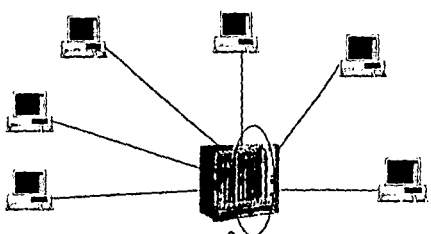
1.1.6 Token Ring, su capa física

1.1.6.1 Antecedentes

Esta tecnología surge de la necesidad de IBM de incursionar en el mercado de las redes locales. El trabajo inicial fue presentado al comité de la IEEE en 1982 y el primer prototipo fue demostrado en 1983 en Ginebra, Suiza.

El sistema de cableado que IBM presentó para Token Ring fue presentado en 1984. Utilizaba únicamente cables UTP y STP. IBM anunció oficialmente el producto en 1985, además de ser normalizado ese año por el comité de la IEEE 802.5 como el único método de acceso en anillo aceptado por el comité de la IEEE. Por muchos años, fue el único método de acceso soportado por IBM. Debido a la tardía implementación de este método de acceso presentado por IBM, Ethernet ganó mucho más mercado y una posición firme en el mismo, cuando una compañía llamada SynOptics presentó una topología cableada en forma de estrella física, para la norma Ethernet. IBM soporta los métodos de acceso IEEE 802.3, FDDI e IEEE 802.5, así como también los protocolos de red TCP/IP, como protocolos para terminales de acceso y sus servidores.

Esta topología es conocida también como estrella anillo. En este caso el anillo se encuentra dentro de un ruteador de señal conocido también como concentrador inteligente (Administrable) o repetidor, al cual se conectan uno a uno las estaciones de trabajo o nodos formando una estrella. La señal siempre pasa por el ruteador. Típicamente este arreglo utiliza cable de par trenzado manejando velocidades de 4 a 16 Mbps. La ventaja de utilizar esta topología y no el anillo físico es que si una estación falla o se desconecta el concentrador de inmediato cierra el anillo evitando la caída de la red.



El anillo se realiza dentro del concentrador central

Figura 1.11. El anillo de Token Ring.

Existen únicamente dos versiones de cableado para Token Ring: Par trenzado sin blindaje (UTP) y par trenzado con blindaje (STP).

Los conectores usados para el cableado de Token Ring pueden ser DB-9, RJ-11, RJ-45 o conector universal de datos (UDC).

Dado que la topología física es en estrella todo el cableado es terminado en un dispositivo central, que se llama unidad de acceso multiestación (MAU). Cuando IBM introdujo Token

Ring en 1984, existía un solo tipo de MAU. Actualmente estos, se han transformado en concentradores de cableado que son similares en funcionamiento a los usados en Ethernet. Así como en Ethernet, Token Ring tiene dispositivos que pueden extender el cableado y son conocidos como repetidores. La fibra óptica puede ser usada entre el MAU y la conexión a la red, cabe aclarar que este no es parte del esquema presentado por IBM. La fibra óptica esta especificada para interconectar MAUs.
La tarjeta controladora de la red es también diferente para Token Ring. Para poder conectar una estación al cable principal de la red, la tarjeta deberá estar especificada como tarjeta controladora de Token Ring. Las tarjetas controladoras no tienen la capacidad para interfuncionar entre los diferentes métodos de acceso.

1.1.6.2 Tipos de cableado para Token Ring

Aún cuando Token Ring utiliza cable UTP o STP, existen algunas versiones diferentes del cable de acuerdo a la clasificación de IBM:

Tipo 1
Es un cable blindado para datos con 2 pares de conductores sólidos trenzados. Puede ser para uso exterior o interior.

Tipo 2
Es un cable tipo 1 con 4 pares de conductores sólidos trenzados de calibre 24 AWG para uso en interiores. Contiene 4 cables para voz y 4 cables para datos.

Tipo 3
Es un cable UTP similar al utilizado en Ethernet. Originalmente fue especificado para voz, pero actualmente se ha cambiado la especificación para datos. Dado que es propenso a la interferencia, este tipo de cable requiere de un filtro que lo proteja.

Tipo 5
Este tipo de cable representa una fibra de 100/140 micrones, que es la especificación de fibra para Token Ring. Es utilizado principalmente para interconexiones entre MAUs.

Tipo 6
Es un cable blindado para datos de calibre 26 AWG, utilizado principalmente para interconexiones entre MAUs.

Tipo 8
Es un cable calibre 26 AWG con cubierta de plástico para ser usado principalmente bajo alfombras.

Tipo 9
Es un cable plano calibre 26 AWG con cubierta de Teflón, resistente al fuego, que se utiliza para cableados sin tubería.

1.1.6.3 Conectores del cable en Token Ring

La tarjeta controladora de Token Ring se conecta al cable principal mediante un cable conocido como lóbulo o *lobe*. Estos cables lobe son del tipo 1,2, o 3 y los cables de parcheo son del tipo 6. Las MAUs son interconectadas con cables de parcheo. Cualquiera que sea el cable, existen únicamente 4 conectores que pueden ser usados en Token Ring.
Hay 2 puntos de conexión en la red Token Ring: uno en la tarjeta controladora y la otra en el MAU. El conector DB-9 está localizado en la tarjeta controladora y permite la conexión

del cable al MAU. El conector DB-9 tiene una capa externa en forma de D y 9 pins dentro del mismo. Este conector soporta tanto UTP como STP.
El conector RJ-11 fue usado en un principio en redes Token Ring, con cable UTP y actualmente es muy raro su uso.
En el otro extremo del cable controlador, es decir del extremo del MAU se pueden usar dos tipos de conectores: el UDC o RJ-45. La mayoría de los concentradores usan el RJ-45.

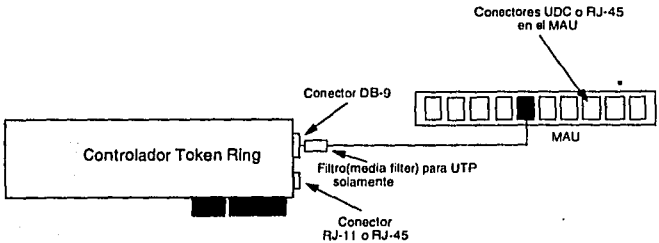


Figura 1.12. Conexión Física de una tarjeta controladora y un MAU.

1.1.6.4 Filtro para cable tipo 3

Este filtro es usado exclusivamente en cable UTP para Token Ring. Su propósito es filtrar señales no deseadas, consiste en una pequeña caja rectangular que suele ser parte misma del cable UTP localizado lo más cerca posible a la tarjeta controladora o directamente montada sobre la misma. El cable UTP no utiliza ningún blindaje y el ruido eléctrico puede penetrar fácilmente este cable. Cualquier señal que no se encuentre dentro de cierto rango será filtrada por este dispositivo.
El filtro puede ser un dispositivo por separado, colocado directamente sobre el conector DB-9, o ser parte integral del cable mismo o de la tarjeta controladora de Token Ring. Puede se usado en configuraciones de 16 a 4 Mbps de Token Ring.

1.1.6.5 Concentradores de Token Ring

El punto terminal del cableado en una red Token Ring es el concentrador de cableado, comúnmente llamado MAU. Existen gran variedad de concentradores dependiendo del proveedor o fabricante específico. Sin importar el tipo de MAU que se use, todos operan bajo el mismo principio.
En el modelo 8228 de IBM existen 10 puertos, de los cuales 8 se usan para conexiones de red. Los otros 2 son usados para conectar a otra MAU y son llamados *Ring In* (RI)y *Ring Out* (RO). Este tipo de MAU no requiere de alimentación externa, lo que significa que son pasivos.
IBM recomienda que para el par trenzado blindado (STP) sólo se conecten 260 dispositivos en el anillo.

Por ello hasta 33 MAU pueden ser interconectados a través de los puertos RI y RO. Cuatro puertos quedan vacíos. Para UTP únicamente 72 dispositivos pueden ser conectados en un solo anillo, por ello solo 9 MAUs pueden ser interconectados. Los MAUs modernos son realmente concentradores que van más allá de las especificaciones para UTP, permitiendo hasta 142 conexiones de UTP a un solo anillo.
El concentrador 8228 de IBM es un dispositivo no inteligente y no contiene la lógica necesaria para una administración de red. IBM presentó el modelo 8230 hace algunos años, parecido al del modelo 8228 en uno mismo, y puede conectar a otros MAUs por medio de cobre o repetidor de fibra. El 8230 se puede encontrar con conectores RJ-45. Este es un dispositivo inteligente que permite administración de red. Esta información permite conocer cuantos puertos de datos están activos, la existencia de problemas en algunos de los puertos, indicación de actividad de los puertos RI y RO (indicando una conexión a otra MAU).
Actualmente IBM está comercializando concentradores conocidos como 8250 y 8260 los cuales funcionan similarmente al concentrador Ethernet. Los módulos se conectan dentro del concentrador a medida que son necesarios, utilizando cable tipo 1, 2 o 3.

1.1.6.6 Conexión Múltiple de MAUs

Para más de 8 estaciones (utilizando el IBM 8228), un MAU debe estar concatenado con otro. Este el propósito de los puertos RI y RO. Estos puertos no se usan para conexiones de red, únicamente para la conexión de MAUs. El puerto RI conecta al RO de otro MAU.
Como se dijo anteriormente el cable STP puede manejar hasta 260 estaciones en un anillo, esto requiere la interconexión de 33 MAUs. Aún con tantos MAUs, el último deberá estar conectado de regreso al primero en el anillo.

1.1.6.7 Conexión del controlador al MAU

Los puertos de datos de los MAU se conectan a las tarjetas controladoras de red. Los cables que hacen esta interconexión son los llamados cables *lobe*, estos son del tipo 1, 2 o 3, con longitud máxima recomendada de 100 metros. Típicamente todo el cableado Token Ring termina en un sólo lugar. Estos cables son tendidos a través de paneles de parcheo que les permite separarlos en diferente anillos, estos anillos pueden entrelazarse mediante dispositivos conocidos como puentes o ruteadores.
Existe una regla específica cuando se tiende cable en este caso: UTP y STP no pueden ser usados al mismo tiempo en un anillo. El no hacer esto puede ocasionar problemas de comunicación.

1.1.6.8 Operación del MAU

Cuando una estación se conecta al puerto de datos del MAU, éste no lo incluye automáticamente al anillo. Existe un procedimiento de inicialización que deberá ocurrir antes de considerar a la estación activa dentro del anillo. Una parte de este procedimiento es la activación de un relevador en el MAU. La conexión al anillo es un proceso de 5 etapas que se explicarán a detalle cuando analicemos la capa de enlace de datos.
Al establecerse una conexión en la red el relevador se activa mediante un pequeño voltaje aplicado a través del cable lobe llamado corriente fantasma o *phantom current*, el cual se aplica en los pins de transmisión al MAU y de esta forma queda conectada la estación lógicamente al anillo activo.

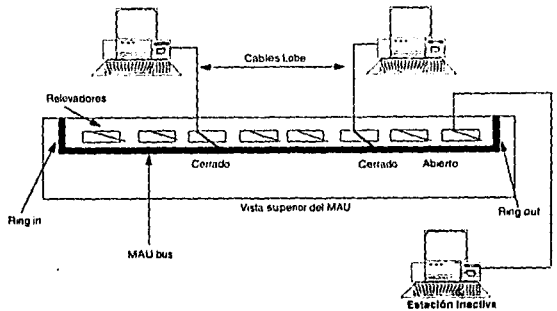


Figura 1.13. Operación del MAU.

1.1.6.9 Longitud del Anillo

Existe un concepto sencillo pero importante a su vez, relacionado a la activación o desactivación de las estaciones en el anillo, esto es la longitud del anillo mismo. Un MAU que tiene 3 de sus 8 puertos de datos conectados, la longitud del anillo será la suma de la longitud individual de los 3 cables lobe.

Por ejemplo, si cada cable es de 100 metros, la longitud del anillo es de 600 metros (100 metros de ida al controlador, 100 metros del regreso al MAU para cada una de las tres estaciones conectadas). Si una de ellas se desconecta, la longitud del anillo se reduce 200 metros. Esto es importante en términos de saturación, retrasos, etc. Entre más estaciones activas existan en el anillo, mayor es la longitud del mismo y por tanto los retrasos.

1.1.6.10 MAUs recientes.

Otros fabricantes se han desviado de los conceptos de diseño para MAU de IBM y han incorporado en un módulo de tarjeta al MAU con la capacidad de ser conectado a un concentrador. El concentrador de Token Ring es muy similar al de Ethernet.

Independientemente del fabricante, cada tarjeta del módulo ofrece 8 conexiones RJ-45. Varias tarjetas pueden ser configuradas en un sólo anillo utilizando un módulo de administración de redes ocupando una sola ranura. Esto quiere decir que si el chasis soporta 8 tarjetas 7 de ellas pueden ser configuradas en un anillo. Cualquiera de las tarjetas de un concentrador pueden separarse para formar múltiples anillos. Los anillos en el concentrador están separados, pero pueden conectarse a través de los puertos RI y RO. Los anillos independientes pueden comunicarse unos con otros utilizando puentes o ruteadores.

Estos concentradores soportan STP y UTP, utilizando conectores RJ-45 pero, los 2 tipos de cable no pueden mezclarse en el mismo anillo.

Las especificaciones de Token Ring permiten la conexión de 260 estaciones a un anillo usando el cableado más caro que es el STP, sin embargo éste no es un buen concepto de diseño. El número ideal de estaciones conectadas por anillo son de 100 a 150 estaciones, sin

importar el tipo de cable usado. Podemos concluir que el cable STP es caro y que si el cable tipo 3 o tipo 5 pueden ser usados en un concentrador que soporte de 130 a 150 estaciones por anillo, el cable tipo 3 será más que suficiente para la mayoría de las instalaciones, reduciendo el costo de éstas significativamente.

1.1.7 Anillo doble redundante (FDDI)

1.1.7.1 Antecedentes

Esta topología fue diseñada para redes que requieren de alta velocidad y consiste en dos anillos de transmisión en contrasentido. El anillo primario es utilizado como canal principal, si por alguna razón el anillo primario es interrumpido el secundario restablece la continuidad del primario en forma automática, actuando como redundancia o anillo de respaldo. Se utiliza como medio principal el cableado de fibra óptica y recientemente el cable UTP (unshielded twisted pair) y STP (shielded twisted pair).
Con esta topología se pueden alcanzar velocidades de 100 Mbps.

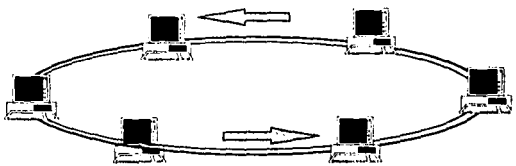


Figura 1.14. Anillo doble redundante de FDDI.

1.1.7.2 La Capa Física en FDDI

FDDI (Fiber Distributed Data Interface) es un medio de acceso establecido por la ANSI. FDDI es un método de acceso en anillo que utiliza un patrón especial llamado testigo, que circula continuamente en el anillo y que las estaciones lo utilizan para tener acceso al cable principal, la velocidad de éste es de 100 Mbps. Puede conectar hasta 500 estaciones en conexión doble en una red de 200 km. máximo. La diferencia de FDDI con otros métodos de acceso en anillo es el protocolo del testigo controlado por tiempo; esto es, cada estación de trabajo tiene un acceso a la red asegurado por un período de tiempo que es negociado entre todas las estaciones activas desde el inicio y cuando una nueva estación se une al anillo.
Las estaciones de FDDI pueden ser de 2 tipos: Estaciones de conexión doble (DAS) y estaciones de una sola conexión (SAS). Para permitir la simplificación de la conexión y mejorar la tolerancia a fallas del anillo, las estaciones pueden ser conectadas a un concentrador el cual es conectado al anillo mismo.
El cableado de FDDI está constituido por 2 anillos, uno transmitiendo en sentido de las manecillas del reloj y el otro en sentido contrario, así como se muestra en la figura 1.14, éstos también son llamados anillo primario y secundario. Aunque algunos datos pueden

viajar en los dos anillos, comúnmente viajan en uno sólo, hasta el momento en que ocurra una falla en un punto dado, en la que los anillos podrán unirse para formar uno sólo de gran longitud. Esto se conoce como *wraping*.

El tipo de conexión más usado en FDDI es fibra óptica. FDDI utiliza fibras multimodo, dado que los costos adicionales de las fibras monomodo no son necesarios, para el caso de redes que operan a 100 Mbps. Esta fibra también utiliza diodos emisores de luz (LED) en lugar de LÁSER, no solo por que es más económico, sino también porque la FDDI se puede utilizar también para conectar directamente las estaciones de trabajo de los usuarios. Existe, sin embargo, el peligro de que la curiosidad de algunos usuarios, pueda propiciar, en ocasiones la desconexión de los conectores de las fibras, para observar directamente el haz de luz, pudiendo causar severos daños físicos en la retina de los usuarios. Los LEDs son demasiado leves para causar un daño en el ojo pero son suficientemente potentes para realizar una buena transmisión de datos a velocidades de 100 Mbps. La especificación de diseño para FDDI no admite más de un error en 2.5×10^{10} bits

El uso de concentradores no es requerido pero es altamente recomendado, los cuales funcionan de manera similar a los que utilizan cable y que explicamos anteriormente para Ethernet y Token Ring. Las estaciones DAS como SAS pueden conectarse a un concentrador y poder ofrecer mayor eficiencia en el diseño de una red FDDI.

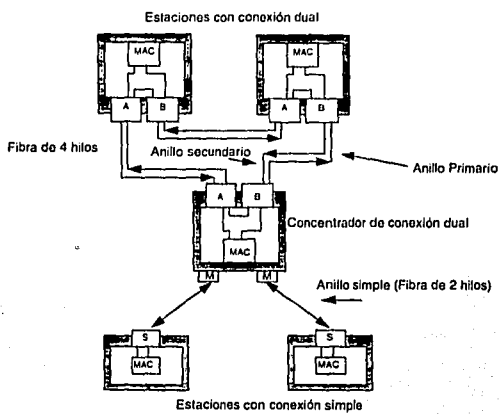


Figura 1.15. Conexión física de estaciones y concentradores en FDDI.

1.1.7.3 Comparación con el modelo OSI

FDDI opera en la capa física y de enlace de datos del modelo OSI. La capa física, se subdivide en dos capas más: La capa de protocolo físico (PHY) y la capa física dependiente del medio (PMD).

La PHY está especificada como la subcapa superior de la capa física. Es responsable de técnicas de codificación y decodificación de la señal, control de reloj y tramas de datos.

La subcapa PMD es responsable de la transmisión y recepción de niveles de voltaje, transmitir y recibir requerimientos de interface, niveles de error y especificaciones de cables y conectores. Comprende 4 normas:

1) Capa física dependiente del medio (PMD).
2) Capa física dependiente del medio para fibra monomodo (SMF-PMD).
3) Capa física dependiente del medio para fibra multimodo de bajo costo (LCF-PMD).
4) Capa física dependiente del medio para par trenzado (TP-PMD), también conocido como CDDI (Copper Distributed Data Interface).

En la capa de enlace de datos, FDDI es definido en la capa de MAC (Media Access Control). Esta se encuentra localizada en la subcapa inferior de la capa de enlace de datos. Es responsable del direccionamientos del enlace de datos (MAC address), acceso al medio, detección de errores y manejo del testigo.

La estación de administración (SMT) está definida en la capa física en la subcapa MAC de la capa de enlace de datos. Es responsable de los servicios de administración incluyendo administración de conexiones, configuración de nodos, recuperación de condiciones de error y la codificación de tramas SMT.

FDDI asume el uso de otro protocolo llamado IEEE 802.2, este protocolo está adoptado para funcionar en cada uno de los 4 protocolos normalizados para LAN. La IEEE 802.1 normalizado y adoptado también para protocolos de las 4 LAN. El más notorio de los protocolos 802.1 es el usado para puentes.

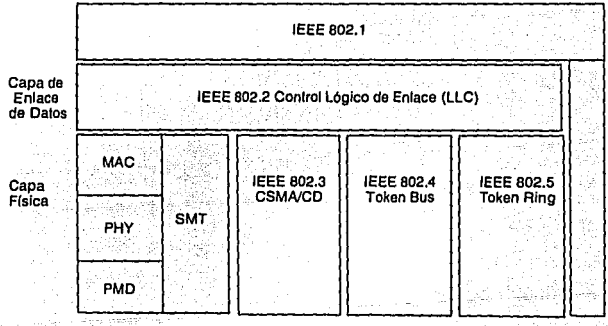


Figura 1.16. Comparación de las capas 1 y 2 del modelo OSI vs. IEEE.

1.1.7.4 Cableado para FDDI

Hay 3 partes fundamentales que componen un cable de fibra óptica: El núcleo, el revestimiento primario y la cubierta protectora. El núcleo es un cilindro de vidrio a través del cual viajan los rayos de luz. El revestimiento primario es un tubo de vidrio que recubre el anterior; su principal, propósito es el de reflejar cualquier rayo de luz, de nuevo hacia el interior del núcleo. La cubierta protectora está hecha de plástico y sirve para proteger el núcleo y el recubrimiento primario.

El núcleo y el revestimiento primario son conocidos generalmente por el tamaño de sus diámetros, siendo los más comunes, los de 50/100 micrones, 62.5/125 micrones y 100/200 micrones, en donde el primer número se refiere al diámetro del núcleo y el segundo al diámetro del revestimiento.

La luz se transmite en un extremo del cable y es recibido en el otro extremo. En esencia todas las conexiones vienen siendo punto a punto. Al cable que tiene la capacidad de manejar diferentes rayos de luz se le llama fibra multimodo (MMF). De aquí que cada modo es un rayo de luz. La fibra multimodo generalmente utiliza diodos como su fuente de luz, existiendo una gran atenuación en este tipo de fibra. La fibra monomodo (SMF) permite a un solo rayo de luz viajar a través de la fibra. Utiliza los LÁSER como fuente de luz y no tiene los grados de atenuación que la fibra multimodo. Su núcleo oscila entre los 8 y 10 micrones de diámetro y el revestimiento primario es de 125 micrones. Este último es más caro debido básicamente a la utilización de los LÁSER. Las estaciones pueden estar separadas hasta 2 km. utilizando fibra multimodo, mientras que con fibra monomodo la separación puede ser hasta de 20 km. El alambre de cobre ha sido aprobado para uso en FDDI adoptando el nombre de CDDI como dijimos anteriormente. La longitud máxima de este cable es de 100 metros con la restricción de que debe ser categoría 5 como lo fija la EIA.

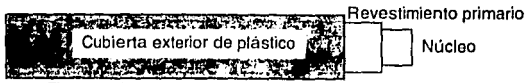


Figura 1.17 Estructura física de la fibra óptica tipo monomodo.

1.1.7.5 Conectores para cableado FDDI

FDDI permite el uso de varios tipos de conectores, sin embargo los más comunes son el conector de interface del medio (MIC) y el conector ST. El MIC es un conector rectangular, plano, utilizado para conexiones multimodo, contiene unas pequeñas partes de plástico que funcionan como una llave que permite la conexión correcta a los puertos. Existen 2 fibras en cada MIC, una para transmitir y otra para recibir.

Los conectores ST son comúnmente usados para conectar una fibra a un panel de parcheo de FDDI. La parte externa del conector es parecida al de un BNC, únicamente más pequeño. Estos conectores no tienen una llave que asegure su conexión por lo que hay que tomar las debidas precauciones. Pueden ser usados en estaciones con conexiones simples y su costo es mucho menor a los conectores MIC.

1.1.7.6 Tipos de puertos

Para evitar conexiones erróneas con otras topologías, FDDI identifica 4 tipos de puertos usados: A, B, M y S. Los puertos son los puntos de conexión en toda FDDI (concentradores, puentes, ruteadores).

Cualquier tipo de conexión podrá utilizar los tipos de puerto antes mencionados; las estaciones de conexión doble podrán tener puertos A y B, los concentradores tienen A, B, M o S como tipo de puerto, las SAS tienen únicamente un puerto tipo S. La norma FDDI también indica las interconexiones permitidas entre cada puerto. La red de FDDI utiliza un sistema de cableado estructurado interconectado formando una red por lo que es necesario asegurar que los tipos de puertos son conexiones legales o autorizadas.

En una operación normal FDDI es una red de 2 anillos. Una DAS tendrá 2 puertos: A y B. Una DAS que entra al anillo usa el puerto A para conectarse a la entrada del anillo primario y a la salida del anillo secundario. Una DAS puede ser una estación final o también un concentrador de conexión doble (DAC). El puerto B es lo contrario del puerto A. Se conecta a la salida del anillo primario y a la entrada del anillo secundario.

El puerto M conecta el puerto de un concentrador a un puerto del SAS, o del DAS, o de cualquier otro concentrador, (DAC o SAC).

El puerto S conecta un SAS o un SAC a un concentrador.

En la figura 1.18 se muestran las conexiones permitidas.

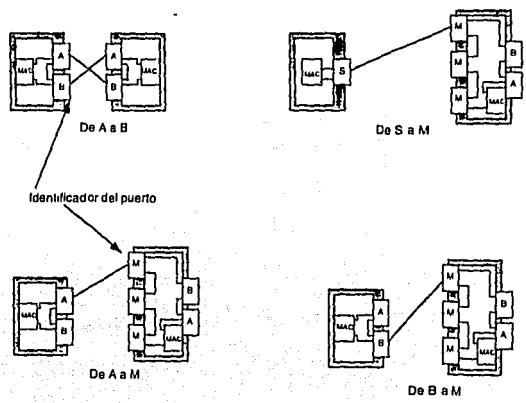


Figura 1.18a. Conexiones permitidas entre puertos en FDDI.

Al puerto / Del puerto	A	B	S	M
A	V, I	V	V, I	V, P
B	V	V,I	V, I	V, P
S	V,I	V,I	V	V
M	V	V	V	X

V= Válido
I = Indeseable
P= Indica una topología conocida como *dual homing*
x= Conexión inválida

Figura 1.18b. Conexiones permitidas entre puertos en FDDI.

1.1.7.7 Clases de estaciones para FDDI

Una estación es cualquier dispositivo que puede conectarse al anillo, a un concentrador, puente, ruteador o estación final de trabajo. FDDI tiene dos clases de estaciones: Estación con conexión doble (DAS: Dual Attachment Station) y la estación con conexión simple (SAS: Single Attachment Station). Una SAS es el medio más barato y sencillo de conexión a una red de FDDI. Tiene un puerto S y conecta al anillo FDDI a través del puerto M de un concentrador. Es un método costeable y confiable para conectarse a este tipo de red. Provee una sola conexión al anillo, sin embargo no está conectado al anillo redundante. Por ello, si una conexión SAS es deshabilitada se pierde el contacto con esa estación.

Las conexiones SAS se usan en estaciones de trabajo que pueden prenderse o apagarse periódicamente. Dado que el puerto S de la SAS es conectado al puerto M de un concentrador, se provee de aislamiento del resto de la red. Esto causará muy poco o ningún problema al anillo principal, dado que cuando un puerto SAS es inhabilitado, la topología no cambia.

La estación DAS se conecta tanto al anillo primario como al secundario en una red FDDI. Esta estación tiene dos puertos: A y B. El puerto A se conecta al puerto B de otra estación y el puerto B se conecta a un puerto A de otra estación. Es importante hacer notar que una estación DAS no requiere conectarse al anillo por medio de un concentrador; Es una conexión de función completa a anillo doble. En caso de una falla, la estación DAS puede envolver el anillo para aislar la falla. Las redes FDDI no deben ser diseñadas utilizando únicamente este tipo de conexiones, dado que puede dar complicaciones, por ejemplo, si existe una falla, el doble anillo puede segmentarse en anillos separados autónomos. La razón de la unión de los dos anillos es aislar los componentes dañados y restablecer el anillo aún cuando existan 2 o más anillos. Las DAS son más caras pero son más confiables que las SAS.

Una conexión diferente conocida como doble conexión *(dual homing)* permite a diferentes tipos de puerto ser conectados para que sean tolerantes a fallas. El puerto B de una DAS puede ser conectada al puerto M de un concentrador. Esto, aísla a la DAS del anillo doble y

permite al concentrador ignorar la DAS en caso de falla. Una estación DAS puede estar en doble conexión a un concentrador si su puerto A y B están siendo utilizados. Cada puerto está conectado a un puerto M pero en diferentes concentradores.

1.1.7.8 Concentradores para FDDI

Los concentradores para FDDI proveen muchos beneficios. Estos funcionan de manera similar a los usados en Ethernet y Token Ring, pero son mucho más avanzados tecnológicamente. Los concentradores para FDDI son repetidores que operan en la capa física, permitiendo a la red estar centralizada en un sólo punto. Es un dispositivo que provee múltiples puertos para la conexión de estaciones de trabajo al anillo. Permite la conexión de estaciones sencillas y dobles.
Los concentradores no necesariamente deben de formar parte de un anillo FDDI, pero permiten una mejor administración de la red, un mejor diseño de topología, y por tanto una mayor eficiencia.
El objetivo principal de un concentrador de este tipo es el de proveer un servicio de FDDI a los dispositivos que pueden encenderse o apagarse periódicamente, situación que causa disturbios en el anillo y ocasiona la segmentación de éste como se mencionó anteriormente. El concentrador aísla las estaciones de trabajo del doble anillo. Estos pueden conectarse en cascada para formar la topología FDDI más común que es la del doble anillo de árbol. Proveen la raíz de la topología de árbol.
Los concentradores pueden tener cualquiera de los 4 tipos de puertos. Por lo que existen 2 tipos de concentradores: Concentradores de doble conexión (DAC) y concentradores de conexión simple (SAC) y/o una combinación de ambos. Los DACs se conectan al anillo como un dispositivo de anillo doble, mediante los puertos A y B, además de ofrecer múltiples conexiones para estaciones SAS, mediante sus puertos M. Los DACs no poseen puertos S y no requieren conexión al anillo doble para activarse. Una red FDDI puede ser tan sencilla como tener conexiones SAS conectadas a un concentrador DAC único y aislado.
Los SACs se conectan al anillo como dispositivos de conexión simple y no pueden conectarse al anillo doble, excepto a través de un DAC. Un SAC tendrá un puerto S para conectarse a otro concentrador mediante el puerto M de éste, y provee múltiples conexiones SAS a través de sus puertos M. Los SAC no tienen necesidad de conectarse en su puerto S para operar, pueden proveer conectividad FDDI a estaciones SAS como un concentrador único y aislado.

1.1.7.9 Funciones de los Concentradores para FDDI

Los concentradores realizan dos funciones primordiales: Desconectar las estaciones inactivas y conectar y dar de alta las estaciones activas. Un puerto cerrado de un concentrador es aquel que tiene inactiva la estación conectada a él. Ningún dato saldrá de esta estación. El puerto es cerrado cuando ocurre alguna o algunas de las siguientes situaciones: Que se apague la estación, que el administrador de red la cierre por exceso de errores, u otro administrador de red haya solicitado su cierre. Esto por lo general no afecta la operación normal del anillo.

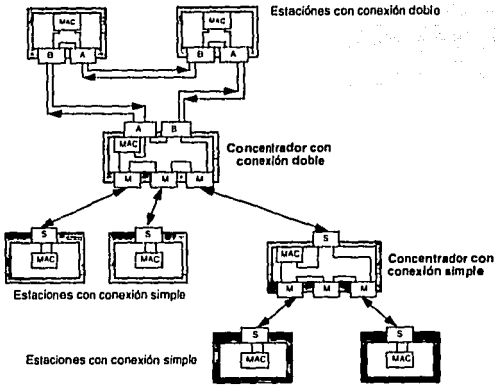


Figura 1.19. Conexión entre concentradores FDDI.

La inclusión de un puerto al anillo es el proceso mediante el cual la conexión a la red y el puerto de su concentrador tienen una buena conexión física y el puerto del concentrador inserta la conexión al puerto FDDI.
El proceso de inserción causa un ligero disturbio momentáneo, pero el anillo se corrige a sí mismo rápidamente, regresando a su operación normal. Esto se logra en un período muy corto de tiempo.

1.1.7.10 Operación de la capa física en FDDI

Las estaciones de FDDI son conectadas a la red en forma punto a punto, conexiones físicas bidireccionales formadas entre la capa física de 2 estaciones conectadas por su cable FDDI. Cada conexión a la red tiene la habilidad de transmitir y de recibir. Una conexión física sencilla, tiene 2 fibras. Una conexión doble tiene 4 fibras. Esto permite la conexión a cada anillo.
La fibra de transmisión de una estación es conectado a la fibra de recepción de otra y así sucesivamente.
En un ambiente de anillo doble, los datos fluyen en sentidos opuestos de cada anillo. Esto no es común ya que requiere de equipo más caro para permitirlo. En la mayoría de los casos los datos fluyen únicamente sobre el anillo primario. El anillo secundario es usado como respaldo. En caso de falla el anillo primario y secundario se unen para formar uno solo y aislar la falla.

1.1.7.11 Rupturas del anillo o de las estaciones en FDDI

Existen varias condiciones que pueden ocasionar que un anillo se colapse, esto es, que el anillo primario se enlace con el secundario para formar uno sólo. Del dispositivo que se

inhabilite dependerá la manera en que los anillos se enlacen. Un anillo FDDI continua enlazándose hasta aislar la falla. Por ejemplo, en una red que tiene 5 conexiones dobles, como el que se muestra en la figura 1.20, los datos fluyen en sentido a las manecillas del reloj. Si existe una falla en la fibra entre las estaciones B y C, se enlazarán entre la estación B hacia A y en la C hacia D. Esto generará una topología de anillo sencillo, y permitirá a la red continuar su operación normal. La administración de red tiene la capacidad de indicar los enlaces realizados y definirá la estación inhabilitada, esto permitiendo la reparación física del cable de ser necesario. Una vez reparada y dada de alta la estación, el anillo automáticamente regresará a la topología original de anillo doble.
En el caso de que una estación de conexión doble esté deshabilitada también el anillo se enlazará para aislarlo. Si la estación B se deshabilitara, las estaciones A y C se enlazarían nuevamente. La estación A enlazaría el anillo con la estación E y la estación C haría lo mismo con la estación D. Si la estación B tiene capacidad de aislarse a través de un conmutador óptico de paso, los anillos puede ser que no se enlacen. La señal sería reflejada a la estación A, como si la estación B estuviera activa. Si la distancia entre la estación C y la A fuera mayor a 2 km., la señal se debilitaría y la estación A no sería capaz de recibir la señal como válida. La estación pierde conectividad con la estación B y los anillos se enlazan.
En otro caso, la estación B y la estación D se inhabilitan, la estación A se enlaza con la estación E y la estación C se verá aislada. Si la fibra se rompiera entre las estaciones A y B y entre E y D, la estación A se enlaza con la E y B, C y D se enlazarían unas con otras. Esto provee dos anillos de conexión doble. Algo tan simple como el encendido de un puerto DAS puede causar un disturbio. Esta es la razón por lo que las estaciones que se conectan a un anillo doble deben ser dispositivos estables. Todos los demás dispositivos que se conecten a una topología FDDI deberán hacerlo a través de un concentrador.

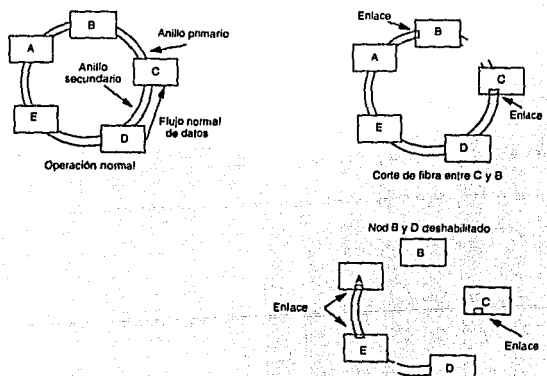


Figura 1.20 Ruptura del Anillo de FDDI.

1.1.8 La capa de enlace de datos para Ethernet, Token Ring y FDDI

La segunda capa del modelo OSI es la capa de enlace de datos. Ésta es la responsable del direccionamiento físico, el manejo de tramas y que la corrección de errores sea adicionada a los datos que son enviados hacia ella por la capa superior de protocolos del modelo OSI. Esta pasará los datos, ahora llamados paquetes, a la capa física para que sean transmitidos a la red.

Un método de acceso es un conjunto de procedimientos o reglas, (un algoritmo) que define, un método de como accesar a la LAN. Como su nombre lo indica es un simple método que determina el acceso. Los datos tienen que se enviados y recibidos en forma confiable.

Los datos viajan hacia y desde las estaciones de la red, pero el método de acceso no se encarga de esto, es sólo un vehículo para hacer uso de un canal de comunicaciones dado y permitir que los datos sean transmitidos y recibidos.

1.1.8.1 Paquetes de datos

Las estaciones se pueden comunicar sólo a través del uso de paquetes. Hay muchos tipos diferentes de paquetes, dependiendo del método de acceso (Ethernet, Token Ring, FDDI) y los programas de protocolos (TCP/IP, IPX, etc.), que pueden ser usados. Pero hay un formato general que puede ser usado para mostrar como está compuesto un paquete.

Cada paquete tiene definido un encabezado, una parte de datos o información de control y un terminador del paquete. Los encabezados y terminadores de la red contienen información que es usada solamente por los componentes de la red, los cuales proveen información al software y hardware de la red sobre como procesar el paquete.

La comunicación en una red ocurre cuando las estaciones envían y reciben datos. Estos datos pueden ser del usuario o algún tipo de comando o mensaje de respuesta indicando una acción que es necesaria ejecutar, como abrir, crear, escribir o cerrar un archivo. Simplemente la lectura de información del disco duro de una estación remota y transmitirlo a la red no es suficiente; los datos deben ser formateados para transmisión en la red. La transferencia de información entre las estaciones se termina cuando la estación fuente empaca los datos para transmisión sobre la red. El paquete contiene los datos para la estación remota; cada tipo de red, Ethernet, Token Ring o FDDI formatean su información de modo diferente. El formateo de los datos se llama encapsulado de datos.

Un paquete es una unidad de información que una estación direcciona a una o más estaciones de la red para hacerle llegar datos o información de control.

1.1.8.2 Direccionamiento de la capa MAC

Las LAN fueron diseñadas para ser independientes al protocolo y por esto cada conexión a la LAN tiene una dirección única llamada control de acceso al medio o dirección MAC. Es llamada así porque está en la subcapa de control de acceso al medio de la capa de enlace de datos, donde es definida su dirección.

En Ethernet, Token Ring o FDDI cada conexión a la red tiene una dirección única que es de 48 bits (6 bytes) de longitud. Las direcciones de 6 bytes son la norma para Ethernet/IEEE 802.3, Token Ring y FDDI. Al principio de cada paquete se contendrán las direcciones físicas conocidas como direcciones de origen y destino. La dirección origen es la de la estación que transmite el paquete y la dirección destino es la de la estación que deberá recibir el paquete.

Hay tres tipos de direcciones en una LAN: única, múltiple o general.
Una dirección única es aquella que no está duplicada por otra estación en la red.
Una dirección múltiple es aquella que está dirigida a un grupo de estaciones conectadas a una red, que han sido programadas para aceptar esa dirección.
Una dirección general, es una forma de dirección múltiple, que está dirigida a todas las estaciones de la red. Esta generalmente está compuesta por unos (en binario) en la dirección destino. Cuando un paquete tiene una dirección general, todas las estaciones de la red reciben y procesan el paquete, salvo aquellas separadas por un ruteador.
Las LAN reciben todos los paquetes que son puestos en la red, pero analizan la dirección destino con la suya propia y de esta manera solo aceptan y procesan los que concuerden con su propia dirección.

1.1.8.3 Definición de los campos de dirección

La dirección puede ser cualquier combinación de números hexadecimales, con la única condición de que no estén repetidos en ningún otro nodo de la red. Las direcciones únicas están garantizadas por la IEEE. La dirección de 6 bytes está dividida en dos campos de 3 bytes cada uno. Los 3 primeros bytes son asignados por la IEEE a un sólo fabricante de equipo para LAN, de tal forma que cada fabricante tiene una codificación propia y es diferente de las demás. Los 3 siguientes bytes son utilizados por los fabricantes para identificar cada uno de sus controladores de tal forma que pueden fabricar hasta 2^{24} controladores.

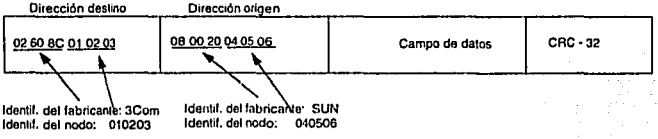


Figura 1.21. Campos de dirección.

1.1.8.4 Formato de los paquetes en Ethernet y el IEEE 802.3

En Ethernet se utilizan dos formatos diferentes para los paquetes:
El formato Ethernet y el formato IEEE 802.3

1.1.8.4.1 El preámbulo en Ethernet

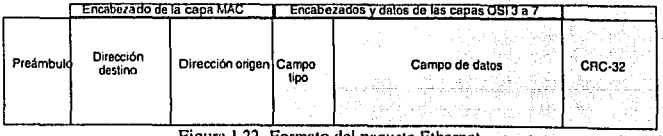


Figura 1.22. Formato del paquete Ethernet.

El principio de una trama Ethernet contiene el preámbulo. Para que los datos en una red Ethernet puedan ser transmitidos y recibidos, la señal debe ser sincronizada. Un mecanismo de reloj se encarga de hacer esta sincronización de bits en la trama. Esto permite la diferenciación entre el bit 0 y bit 1. Las señal de reloj esta contenida en la señal de datos.
Cada estación que transmite en la red un paquete debe proveer su propio reloj para el paquete. La frecuencia de reloj para Ethernet es de 20 Mhz., la cual combinada con los datos, alcanza una velocidad de transmisión de 10 Mbps. Dado que no hay un reloj maestro en una LAN Ethernet, la señal de reloj en el controlador de Ethernet es generada por un circuito en el transceptor. Puede haber una pequeña desviación de la señal de reloj de una tarjeta controladora a otra, y debe haber un mecanismo para que todos los controladores Ethernet puedan sincronizar su receptor lógico a ese reloj de la estación transmisora. Así pues el preámbulo es una transmisión de 64 bits para asegurar que todos los concentradores Ethernet sincronicen sus receptores lógicos con el reloj del paquete que esta llegando.

1.1.8.4.2 El orden de los bit y transmisión para Ethernet e IEEE 802.3

Un paquete es transmitido en una secuencia de bit por bit hasta que todos los bit en el paquete han sido transmitidos. El primer bit transmitido es el bit de transmisión múltiple (M), el cual indica si el paquete tiene una dirección única o múltiple. Si este bit es 1 (binario) es un paquete que esta destinado para un grupo de estaciones en la red. Si el bit es 0 (binario) el paquete esta destinado a una sola estación en la red.

1.1.8.4.3 El formato del paquete Ethernet

El paquete Ethernet es donde la capa superior de software pone sus datos para ser transmitidos en la red. El formato MAC de la trama Ethernet contiene 5 campos:
1.- la dirección destino,
2.- la dirección origen,
3.- el campo tipo,
4.- el campo de datos, y
5.- el chequeo de redundancia cíclica (CRC).
Las direcciones de origen y destino ya fueron explicadas anteriormente. El campo de tipo, con una longitud de 2 bytes, identifica el protocolo de la red que envió el paquete. Hay muchos protocolos de red que pueden correr en una LAN. Si el sistema cliente servidor de Novell NetWare esta siendo usado en una red, el campo tipo contendrá un número único que identifica al propietario del paquete como Novell NetWare. Si el paquete es originado por el protocolo de control de transmisión/ protocolo Internet (TCP/IP), entonces otro número único estaría en este campo. La estación que recibe el paquete tendría que estar corriendo también TCP/IP para poder recibir un paquete TCP/IP. Este paquete sólo será recibido por un protocolo similar en el lado del receptor. En otras palabras, un paquete NetWare no puede ser recibido por una estación que esta corriendo en protocolo TCP/IP. El campo tipo fue originalmente controlado por Xerox, pero posteriormente fue asignado a la IEEE. Cada protocolo es asignado como un número único.
El CRC es un campo de 4 bytes que es usado para garantizar una confiabilidad del paquete del 99.999%. El CRC no es un mecanismo de corrección de errores, solamente es un mecanismo de detección de errores. En Ethernet es el responsable de que los protocolos de

capas superiores identifiquen un paquete erróneo. El controlador de Ethernet puede descartar un paquete sin notificar a la estación que lo envía.
Cuando un paquete es transmitido, un CRC es generado para el paquete completo, incluyendo las direcciones. Cuando el paquete es recibido, el controlador del receptor generará también el CRC para el paquete que esta llegando. Este comparará su CRC con el CRC del paquete recibido, y si los dos no coinciden, el paquete es descartado.

1.1.8.4.4 Formato del paquete de la IEEE 802.3

Ethernet y la IEEE 802.3 siguen el mismo algoritmo de medio de acceso. Las diferencias entre los dos es el formato de los paquetes; ambas normas coexisten sin mayor problema en el mismo cable.
Al principio del paquete está el preámbulo y el delimitador de inicio de la trama (SFD). La IEEE divide el preámbulo de Ethernet de 8 bytes en un preámbulo de 7 bytes y un byte de SFD. Hay otras 2 diferencias en esta trama en la que el bit de dirección múltiple se cambió por bit Individual/Grupal (I/G). Este bit está en el mismo lugar que el bit M para Ethernet pero es ahora llamado dirección individual o grupal. El segundo bit está ahora reservado y es llamado dirección universalmente o localmente administrada, el bit (U/L). Si este bit es cero, la dirección es asignada por la IEEE; si el bit es 1, la dirección es generada localmente.
La IEEE decidió que se permitirían las direcciones localmente administradas. Esto significa que las direcciones en la PROM de la tarjeta pudieran sobreescribirse por otra dirección asignada por el administrador de la red.

1.1.8.4.5 Operación normal de Ethernet

Cuando una estación intenta transmitir un paquete al cable principal, la estación monitorea al cable principal para asegurarse que ninguna otra estación está transmitiendo. Si se encuentra en silencio, esto es, que nadie está transmitiendo, el controlador inmediatamente empieza a transmitir el paquete al cable. Durante la transmisión, el controlador monitorea al cable para asegurarse que ninguna otra estación está intentando transmitir al mismo tiempo. Si los 64 bytes son transmitidos sin incidente, el controlador ha pasado satisfactoriamente la ventana de colisión, la cual es el número de bytes que se requieren para ser transmitidos a 10 Mbps para viajar 2500 metros, que es la longitud máxima del cable para Ethernet. Esto aseguraría que cualquier estación sea capaz de detectar que el cable está siendo usado por otra estación. Cualquier estación que desee transmitir y detecte a otra estación transmitiendo en ese momento, detendrá la transmisión hasta que el cable este en silencio otra vez. Una vez que el cable esté libre, se le permite transmitir a otra estación. Si no hubo colisión durante la transmisión, ésta es considerada satisfactoria.
No se usa un esquema de prioridades en Ethernet. Todas las estaciones tienen la misma oportunidad de transmitir. Bajo ciertas condiciones, 2 o más estaciones intentarán apoderarse del cable al mismo tiempo y Ethernet tiene un método para manejar la situación, que es la detección de colisiones, la cual será explicado a continuación.

El paquete más largo que está permitido transmitir en una estación Ethernet es de 1,518 bytes. El paquete de menor tamaño es de 64 bytes. Cualquier paquete menor de 64 bytes o más grande de 1,518 bytes es ilegal.

1.1.8.4.6 Detección de Colisiones Ethernet

Cuando un controlador Ethernet empieza a transmitir, hay un pequeño período de tiempo durante el cual otras estaciones no pueden detectar la primera transmisión y empezar a transmitir también. Como solo a una estación se le permite transmitir al cable al mismo tiempo, dos o más transmisiones se interferirán entre si. A la transmisión de dos o más estaciones al mismo tiempo, se le conoce como colisión.
Las colisiones son inherentes al diseño de Ethernet. No son errores graves y la mayoría de las veces no causarán que la red falle. La red se recupera de este error con un algoritmo de detección de colisión. Sin embargo si más del 0.5 % de las transmisiones en Ethernet son colisiones, las red debe ser monitoreada muy de cerca. Si las colisiones son excesivas es indicador de que algo anormal está sucediendo en la red.

1.1.8.4.7 Definición de Acceso Múltiple por Detección de Portadora y Detección de Errores

Cuando una estación desea transmitir, escuchará para determinar si alguien más está actualmente transmitiendo. Si hay otra transmisión en el cable en ese momento, el controlador entrará en modo de espera por un período de tiempo especificado, por lo menos de 9.6 microsegundos, antes de intentar transmitir nuevamente. Esto es conocido como detección de portadora.
En un sistema Ethernet puede haber hasta 1024 estaciones (incluyendo repetidores) conectadas a un sólo segmento. Esto es conocido como acceso múltiple. Si el controlador ha detectado que el segmento está libre, inmediatamente inicia la transmisión y continua escuchando. Si al final de la transmisión no ha habido errores, la transmisión se considera hecha.

1.1.8.4.8 Concepciones equivocadas de Ethernet.

Aunque Ethernet corre a 10 Mbps, esto no quiere decir que es menos eficiente que Token Ring a 16 Mbps. Token Ring es mejor bajo ciertos ambientes como redes muy congestionadas, manejo de imágenes y gráficas, y Ethernet es mejor bajo otras como tráfico con picos de demanda muy altos.
Ethernet puede transmitir y recibir a 10 Mbps, pero hay otros factores que afectan esta velocidad, como son: la velocidad de transmisión de la máquina, la velocidad del disco duro, el protocolo usado, etcétera. La velocidad de transmisión de 10 Mbps es solamente en la capa física.
El tamaño de los paquetes en Ethernet no afectan el desempeño de la red, paquetes de 64 bytes no permiten mejor utilización del ancho de banda. Lo que hacen es permitir que más estaciones puedan accesar a la red, ya que las estaciones transmiten más rápidamente sus paquetes y dejan que otras esperen menos tiempo para iniciar su transmisión. Sin embargo se requerirán más transmisiones para mover los datos de un lado a otro.

La topología de un sistema Ethernet afecta directamente al desempeño. Una red diseñada pobremente causa muchos retardos en la transmisión y recepción de los paquetes, por lo tanto es el aspecto más crítico de la implementación de la red.

1.1.8.4.9 Fast Ethernet

Las nuevas aplicaciones de escritorio coinciden en que son intensamente demandantes de gráficos y con gran consumo de ancho de banda, esto sumado al gran incremento en el poder de procesamiento de las PCs, aplicaciones multimedia, aplicaciones de diseño y administración de base de datos, demandan una red con mayor ancho de banda. El tamaño de los archivos es mayor, las redes se están distribuyendo más, y hasta el entretenimiento están incrementando la congestión de las redes.
Para atender esta necesidad surge Fast Ethernet la cual se basa en una mejora a la velocidad de Ethernet para alcanzar los 100 Mbps.

1.1.8.4.10 Fast Ethernet 100BASEVG

A principios de 1994 el IEEE anunciaría el borrador de propuesta de la norma que ha denominado 802.12 para 100BASEVG con el que se piensa accesar velocidades de transmisión de 100 Mbps para tráfico de datos sobre cable de par trenzado. Este es un caso único para la historia de los procesos de normalización, originalmente desarrollado por las compañías AT&T y H.P. y todo apuntaba que sería una norma propietaria. Pero el IEEE resolvió convertirlo en norma junto con el Fast Ethernet de 100 Mbps sobre CSMA/CD, el cual fue ideado por Synoptics y 3COM. De esta manera nos encontramos con dos normas diferentes para soluciones similares. 100BASEVG tiene incorporados mecanismos que responden a condiciones de tráfico intenso, para aprovechar mejor el ancho de banda asignando prioridades en el acceso al medio (algo similar se tuvo proyectado para el Token Ring tradicional).
Este mecanismo de prioridades es conocido como protocolo de prioridad por demanda (PD). El mecanismo se basa en un controlador inteligente que detectará aquellas tramas con mayores prioridades asignadas para permitirles el tránsito por el medio, y así colocar en una lista de espera a las otras tramas que arriben al concentrador. Con PD, 100BASEVG posee retardos del orden de los 121 microsegundos, como mínimo. El retraso se incrementa en 120 microsegundos por cada trama que arribe con igual prioridad. A pesar de tal incremento es posible utilizar 100BASEVG para aplicaciones de multimedia.

1.1.8.4.11 Fast Ethernet 100BASE-T

Aprobado por el IEEE se convertirá en un anexo del 802.3. Todavía no está ratificado y el primer borrador fue anunciado a principios de 1994.
Fast Ethernet sobre CSMDA/CD es la única norma para redes LAN de alta velocidad que no provee mecanismos de prioridad como Token Ring o 100BASEVG o de multiplexaje del medio de transmisión como FDDI/II, para responder a situaciones de tráfico intenso.
Esto es porque sigue conservando el mismo esquema de acceso al medio, es decir el CSMA/CD, en el cual se compite para tener acceso al medio como lo hace la 802.3 tradicional que no distingue los diferentes tipos de tráfico.
Se espera que esta norma tenga retraso del orden de los 30 milisegundos, comparado con el 802.3 convencional cuyo retraso puede llegar a medirse en minutos.

1.1.8.4.12 Alternativas de cableado para Fast Ethernet

Nombre	Norma	Cable UTP
100BASE-TX	IEEE 802.3	Categoría 5, 2 pares
100BASE-T4	IEEE 802.3	Categoría 3/4/5, 4 pares
100VG-AnyLAN	IEEE 802.12	Categoría 3/4/5, 4 pares o Categoría 5, 2 pares

Figura 1.23. Cableado UTP para Fast Ethernet.

1.1.8.5 La capa de enlace de datos en Token Ring

1.1.8.5.1 Antecedentes

Token Ring es un método de acceso en el cual las conexiones en una topología de estrella física ganan el acceso al segmento. El derecho para transmisión se da al convertir un testigo (token) en una trama de datos. El testigo es un patrón específico de 24 bits que circula constantemente en el anillo permitiendo el acceso a las estaciones que desean transmitir. Existe un sólo testigo en cualquier anillo.

Una estación que necesita transmitir espera el arribo del testigo. Cuando este llega, y no está reservado para otra estación, se convierte en un paquete de datos. La estación coloca la información en este paquete y lo envía al anillo. Cuando la estación de trabajo termina la transmisión, ésta espera el regreso de la trama antes de liberar el testigo (esto es exclusivo únicamente para anillos de 4 Mbps de velocidad).

Token Ring es un medio de transmisión en el que todas las estaciones pueden ver lo que ocurre en el anillo. Para poder recibir los datos correctamente, un controlador Token Ring compara la dirección destino en el paquete recibido con su propia dirección (dirección de MAC), si coinciden, el controlador copia la trama y la repite de regreso al anillo. De igual modo cambia algunos bits en el paquete para indicarle a la estación fuente que la dirección fue reconocida y se pudo copiar todo el paquete.

Cuando la trama llega de regreso a la estación fuente, ésta toma el paquete del anillo y regresa el testigo nuevamente al anillo. Con el testigo liberado, otra estación puede seguir el mismo procedimiento.

El Token Ring original corría a 4 Mbps; en 1989, fue mejorado a 16 Mbps. La norma de Token Ring no especifica ni velocidad ni longitud de la trama. Sí especifica el tiempo en el que una estación puede mantener el testigo (10 milisegundos).

1.1.8.5.2 El proceso de conexión en Token Ring

La operación de Token Ring es muy compleja en relación con Ethernet. El formato de la trama es muy compleja, así como la operación del anillo y el controlador mismo.

1.1.8.5.3 Operación del controlador

Existen muchos tipos de tarjetas controladoras para Token Ring, cada una de ellas posee un circuito integrado que controla el método de acceso. El protocolo del anillo es cargado en las PROM de la tarjeta controladora. Esto asegura que todos los controladores operen de la misma manera en el anillo.

La administración de Token Ring es bastante estructurada. Comienza cuando el controlador se inicializa. Antes de que la tarjeta controladora pueda convertirse en participante activo en el anillo, existen 5 fases de procedimientos de inicialización que debe seguir la tarjeta controladora antes de poder ser considerado participante activo del anillo. Cualquier error durante este procedimiento, retirará la tarjeta controladora del anillo.

Fase 0 es la prueba del lobe que se obtiene antes de que el controlador se conecte lógicamente al anillo. El lobe es una sección de cable que conecta el controlador al MAU. La prueba consiste en enviar una serie de tramas MAC especialmente formateadas, entre el controlador y el MAU. El relevador dentro del MAU no ha sido cerrado; por ello, el controlador no está activo en el anillo en este momento. Las tramas son transmitidas al MAU, quien las regresa inmediatamente al controlador. Si estas tramas regresan sin error, se validará el receptor lógico del controlador mediante la transmisión de tramas de prueba MAC de direcciones duplicadas. Si estas tramas son recibidas sin error, el controlador se conecta al anillo activando el relevador en el MAU, y procede a la fase 1. De otra manera las pruebas son deshabilitadas y el error es reportado.

Fase 1 es una validación del monitor. Este es el proceso por el cual el controlador espera a que pasen ciertas tramas MAC como el monitor activo presente, monitor en espera presente, o purga del anillo. Si recibe cualquiera de las tramas anteriores procederá a la fase 2. Si el controlador no ve estas tramas, asumirá que es la primera estación en el anillo, que no existe un monitor activo presente o que la inserción a deshabilitado el anillo. El controlador realiza la función de reclamo de testigo. Si es la primera estación en el anillo, se convertirá en el monitor activo.

Fase 2 es la validación de tramas de dirección MAC duplicadas, esto es para asegurarse que otras estaciones no tengan la misma dirección MAC. Dado que los controladores de Token Ring poseen la habilidad de asignar sus propias direcciones a través del administrador de la red, el controlador genera tramas de direcciones duplicadas durante esta fase para asegurarse que su dirección MAC no esté siendo usada en la red. Si una dirección duplicada es encontrada el controlador se retira del anillo.

Fase 3 es la notificación del vecino. La cual ocurre cuando una estación de la red encuentra la dirección de la tarjeta controladora de la estación anterior más próxima a ella. Este concepto se define como vecino activo anterior más cercano (NAUN). Esto también le permite a la tarjeta controladora identificarse ella misma con su vecino posterior.

Fase 4 es la fase de solicitud de inicialización. Esta es la solicitud del controlador para cambiar parámetros operacionales de una zona especial del anillo conocida como *servidor de parámetros del anillo*.

Si cualquiera de esta información es incorrecta o amenaza la integridad del anillo, o si muchas estaciones están ya conectadas al anillo, el servidor de parámetros del anillo notificará al administrador de la red para que solicite el retiro de una estación del anillo.

Si el controlador aprueba todas las fases, se convertirá en miembro participante activo del anillo.

1.1.8.5.4 Formato de las tramas IEEE 802.5

Hay diferentes tipos de tramas que pueden ser transmitidos. Su formato es muy diferente al de Ethernet.

Las direcciones origen y destino son de 6 bytes de longitud, igual que en Ethernet, las tramas usan el bit I/G para indicar si la trama está direccionada a un grupo de estaciones o a una sola, así mismo utiliza el bit U/L para indicar si la trama está direccionada por la IEEE o está localmente asignada.
En el nivel de enlace de datos existe una importante diferencia entre la trama de Ethernet y Token Ring y esta es el orden de la transmisión de los bits. Las tramas tanto de Ethernet como del IEEE 802.5 siempre transmiten primero el bit cero. La diferencia es que el bit cero es el bit más a la derecha en un byte de Ethernet y será el bit más a la izquierda en la IEEE 802.5. Esto es muy importante cuando se están intercambiando paquetes entre Token Ring y Ethernet.

1.1.8.5.5 Las Tramas de Token Ring

Existen 4 tipos de tramas que pueden circular por el anillo de Token Ring. Estas son: la del control lógico de enlace (LLC), la del control de acceso al medio (MAC), la de testigo y la de trama rechazo.
La LLC es usada por los controladores para distribuir el uso de datos.
La MAC es usada por los controladores para fines de ordenación interna. Ésta ayuda a mantener la operación adecuada del anillo y no es usada para llevar consigo datos de usuario. Es una trama local que se queda en el anillo en el que fue transmitido, por lo que no puede ser llevado más allá de puentes y ruteadores.
La trama de testigo está compuesta por 3 bytes, conocida como testigo. Esta trama continuamente está dando vueltas en el anillo, esperando la señal del controlador que requiere una transmisión. Si un controlador necesita transmitir, deberá esperar el testigo. Si la trama del testigo llega al controlador, éste convierte al testigo y salvo algunas excepciones, comienza a transmitir sus datos. La tarjeta del controlador cambia un bit en la trama del testigo y lo convierte en un encabezado inicial de datos. El controlador entonces agrega las direcciones de origen y destino a la trama de datos y lo transmite al anillo. Una vez que los datos han sido transmitidos, el controlador espera que regrese la transmisión y libera el testigo. Con Token Ring, existirá únicamente que atraviese todo el anillo.
La trama de rechazo es usada por el controlador para indicar que trama debe ser ignorada. Puede ser transmitida debido a un error interno en el controlador que no es lo suficientemente severo como para forzar al controlador a salirse del anillo. Después de la transmisión de la trama de rechazo, el controlador continúa participando en el anillo.

1.1.8.5.6 Definición de los campos de las tramas en Token Ring

1.- El Delimitador de Inicio (SD) es el primer byte de una trama. Indica a un controlador que una trama está a punto de llegar (Testigo, MAC o LLC).
El delimitador de inicio son 8 bits usados para sincronizar la transmisión del testigo o la trama.
El delimitador inicial utiliza una violación a la codificación Manchester diferencial que significa el comienzo de una trama. El formato es el siguiente: JK0JK000. En donde J y K son bits conocidos como bits de violación de fase y serán reconocidos por la tarjeta controladora como bits de no-datos y serán reconocidos únicamente como símbolos J y K.

2.- El Control de Acceso (AC) indica si la trama en un testigo o una trama de datos. Este byte contiene bits de reservación y prioridad que permiten a la estación acceso a la captura del testigo o no. También contiene un bit de monitor.
El campo de control de acceso contiene 8 bits con el siguiente formato: PPPTMRRR

PPP = bits de prioridad e indica la prioridad del testigo o trama en el anillo.
T = bit de testigo. Está fijado en 0 para testigo y fijado a 1 para tramas.
M = bit de monitor y es fijado por el monitor activo para mantener un testigo o una trama circulando continuamente en el anillo. El monitor activo cancela cualquier trama que tenga el bit M fijado a 1 porque este bit indicaría que es una trama huérfana.
RRR = bits de reservación e indican la prioridad de reservación fijada para el testigo. El bit de prioridad determina cual estación tiene acceso al testigo, cuando éste se encuentre disponible.

3.- El campo de Control de las Tramas indica si una trama es LLC o MAC. Las tramas LLC generalmente contienen datos del usuario, pero las tramas MAC tienen funciones especiales en el anillo que no tienen que ver nada con los datos de usuario, reportan errores y permiten mantener el anillo.
El campo de control de las tramas está compuesto por un byte de información. Es utilizado para indicar el tipo de trama y la información MAC. Tiene el siguiente formato FFrrZZZZ en donde:

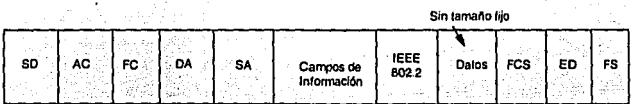
FF = Tipo de trama. Si FF=00 es una trama de MAC. Si FF=01 es una trama LLC y los valores 10 y 11 están reservados para uso futuro.
rr = Reservados y son siempre fijados en 0
ZZZZ = bits de control. Para tramas de MAC los bits de control indican si el almacenamiento rápido será o no utilizado. El almacenamiento rápido es utilizado cuando una trama MAC debe ser copiada inmediatamente y cuando las estaciones tienen lleno su espacio de almacenamiento de recepción. El almacenamiento rápido está disponible para guardar las siguientes tramas de MAC:

Alertas (beacon), reclamo del testigo, purga del anillo, monitor activo presente, monitor en espera presente, dirección duplicada, remoción de estación del anillo.

Para tramas LLC los bits de control son ignorados y reservados para uso futuro
4.- La Dirección Destino (DA) es la dirección de la estación a la que se intenta llegar.
5.- La Dirección Origen (SA) es la dirección del controlador que transmitió el paquete.
6.- El Campo de Información de Ruteo (RIF) es opcional y es usado en tramas que son enviadas a otros anillos mediante una fuente de ruteo.
7.- El Campo IEEE 802.2 que hace más flexible las conexiones LAN/WAN.
8.- El Campo de Datos. El campo de datos es responsable de llevar y traer los datos. El campo puede variar en tamaño, pero debe por lo menos tener un byte de longitud. En un anillo de 4 Mbps este campo puede ser de una longitud hasta de 4,472 bytes y en el de 16 Mbps el anillo puede manejar hasta 17,800 bytes.
9.- El Control de Secuencia de Tramas (FCS) es un campo de 32 bits que es usado para detección de errores a nivel bit.

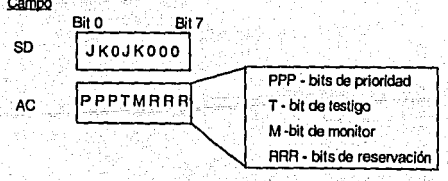
10.- El Delimitador Final (ED) indica el fin de una trama. Contiene el bit I (intermedio) y el bit E (error). El bit I fue implementado como un método de transmisión de múltiples tramas mientras se retiene el testigo y no es implementado usualmente. El bit E indica si alguna estación del anillo encontró algún problema con la calidad de la señal, directamente relacionado con la señal eléctrica en el cableado. Si está puesto en 1, ninguna estación copió la trama.

11.- El campo de estado de la trama (FS) es usado por el controlador si la estación destino recibió el paquete y fue capaz de copiar su contenido. Este campo no está cubierto por el FCS porque es cambiado por el destino y no por la estación de origen. La estación destino fija un bit para indicar que reconoció su dirección y que copió la trama al fijar los bits de reconocimiento de dirección, así como el bit de trama copiada a 1.



Leyendas

SD - Delimitador de Inicio
AC - Control de Acceso
FC - Control de la Trama
DA - Dirección Destino
SA - Dirección Origen
FCS - Secuencia de Control de la trama
ED - Delimitador Final
FS - Estado de la Trama
IEEE 802.2 - Norma utilizada para comunicaciones LAN-WAN



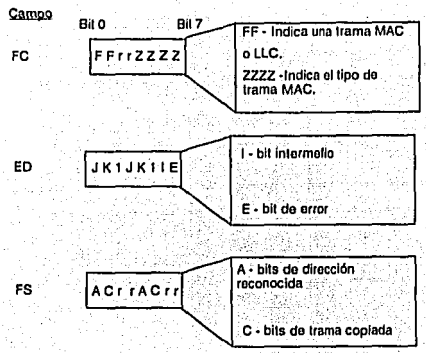


Figura 1.24. Definición de los campos de la trama de Token Ring.

1.1.8.5.7 Errores en Token Ring

Los errores en Token Ring están clasificados en 2. Los errores suaves y los errores duros. Un error suave es una condición de la que el anillo puede recuperarse fácilmente. En esta situación el anillo sigue operando normalmente pero existen errores que requieren ser monitoreados. El reporte de errores suaves se logra a través de las tramas MAC, las cuales son enviadas a los monitores del anillo.

Un error duro es una falla permanente de la cual el anillo no puede recuperarse por sí mismo. Los errores duros son generados muchas veces por equipo dañado. Todas las operaciones de datos en el anillo cesan hasta que el error es corregido. Unos ejemplos sencillos de estos errores pueden ser: malas conexiones en los cables lobe, una estación inicializando su entrada al anillo a una velocidad equivocada.

Cuando existe una condición de error duro, el anillo empezará a emitir una señal de alerta llamada beacon, que es una trama de MAC que indica quién está emitiendo esta señal en el anillo y quién es el vecino disponible posterior más próximo (NAUN). De esta manera la estación que está causando el problema puede ser fácilmente detectada.

1.1.8.5.8 Proceso de reclamo del testigo

Antes de que opere una red Token Ring tiene que haber un testigo en la red para que las estaciones puedan transmitir.

El proceso de reclamo del testigo sirve para dos propósitos. Primero, elige el Monitor Activo (AM), el cual controla la operación del anillo. Después de que ha sido elegido el AM, purga el anillo; esto es, hace una limpieza del anillo para asegurar que puede transmitir un paquete en el mismo y recibirlo de regreso en buenas condiciones. El AM es la única estación que puede colocar un testigo en el anillo.

El proceso de reclamo del testigo comienza cuando alguna de las siguientes situaciones le ocurren al monitor activo:

1.- Detecta pérdida de señal de su reloj.
2.- Un temporizador expira sin haber recibido la trama MAC de su monitor activo.
3.- No puede recibir suficientes tramas de MAC de purga de anillo propias.
El proceso de reclamo de testigo comienza cuando una de las siguientes condiciones le ocurre al monitor en espera:
1.- Detecta pérdida de señal.
2.- Detecta expiración de su temporizador por recibir sus tramas de monitor en espera o para la recepción de un testigo.
Este proceso ocurrirá cuando algo tan sencillo como la inserción al anillo ocurre. El AM detectará pérdida de la señal del reloj (el relevador en el MAU causó el error) y comenzará el proceso de reclamo de testigo.
Una vez que las estaciones han empezado el proceso de reclamo, otras estaciones repetirán las tramas de la estación o se involucrarán en el proceso. Este es muy simple, ya que se basa en prioridades. Si una estación del anillo recibe una trama MAC de reclamo del testigo, comparará su prioridad (no confundir con los bits de prioridad en el campo AC) con la trama MAC recibida. Si su prioridad es alta, la estación del anillo no repetirá la trama recibida. Transmitirá su propia trama MAC de reclamo del testigo. Cuando la estación original reciba esta nueva trama, parará las transmisiones propias de tramas MAC de reclamo de testigo y repetirá las tramas de mayor prioridad. Cualquier estación participante en este proceso desarrollará la misma comparación. La prioridad está generalmente basada en la dirección MAC de la estación del anillo. Entre más alta sea esta dirección, mejor será la probabilidad de que esta estación se convierta en el monitor activo.

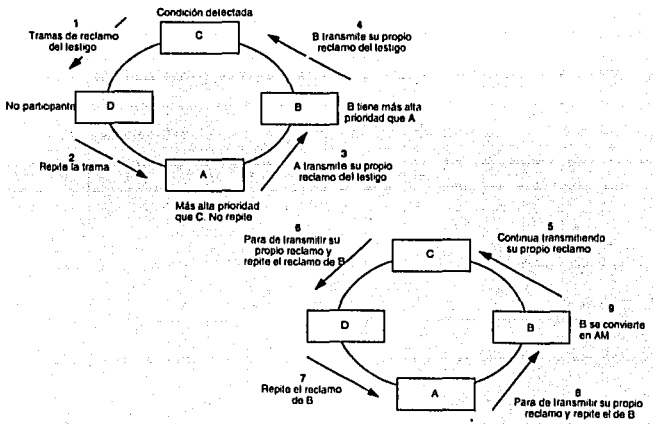


Figura 1.25. Proceso de reclamo del testigo.

1.1.8.5.9 Proceso de Notificación de Vecino

Uno de los procesos internos más importantes en el anillo es el proceso de notificación de vecino.

Dado que los datos viajan sobre el anillo en una sola dirección, una estación del anillo recibe las tramas únicamente de su vecino anterior y pasa estas tramas únicamente a su vecino posterior. Si una estación del anillo adquiere un nuevo vecino anterior, notifica a uno de los monitores. Este proceso ocurre cada 5 segundos.

La notificación de vecinos es una parte muy importante de la administración del anillo. El proceso comienza cuando el monitor activo transmite una trama MAC de monitor activo presente. La primera estación que recibe esta trama la copia y fija el bit A de reconocimiento de dirección y el bit C que es el de trama copiada en el byte de estado de la trama (la fija a 1 binario) a medida que la repite. Reconoce que es la primera estación en recibir esta trama porque los bits A y C están en 0, queriendo decir que ninguna otra estación ha recibido esta trama anteriormente. Esta estación del anillo guarda la estación origen de la trama recibida como el NAUN, quien en este caso es el monitor activo. Después de copiar la trama fija un temporizador. Cuando el tiempo en éste expira, mandará una trama MAC de monitor en estado presente.

La siguiente estación que recibirá esta trama, lo ignorará porque los bits A y C han sido modificados, indicando que hay más de una estación entre él y el monitor activo. Se fija un temporizador esperando recibir una trama MAC de monitor presente de su NAUN. Cuando recibe esta trama, una trama de monitor presente, los bits A y C están en 0 binario, copia y guarda la dirección origen como su NAUN y fija los bits de A y C en el campo FS a 1 binario. Repite esta trama de regreso al anillo. Esta estación fija su temporizador, transmite su propia trama de monitor presente para ser copiado y registrado por la estación posterior.

Cada estación repite el proceso mencionado. Finalmente, todas las estaciones estarán notificadas de su NAUN y el proceso para cuando el monitor activo recibe la trama MAC de monitor presente de su vecino anterior. El monitor activo reconoce esto porque en la trama MAC recibida, los bits A y C vienen en 0. El monitor activo fija estos bits y los repite de nuevo en el anillo. Sucedido esto, el proceso de notificación a vecinos está completo y será reinicializado por el monitor activo cuando el temporizador de notificación a vecino haya expirado.

1.1.8.5.10 Modo de transmisión en Token Ring

En un modo de transmisión normal, el controlador ha capturado y convertido al testigo. Fija los bits del campo A y C del testigo a 1 para indicar una trama de datos. Entonces transmite el resto de los campos AC y FC. El controlador de Token Ring revisa entonces la presencia del campo ED. Si el controlador no lo encuentra, asume que ha identificado incorrectamente la trama recibida como testigo, e inmediatamente transmite una trama de rechazo. Si encontrara el campo ED, insertaría el resto de su información en la trama, colocaría ED, CRC, y el campo FS al final de la trama y transmitiría el resto.

Si el controlador encuentra el campo ED, el resto de la trama incluye direcciones de origen y destino, el campo de ruteo de origen opcional, el campo de información y el campo CRC. Entonces es cuando anexará los campos ED y FS. Esto completa la transmisión del paquete. Habiendo completado la transmisión, el controlador espera el regreso de la trama, buscando su encabezado físico. Si el controlador no recibe este encabezado físico antes de transmitir

el campo de estado de la trama, transmitirá 0 binarios hasta que regrese la trama. Si el encabezado físico no regresa, el controlador se pondrá en el modo de repetición normal sin iniciar un testigo.
Cuando el encabezado físico regresa el controlador analiza la trama del anillo y libera el testigo. Después de sacar su paquete del testigo, el controlador entra en modo de repetición normal.

1.1.8.5.11 Modo de copiado en Token Ring

Una estación copiará la trama que coincida únicamente con su dirección, o sea una transmisión a un grupo de estaciones o general.
En modo de copiado, si el controlador encuentra que 1 de estas 3 condiciones existen, empezará a copiar hacia su dispositivo de almacenamiento la trama.
Si se detecta en cualquier momento un error en la trama, el controlador fija los dos bits de A y el único de E y repite la trama en el anillo. Si no encuentra errores, el controlador fija los dos bits de A y los dos bits de C, indicándole al origen que ha recibido la trama, y fue capaz de copiar la trama sin error. La estación logra esto mientras regresa la trama al anillo.
La estación que transmitió originalmente el paquete al anillo, lo retira. La estación destino no es la que retira el paquete del anillo.

1.1.8.5.12 Modo de repetición en Token Ring

Si la estación no copia una trama (esto es, que la trama no esté destinada para esta estación del anillo), la tarjeta controladora simplemente repetirá la trama a su vecino posterior, revisando los datos en el testigo y las tramas recibidas por si existieran errores. La estación fijará el bit de detección de error en el momento de reconocer el error mismo.

1.1.8.5.13 Token Ring de 16 Mbps.

El Token Ring de 16 Mbps utiliza un procedimiento de testigo único en el cual existe una liberación temprana del testigo (ETR). En el procedimiento ETR la estación origen libera el testigo al anillo al poco tiempo después de haber transmitido la trama. Esto quiere decir que el testigo está disponible antes de que regrese el encabezado de la trama a su estación origen. El testigo está disponible para la siguiente estación que se encuentra en línea y desee transmitir, esta estación repite el procedimiento de liberación temprana del testigo. Aunque el procedimiento ETR permite el acceso de múltiples tramas al anillo, existe únicamente un solo testigo en el anillo a la vez.
El ETR es una característica opcional que puede ser habilitada o deshabilitada en la tarjeta controladora de acuerdo a las necesidades.
El número de tramas que pueden circular en el anillo, en el caso de ETR, depende del tamaño del mismo anillo. Puede darse el caso de que un anillo pequeño pueda acomodar únicamente una trama a la vez. Los anillos de gran tamaño pueden entonces, beneficiarse del proceso ETR aún más que los anillos pequeños.

1.1.9 La capa de Enlace de Datos en FDDI

1.1.9.1 Antecedentes

FDDI permite a las estaciones comunicarse sobre una topología de anillo doble, con acceso garantizado al segmento a intervalos predeterminados de tiempo, usando un testigo. Esto podría parecer igual a Token Ring, pero los algoritmos de los métodos de acceso son diferentes.

Una estación debe esperar el arribo del testigo antes de que la transmisión empiece. Hasta el arribo del testigo, la estación captura el testigo y esto detiene el proceso de repetición del testigo. Una estación transmite una serie de símbolos combinados dentro de las tramas a la siguiente estación activa de la red. La transmisión de la trama continuará hasta que el tiempo permitido para retener el testigo expire o que no tenga más que transmitir, lo que significa que se pueden transmitir varias tramas, no sólo una. Hasta entonces la estación libera el testigo.

El vecino posterior recibirá estos símbolos, los regenera, y los repite a su vecino posterior. Cuando la trama regresa al originador, éste retirará el cuadro del anillo.

1.1.9.2 Temporizadores del anillo FDDI

Para la adecuada operación del anillo se requiere de establecer una conexión, una inicialización del anillo, un estado estable de la operación y mantenimiento del anillo mismo. Para esto se tiene una serie de temporizadores que ocupan un lugar muy importante en la adecuada operación del anillo.

Estos temporizadores son:

Temporizador rotacional del testigo (TRT), el cual es usado para medir la duración de operaciones en una estación.

Temporizador de retención del testigo (THT), el cual determina el tiempo que una estación puede retener el testigo.

Temporizador de transmisión válida, el cual detecta ruido excesivo en el anillo, pérdida del testigo y otros errores.

Temporizador de la velocidad de rotación del testigo (TTRT), el cual es un parámetro que fija la velocidad de rotación del testigo en el anillo.

1.1.9.3 Las tramas de FDDI

Dado que no hay un reloj maestro en el anillo de FDDI, cada estación produce su propio reloj cuando transmite. Las tramas de FDDI usan un preámbulo que permite que la estación receptora sincronice su reloj con la señal de reloj recibida en el paquete que está siendo transmitido.

El delimitador de inicio (SD) es una trama especialmente formateada que contiene violaciones de fase en la señal. De esta forma el SD indica que una trama está por recibirse.

La trama de control (FC) indica qué clase de trama es la que se aproxima. Por ejemplo, podría ser una trama de testigo, reclamo del testigo, trama de datos, etc.

La dirección destino y la dirección origen (DA y SA) puede fijarse a 16 o 48 bits. Esto está indicado por la longitud L en bits en el campo FC. Todas las estaciones del anillo deberán fijarse a 16 o 48 bits. En la mayoría de los casos FDDI implementa 48 bits de dirección.

El delimitador final (ED) indica el final de la trama. Igual que el delimitador de inicio contiene violaciones de fase en la señal, colocada en ciertos lugares de ED para que el controlador reconozca este campo como el final de la trama.
La trama del campo de estado FS contienen 3 bits importantes que son fijados por otras estaciones en el anillo. Éstos son la dirección reconocida, la trama copiada y los bits de error. El bit de dirección reconocido es fijado por una estación debido a 1 o 2 razones. Ha reconocido su dirección en una dirección duplicada de trama SMT (administración de estación) o reconoció su dirección en una trama LLC. Esto no quiere decir que si una estación reconoció su dirección haya tenido que copiar la trama. Pudo haber estado demasiado ocupada. El bit C indica que una estación destino pudo copiar la trama. El bit E indica que alguna estación (no necesariamente la estación destino) encontró una señal de error en la trama. Si este bit es fijado, el bit C no podrá ser fijado ya que para cualquier trama encontrada en error, no será copiada.

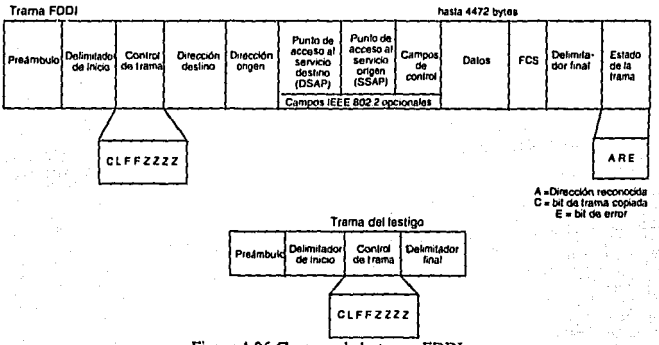


Figura 1.26 Campos de la trama FDDI.

El direccionamiento en FDDI es similar al direccionamiento de MAC del IEEE 802. La orden de transmisión de los bits es similar al de Token Ring y opuesto en ordenamiento al de Ethernet como se explicó con anterioridad.

1.1.9.4 Proceso de inicialización del anillo

Después de haber logrado la conexión física de las estaciones, éste se debe de inicializar. Una de las estaciones debe colocar el testigo en el anillo, lográndose esto cuando una nueva estación se conecta al anillo, cuando no existen otras estaciones en el anillo o cuando se pierde el testigo por alguna otra razón. Cualquier estación en el anillo tiene la capacidad de iniciarlo, pero existe un proceso de contienda en la que sólo una estación puede inicializar el anillo. La estación con el menor TTRT ganará el derecho de inicializar el anillo.

El proceso termina cuando una estación recibe su trama de reclamo de regreso. Esto quiere decir que las demás estaciones en el anillo le han concedido el derecho de inicializarlo. La estación que ganó genera un nuevo testigo en el anillo.
Si se llegaran a presentar 2 TTRT iguales se decidiría por la estación que tuviera la dirección de MAC mayor.
La primera vez que el testigo circula en el anillo no será retenido por ninguna estación, en lugar de esto, las estaciones fijarán su TTRT para coincidir con la estación inicializadora.
En el segundo paso del testigo las estaciones de la red podrán transmitir tráfico síncrono y en el tercer paso del testigo tráfico asíncrono.
Normalmente el tipo de tráfico que se utiliza es el asíncrono ya que el síncrono sólo se utiliza para ciertas aplicaciones de transmisión de voz y video.

1.1.9.5 Notificación del vecino y detección de direcciones duplicadas

Este proceso es, en términos generales similar al que se realiza en Token Ring. Este proceso se produce cuando una estación entra al anillo y posteriormente cada 30 segundos. Este proceso se llama proceso de notificación de vecino (NNP) y también sirve para identificar las direcciones duplicadas.

1.1.9.6 Operación normal

Una vez que todas las pruebas de verificación han sido satisfactorias, el anillo puede comenzar su transmisión de datos normalmente en un *estado estable de operación*. Con esto las estaciones pueden transmitirse tramas una a otra bajo las reglas del anillo FDDI el cual permanecerá en este estado hasta que un nuevo proceso de reclamo se inicia.
El proceso de operación es muy similar al de Token Ring, con la diferencia de que en este caso se puede transmitir más de una trama a la vez, tantas como lo permita el valor del THT.

	FDDI	IEEE 802.3	IEEE 802.5
Ancho de banda	100 Mbps	10 Mbps	4 o 16 Mbps
Número de estaciones	500	1024	250
Distancia máxima entre estaciones	2 km (MMF) 20 km (SMF)	2.8 km	300 m (4 Mbps); Norma recomendada: 100 m para 16/4 Mbps
Longitud máxima de red	100 km	2.8 km	300 / 100 m
Topología lógica	Doble anillo y doble anillo de árboles	Bus	Anillo único
Topología Física	Anillo, estrella	Estrella, bus	Anillo, estrella
Medio de conexión	Fibra óptica	Fibra óptica UTP Cable coaxial	STP, UTP Fibra óptica
Método de Acceso	Paso de testigo medido	CSMA/CD	Paso de testigo
Adquisición del testigo	Captura del testigo	N/A	Convierte el testigo en trama
Liberación del testigo	Después de transmitir	N/A	Después de retirar su trama (4) o después de transmitir (16)
Tramas sobre la LAN	Múltiple	Una	1 (4) o múltiple(16)
Tramas en la LAN por acceso	Múltiple	Una	Una
Tamaño máximo de trama	4500 bytes	1518 bytes	4,500 bytes (4) o 17,800 bytes (16)

MMF = Fibra multimodo, SMF = Fibra monomodo

Figura 1.27. Cuadro comparativo de Ethernet, Token Ring y FDDI.

1.1.10 Modo de transferencia Asíncrona (ATM)

1.1.10.1 Antecedentes

El modo de Transferencia Asíncrona,o ATM, define un método de transmisión y conmutación de datos entre sistemas de redes. Las tecnologías que definen ATM se componen de otros métodos de comunicación existentes, tales como conmutación de circuitos y la conmutación de paquetes. ATM ha tomado estas metodologías y ha aplicado los conceptos de una manera nueva y revolucionaria.

Una de las principales fortalezas de ATM es su habilidad para soportar los servicios de multimedia. Estos servicios de multimedia, a su vez proveen servicios de transportación de tráfico en sistemas de redes, este tráfico de base de datos es el mismo existente entre dos estaciones de trabajo, pero además incluye tráfico para conexiones de voz y aplicaciones de video. Anteriormente, cada tipo de servicio requería que su propia red proporcionara el tipo de servicio necesario para la transportación de información generada por el mismo servicio. Con ATM, toda la información de los diferentes tipos de servicios son adaptados a un formato común para que la red transporte una pieza o parte común de datos a través de su troncal o backbone. El formato es conocido como célula, al

ser fija su estructura le permite al método ATM dar soporte a diferentes tipos de información.
Otro de los puntos sobresalientes de esta nueva tecnología es su interface con las redes. Primero, las conexiones ATM de una estación de trabajo a la red son típicamente de un alto ancho de banda. Muchas propuestas o especificaciones para el servicio de ATM empiezan con un mínimo de ancho de banda de 45 Mbps e incrementan hasta 2.5 Gbps. Con esto podemos ver que ATM ofrece por mucho una diferencia sustancial de los servicios actualmente ofrecidos.
ATM es un servicio orientado a conexión, lo que significa que ATM soporta un concepto llamado circuitos virtuales. Un circuito virtual le permite a un dispositivo ATM solicitarle a la red la conexión remota de uno o varios sistemas.
También, todas las conexiones tanto locales como remotas son iguales, lo que permite integrar un tipo de red más sencilla y homogénea. ATM no está definida completamente para redes Locales, Amplias o Metropolitanas (LAN, MAN y WAN), lo que está definido son dos tipos de interfaces. La Interface Usuario-Red (User Network Interface), UNI que define interconexión entre el usuario y la red, y La Interface Nodo De Red (Network Node Interface), NNI que define interconexión entre dos redes.
Un usuario en una red ATM puede consistir en diferentes dispositivos. Podría ser una PC o estación de trabajo con interface ATM, otro podría ser un puente o rutedador.
Un Nodo de Red en una red ATM serían los conmutadores involucrados en crear la malla del Backbone o troncal. Los conmutadores pueden ser accesados por vía de una empresa pública, como la compañía de teléfonos o por vía privada según el caso. De cualquier modo, una conexión de un conmutador a otro dentro de un mismo dominio, se considera una conexión NNI.
Por último, ATM se basa en especificaciones de documentos ITU-TSS (CCITT).
ATM es una tecnología nueva y emergente. Consecuentemente, las normas que definen ATM están bajo constante revisión y actualización.
El desarrollo inicial de ATM lo realizó el CCITT Comité Consultivo para Telegrafía y Telefonía Internacional, llamado ahora ITU-TSS.
Los primeros conceptos de ATM nacieron de un trabajo realizado por AT&T y CNET relacionado a la conmutación de células, en 1983. Cinco años más tarde, la CCITT adoptó estos conceptos como modo de transferencia para la BISDN (Red Digital de Servicios Integrados de Banda Ancha).
La ANSI ha participado activamente en el establecimiento de normas para ATM en aplicación dentro de los Estados Unidos.

1.1.10.2 Generalidades de BISDN

ATM está basado en el concepto llamado Red Digital de Servicios Integrados de Banda Ancha (BISDN). BISDN fue definido por la CCITT (ITU-TSS) adoptando a ATM en 1988 como el servicio que proveería el soporte para BISDN.
El concepto BISDN define una red integrada . La integración combinaría varios servicios de comunicación en una sola red. Los servicios consistentes en aplicaciones de datos entre computadoras conectadas, sistemas de voz interconectando usuarios de teléfonos y aplicaciones de video para utilización de gráficos en monitor. Anteriormente, cada uno de

estos servicios eran soportados por su propio sistema de transporte en red. BISDN propuso la combinación de todos estos servicios en un transporte común que fue ATM.
BISDN tiene la capacidad de combinar todos los servicios gracias al tipo de transporte en red que propuso, esto es, la utilización de células. Mediante el uso de transmisión digital. Como un servicio de banda ancha, BISDN provee el acceso a múltiples canales de transmisión a los usuarios de la red.
BISDN definió inicialmente el acceso a través de redes públicas, sin embargo, fue comprobado que al aplicarse perfectamente a las LAN, podría llegar a implementarse en las WAN.
Para permitir un soporte integrado, BISDN debe adaptar los tipos de servicios como voz, video y datos a un formato que permita la transmisión y conmutación de éstos sobre una red. Una célula normal de longitud fija es usada para éstos fines. La célula es aceptada por la red, transmitida y conmutada de su fuente a su destino apropiado.

1.1.10.3 Generalidades de ATM

ATM está basada en la conmutación de células, lo cual define el método de cómo la información es transmitida de una estación a otra y conmutada a través de los diferentes enlaces. Como resultado de esta transmisión y método de conmutación, un patrón irregular y recurrente de células pueden ser transmitidas por conexión. Algunas características importantes del relevo de células son:
Baja latencia debido al pequeño y fijo tamaño de la memoria intermedia y transmisión de colas.
Baja relación de errores debido a la eficiencia de las redes digitales de alta velocidad.
La detección de errores en los datos y el control de flujo no es realizado enlace por enlace.
Como es un servicio orientado a conexión, posteriormente a ésta no se requiere:

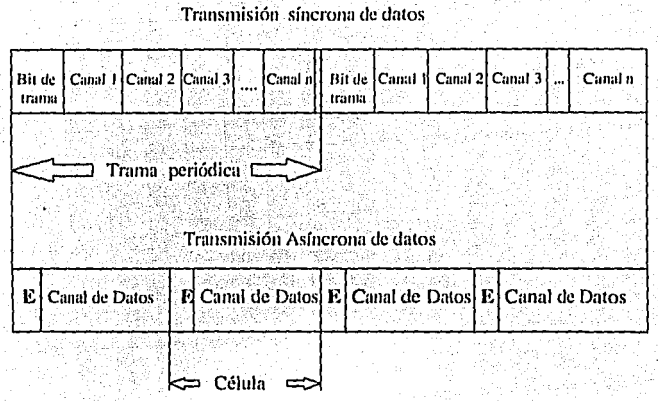
- La dirección de fuente y destino
- Control de Secuencia
- Solicitudes de retransmisión.

Utiliza una arquitectura de célula de longitud fija, compuesta por 53 bytes.

- El encabezado es reducido a 5 bytes.
- Un pequeño campo de información de 48 bytes.

Servicio de una o de dos vías (half duplex o full duplex).

1.1.10.4 Modos de Transferencia



E = Encabezado

Figura 1.28 Transmisión Síncrona y Asíncrona de Datos.

De las tecnologías actuales, existen tres métodos de comunicación:

Modo de Transferencia Síncrona
Modo de transferencia de Paquetes
Modo de Transferencia Asíncrona

El Modo de Transferencia Síncrona, o conmutación de circuitos, es el método más común de los tres. Consiste en conexiones telefónicas, líneas privadas o enlaces E1 o T1, variando en rangos de velocidad hasta 45 Mbps. Cada uno de estos servicios se adapta perfectamente en velocidad a la relación de bits constantes, para la aplicación de voz y video, así como variable para las aplicaciones de transmisión de datos.

La disponibilidad del ancho de banda, así como la baja latencia de cada conexión, son los factores que le permiten trabajar adecuadamente con todas las aplicaciones. Lamentablemente, debido a la configuración fija de las conexiones punto a punto, la transferencia síncrona no se adapta del todo bien a las aplicaciones que requieren conectividad de múltiples sistemas.

Por otro lado, el modo de transferencia de paquetes o conmutación de paquetes, provee una conexión flexible, como lo son X.25, Frame Relay, SMDS para WAN, así como los medios de acceso mencionados anteriormente para LAN. Aunque cada una de estas tecnologías proveen excelente soporte para la transmisión de datos, carecen de la habilidad para soportar aplicaciones de voz y video.

El modo de transferencia asíncrona combina las mejores características de los dos métodos anteriores. Por consiguiente, las aplicaciones de voz, video y datos trabajan perfectamente bien utilizando este método de transmisión. La razón radica en la disponibilidad de ancho de banda y la baja latencia asociada al método síncrono, así como a la flexibilidad de conexión del modo de conmutación de paquetes.

1.1.10.5 Clasificación de servicios ATM

Cada tipo de tráfico, sean voz, video o datos, residen en el mismo transporte de la red, la cual deberá adaptar cada requerimiento de servicio a un formato común. Esto se logra mediante la capa de adaptación de ATM (AAL).
AAL define cómo la información de la aplicación es encapsulada en la célula y posteriormente desencapsulada y reorganizada a su formato original. Cada tipo de tráfico tiene diferentes características, por lo que se definen los diferentes servicios de la siguiente manera:
Clase A/AAL 1. Utilizado en aplicaciones de alta calidad de video y voz.
Clase B/AAL 2. Utilizado en aplicaciones de compresión de video y voz de baja calidad.
Clase C/AAL 3,4 y 5 . Utilizado en aplicaciones de datos en general.
Clase D/AAL 3 y 4 . Utilizado en aplicaciones de alto tráfico de datos.

	Clase A	Clase B	Clase C	Clase D
Temporización	Requerida	Requerida	No Requerida	No Requerida
Velocidad de bits	Constante	Variable	Variable	Variable
Modo	Orientado a Conexión	Orientado a Conexión	Orientado a Conexión	Sin conexión
Tipo	AAL1	AAL2	AAL3/4, AAL5	AAL 3/4

Figura 1.29. Comparación de servicios ATM.

Aplicaciones en tiempo real como son voz y video, requieren de medición de tiempo de punta a punta, mientras que la transmisión de datos no lo requiere.
La relación de bits es directa, algunos servicios mandan tráfico constantemente aunque parte del tráfico no contenga información. Otros servicios como transmisión de datos o tráfico repentino, transmiten únicamente cuando es necesario.
Los modos de conexión identifican si un servicio o aplicación requiere de un camino predefinido entre los sistemas de origen y destino.

1.1.10.6 Especificaciones de interfaces de Redes

Interface Usuario-Red (UNI).
Esta especificación define cómo un usuario se interconecta con la red. Un usuario es cualquier dispositivo conectado a la red (ruteador, concentrador, etc.) que para el caso de ATM, contiene una interface de red ATM que permite el acceso a la utilización de la red. Aunque son similares, existen dos especificaciones UNI:
La UNI pública, la cual es usada para interconectar un usuario a un servicio público de ATM. Una implementación típica es similar al de una WAN, tal como Frame Relay.

La UNI privada, es usada para interconectar usuarios a un conmutador que es administrado como parte de la misma red corporativa, esta implementación es similar al de las LAN.
Muchas recomendaciones han sido presentadas en función de las especificaciones ATM UNI, las versiones más recientes son:
Especificación ATM UNI Versión 3.1 (Verano 1994)
Especificación ATM UNI Versión 3.0 (Septiembre 1993)
Especificación ATM UNI Versión 2.0 (Junio 1992)

1.1.10.7 Interface Nodo-Red (NNI)

La especificación NNI define cómo una red ATM se interconecta con otra red ATM. Este tipo de conexión se logra mediante el enlace de un conmutador ATM a otro.
Similar a las especificaciones UNI, la NNI también tiene definiciones públicas y privadas. Las conexiones típicas NNI se encuentran frecuentemente contenidas en redes de servicio públicas ATM, como parte de una topología de malla o nube.
En general, la NNI existe para asegurar que los conmutadores de red ATM conozcan la topología interconectada de la red, permitiendo a los conmutadores tomar la mejor decisión en cuanto a conmutar un circuito virtual a su destino.

1.1.10.8 Interface Transportadora de Intercambio de Banda Ancha (B-ICI)

La especificación B-ICI define la interconexión de dos redes públicas, siendo la interconexión de los conmutadores de cada una de la redes.

1.1.10.9 Aplicaciones ATM

Una posible implementación para ATM, es la de un a troncal o backbone, interconectando varias LANs, como Ethernet, Token Ring y FDDI. Las razones del por qué ATM puede funcionar exitosamente como un servicio de backbone son:

Facilidad de interface común para todo tipo de conexiones, incluyendo interconexión LAN-WAN.

El ancho de banda asociado al conmutador es mayor o equivalente a la suma de todos sus enlaces, ofreciendo así un servicio ininterrumpido, ya que la red nunca se verá saturada por tráfico.

Baja latencia punto a punto, basada en conmutación de hardware (física).

Ancho de banda escalable, incrementos en enlaces de ancho de banda fácilmente implementables.

Necesidades mínimas de administración, la implementación de los conceptos de redes virtuales ofrecen mayor responsabilidad y seguridad.

El flujo de tráfico no necesita ser balanceado ya que se tiene un ancho de banda asegurado y constante.

Otra implementación es el acceso remoto, reemplazando WANs existentes. La relación de transmisión de ATM es mucho mayor que la gran parte de las WAN existentes en la actualidad, incluyendo X.25, Frame Relay y conexiones dedicadas punto a punto que utilizan protocolos como PPP y HDLC. Además de que ATM soporta aplicaciones de multimedia sumado a todos los demás servicios remotos, eliminando así un posible costo adicional de redes paralelas o redes separadas.

También ATM puede ser usada en implementaciones tipo LAN, como emulación de las mismas, ofreciendo así una característica que muchas LANs no pueden, la transmisión en ATM es full duplex, es decir, una estación ATM puede transmitir y recibir simultáneamente a diferencia de las estaciones Token Ring, Ethernet o FDDI que únicamente transmiten o reciben, pero no simultáneamente. Como consecuencia podemos pensar en que ATM será sumamente útil en situaciones donde exista un alto volumen de tráfico como son servidores de archivo o sistemas de imagen. La emulación de LANs ofrece beneficios adicionales como el tamaño ilimitado de paquetes que puede manejar ATM comparado con el tamaño manejado por las normas LAN. Aún cuando el paquete está segmentado en células, ATM cuenta con las herramientas necesarias para realizar las tareas de segmentación. Por lo que el desempeño en general del sistema se verá mejorado de manera notable.
Se tiene contemplado que a finales de 1994 ya se maneje en empresas un tráfico considerable basado en ATM, que a finales de 1996 o antes se emplee BISDN y alrededor de 1999, éste se emplee públicamente. Los factores que acelerarán dicho avance serán la instalación generalizada de fibras ópticas y el empleo extendido de SDH.

1.1.10.10 Formato de la Célula de ATM

El formato de la célula de ATM está formado por los siguientes campos:
Control de Flujo Genérico (GFC). Está compuesto por 4 bits de longitud y controla el flujo de tráfico de la terminal a la red.
Identificador de Ruta Virtual (VPI). Tiene 8 bits de longitud. Permite hasta 256 rutas virtuales y cada ruta puede tener varios canales virtuales.
Identificador de Canal Virtual (VCI). Tiene 16 bits de longitud.
Indicador de tipo de contenido (PTI). Tiene 3 bits de longitud e identifica tráfico normal y tráfico de mantenimiento.
Prioridad de pérdida de célula. Tiene 1 bit de longitud e identifica una célula de alta prioridad (0) o una célula sujeta a desecharse (1).
Revisión de error en encabezado (HEC). Tiene 8 bits de longitud y realiza revisiones de error en el encabezado. Realiza detecciones múltiples o individuales de bits con error. Es capaz de corregir errores de un solo bit.
Contenido (Payload). Contiene la información de la capa superior de datos o de servicios.

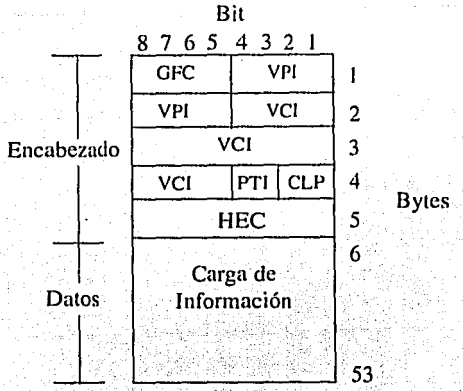


Figura 1.30. Formato de la célula ATM con encabezado UNI.

1.2 Dispositivos de conexión entre Redes

1.2.1 Repetidores

Los repetidores proveen la forma más barata y sencilla de conexión entre dos LANs.
Un repetidor regenera la señal que recibe, sin efectuar ningún cambio en la misma. Es decir el dispositivo debe enlazar dos redes de tipo idéntico (Ej.: Ethernet-Ethernet) y protege la señal contra atenuación o degeneración producida por el mismo medio de conexión.
Los repetidores deben usarse cuando se requiere extender la distancia a la cual se transmite la señal de la PC sin afectar la calidad de la transmisión. Simplicidad de conexión a costa de aumentar la congestión en la red, luego entonces no se recomienda su uso para secciones de la red que manejen funciones críticas en cuanto a recursos de máquina.
Cabe mencionar que las reglas de topología de red del IEEE 802.3 especifican que "Un paquete de datos podrá atravesar no más de cuatro repetidores".

En la figura 1.31 se muestra un ejemplo de conexión a través de repetidores, para dos redes Ethernet:

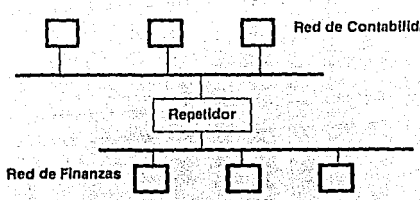


Figura 1.31. Conexión de un repetidor entre redes.

1.2.2 Puentes (Bridges)

Los puentes proveen una conexión más inteligente que los repetidores.
Al añadir un puente en una red de área local, se divide a ésta en dos secciones funcionales, llamadas segmentos. El puente lee las direcciones MAC contenidas en cada paquete de cada segmento y sólo deja pasar los paquetes que pertenecen al otro segmento.
Esta función la efectúa mediante una tabla de direcciones y requiere que ambas redes manejen el mismo protocolo. En los equipos actuales las tablas son generadas automáticamente por el mismo equipo, es decir, al encender el puente, éste manda señales a los dispositivos para leer qué tiene conectado en ambos lados y obtener la información de sus direcciones.
Ya en operación el puente lee para cada paquete la información de origen y destino, busca la dirección de origen en sus tablas, si la encuentra, verifica si la dirección de destino está en la misma tabla, en caso contrario deja pasar el paquete al otro lado sin modificarlo.
La colocación de un puente permite reducir la cantidad de tráfico sobre una red y aumenta así su desempeño. Adicionalmente permite conectar más de dos redes LAN, y así desde el punto de vista del usuario el puente le permitirá crear una red extendida dándole acceso a dispositivos y/o servicios, a los cuales antes no tenía acceso.
Con puentes remotos pueden conectarse transparentemente redes distantes usando líneas de enlace, es decir, un segmento de red pudiera estar en la Ciudad de México y otro en la Ciudad de Monterrey.
Los puentes se usan entonces cuando se requiere hacer crecer el tamaño de las redes sin sacrificar desempeño en las funciones locales de cada segmento, o bien conectar usuarios remotos de manera transparente. En cuanto a costo son más caros que los repetidores, pero no se sacrifica velocidad de la red local.
Varios puentes se pueden interconectar a través de varias LANs a fin de crear rutas diferentes para envío de la información, sin embargo no es la mejor forma de lograr este propósito.

Presenta también la limitante de que no permite trabajar con diferentes topologías de red (EJ.: Ethernet-Token Ring).
Al utilizar los puentes para efectuar un ruteo básico se utiliza un algoritmo llamado "Spanning Tree" (Árbol de tolerancia) que está normalizado por el IEEE 802.1d, con esta topología lo que se pretende es tener una ruta alternativa para comunicación dentro de una WAN o LAN, para los casos en que se perdiera la comunicación con un enlace, automáticamente el puente busca a través de otro puente enviar la información a fin de que llegue a su destinatario. Este algoritmo no permite seleccionar cual ruta es mejor, únicamente las accesa en el orden en que se le programaron las tablas de desición.
En la figura 1.32 se muestra la conexión de redes Ethernet a través de puentes.

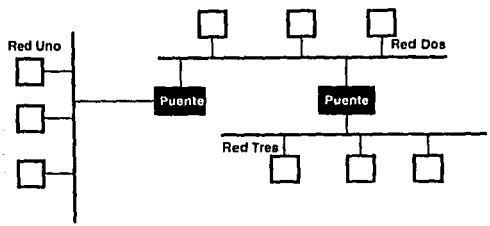


Figura 1.32. Conexión de redes a través puentes.

1.2.3 Ruteadores

Lo mismo que los puentes, el ruteador está diseñado para extender el tamaño de las redes, sin embargo lo hacen de una manera todavía más inteligente, cuando las redes crecen ya sea en tamaño o complejidad será más recomendable el utilizar un ruteador.
Estos dispositivos permiten el construir una red compleja, utilizando una topología de malla, a fin de tener múltiples rutas de acceso para solucionar los problemas posibles de comunicación entre puntos y dar una flexibilidad mayor a la red, aumentando el desempeño y tratando de optimizar la utilización de los recursos de enlace y puntos de conexión.
El ruteador también lee las direcciones de origen y destino de los paquetes, pero éste los puede manejar de manera más eficiente, es decir, si un paquete es recibido en el ruteador el equipo analiza cuál es la vía más rápida y más barata para enviarlo y aún más si el paquete es demasiado extenso lo pude partir y enviarlo por diferentes rutas a fin de que llegue lo más pronto posible. Adicionalmente, puede traducir entre diferentes protocolos de redes para poder interconectar prácticamente cualquier red a una WAN.
Así pues un Ruteador puede dirigir los paquetes de datos hasta su destino a través de la vía más eficiente o bien la ruta deseada por el usuario dentro de una red. El Ruteador examina el protocolo de red para cada paquete que recibe, permitiendo la implementación del

filtrado necesario, el control de seguridad y la redundancia de rutas necesaria, según se requiera.
Las capacidades de este dispositivo lo hacen la elección idónea para redes de constante crecimiento y que puedan alcanzar grandes tamaños y mayor complejidad.
Resumiendo, estos dispositivos no sólo proveen redundancia, seguridad y segmentación adecuada de redes, sino también flexibilidad (pueden usar rutas alternas) y mejor utilización del ancho de banda (la mejor ruta se elige antes de enviar la información).
El ruteador interviene en las capas 1, 2 y 3 del modelo OSI.
En la figura 1.33 se muestra un conexión típica usando ruteadores:

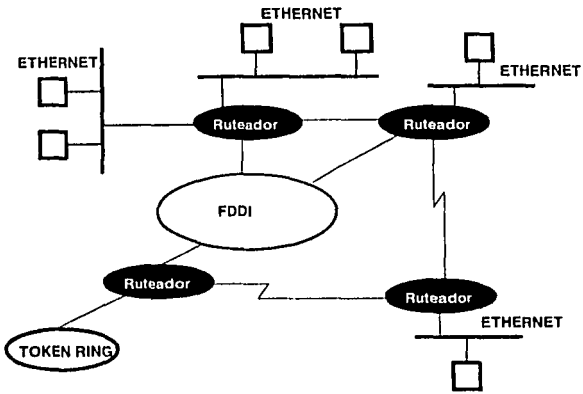


Figura 1.33 Conexión típica utilizando ruteadores.

1.2.4 Gateways o compuertas de ruteo

Una compuerta provee el modo más inteligente de conexión, sin embargo es el más lento. Se puede decir que el gateway puede hablar en varios idiomas o más apropiadamente para el caso manejar varios protocolos de manera simultánea, así bien puede comunicar efectivamente una máquina que utiliza TCP/IP con una que utiliza DECnet o bien SNA. Entonces el gateway permite a los dispositivos dentro de la red comunicarse y no meramente conectarse con otros dispositivos en otras redes.
Las compuertas intervienen en las capas 1, 2, 3 y 4 del modelo OSI.

1.2.5 Conmutadores (Switches)

Ésta es una tecnología reciente para redes Ethernet, la cual hace las funciones de conexión sin un completo análisis de la información, así se aumenta la velocidad en forma

dramática, pero no puede hacer conversiones de protocolos. Básicamente sustituye al puente en ambientes locales (LAN).
Esta tecnología permite un alto desempeño de la red a un bajo costo. A diferencia de los puentes y ruteadores, el conmutador entrega la información a una velocidad muy superior a cualquiera de los otros dispositivos.
Como ejemplo comparemos el tiempo de transmisión de 800 bytes a través de cada uno de los siguiientes dispositivos:

Puente	800 µs
Ruteador	1000 µs
Conmutador	40 µs

El conmutador maneja la información en tramas. Esta conmutación, a diferencia de los puentes, maneja el tráfico dirigido desde el origen hasta el destino, es decir, que el tráfico es entregado únicamente a los integrantes de la misma red lógica, mientras que el puente lo entrega al segmento físico.

1.3 Redes de Área Amplia (WAN)

1.3.1 Antecedentes

Muchas redes de área local hoy en día están distribuidas alrededor del mundo. Usualmente se requiere conectarse a una o más computadoras centrales, ya que compartiendo recursos se aumenta el desempeño de un sistema de información y procesamiento de datos.
Las compañías están sustituyendo sus viejos centros de cómputo con un nuevo concepto: Los centros de control de redes, los cuales concentran en un sólo punto todos los recursos de datos de la empresa en forma simple y con seguridad.
Dos factores influyen notablemente en esta tendencia:

1) Los recursos de trabajo de cómputo, así como los servidores de los mismos pueden ser administrados y respaldados de forma más eficiente si están centralizados en una sola posición.
2) Las compañías cada vez dirigen más aplicaciones críticas y datos confidenciales hacia las redes, entonces la seguridad y protección de los datos se convierte en una situación de gran importancia.

Una red de área local (LAN) puede servir como ya vimos a un grupo de edificios u oficinas. Ahora bien cuando es necesario cubrir una gran superficie o distancia geográfica se utilizan las redes de área amplia (WAN), las cuales utilizan diversas interfaces para interconectar LANs en un ambiente transparente y de múltiples fabricantes.
Una red WAN puede cubrir una ciudad, un estado, un país o países o bien todo el mundo.

1.3.2 X.25

En los años 70 el CCITT empezó a trabajar en la norma X.25. A través de este esfuerzo, el comité trató de proveer un método normalizado de transportación de datos a través de una red de área amplia (WAN).
La recomendación X.25 está caracterizada por:

Normas definidas por el CCITT. En aquella época el comité era una organización normalizadora reconocida internacionalmente por las industrias de las telecomunicaciones y comunicaciones de datos.

Arquitectura de tres capas. La recomendación X.25 actualmente incorpora varias normas que pertenecen a las tres capas inferiores del modelo de referencia OSI.

Conmutación de paquetes. La recomendación define los procedimientos de conmutación de paquetes de datos.

Desde el principio, las Redes Públicas de Datos (PDN) se propusieron resolver su problemas de interoperabilidad. Usando X.25 como un protocolo de acceso obligatorio, resolvieron este problema. De esta forma cualquier compañía podría conectarse a través de una PDN y comunicarse con otras oficinas de su propia compañía o de otras sin mayor problema.

Debido que hay muchas compañías que ofrecen los servicios públicos de X.25, es necesario poder interconectar estas redes de X.25. Dos PDN se conectan entre sí a través de una conexión X.75. La especificación X.75 define los procedimientos de interconexión entre redes X.25.

Las características de los protocolos contenidos en la recomendación X.25 incluyen:

Diseño para uso en Redes Públicas de Datos (PDN). La recomendación X.25 está basada en la premisa de que el usuario puede mandar datos a otra PDN, así como se puede establecer una llamada de voz con quien sea y donde sea.

Uso sobre servicios telefónicos analógicos de mala calidad. La recomendación de X.25 asume la responsabilidad de asegurar la transmisión sobre líneas con problemas.

Caracterizado por una exhaustiva detección y recuperación de errores. Provee almacenamiento temporal y retransmisión de tramas y paquetes. Las estaciones finales así como los nodos de conmutación proveen estos servicios para asegurar que todos los datos que viajan en la red están libres de error.

Orientado a conexión en la capa tres. A diferencia de otras arquitecturas, X.25 mantiene conexiones en la capa tres. De forma similar a las llamadas de voz, se establece una ruta de punta a punta.

Multiplexaje de circuitos lógicos sobre un mismo circuito físico. Un nodo puede rutear hasta 4096 circuitos virtuales sobre el mismo enlace punto a punto entre nodos.

1.3.2.1 Circuitos virtuales conmutados (SVC)

El SVC en X.25 es similar a una llamada de voz. Supongamos que A, B, C, y D son nodos terminales en una red X.25; la nube contiene conmutadores X.25. Para establecerse una llamada se da lo siguiente:

1.- A genera una solicitud de llamada dirigida a D.

2.- Dado que A es una estación con un solo puerto a la red de X.25, envía la solicitud de llamada a un conmutador en la nube.

3.- El conmutador en la nube observa la dirección en la solicitud de llamada y la correlaciona en una su tabla de ruteo, transmite la solicitud de llamada al siguiente conmutador, y registra el puerto a través del cual viajó la solicitud.

4.- El siguiente conmutador repite el paso 3.

5.- En algún punto, uno de los conmutadores en la nube entrega la solicitud de llamada directamente a D.
6.- Cuando D recibe la solicitud de llamada, la acepta mediante el envío de una señal de llamada aceptada que viaja de regreso al conmutador que recibió la solicitud.
7.- Dado que los conmutadores registraron la ruta y la solicitud de llamada, simplemente envían la señal de aceptación de llamada de regreso por el mismo camino.
8.- Una vez que A recibe la señal de llamada aceptada, se establece un SVC y comienza la transferencia de datos.
9.- Tanto A como D pueden terminar la llamada en cualquier momento, terminando así el SVC.

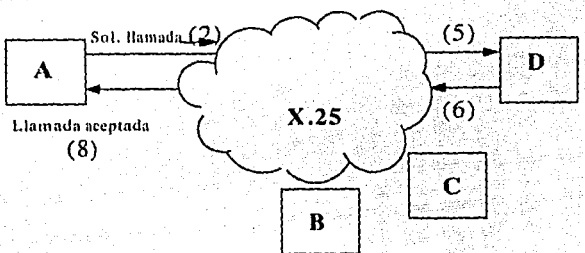


Figura 1.34 Circuitos Virtuales Conmutados en X.25.

1.3.2.2 Circuitos Virtuales Multiplexados

Estos circuitos se dan cuando una estación tiene más de un circuito virtual entre la estación y el conmutador con el cual se está comunicando a la nube. Esto permite que se puedan tener múltiples circuitos establecidos con diferentes destinos.

1.3.2.3 Circuito Virtual Permanente

A diferencia de los SVC que se establecen por la demanda de una solicitud de llamada, los PVC entre los nodos terminales de X.25 están siempre presentes. Para lograr esto, el administrador de la red tiene que asignar la ruta para cada PVC en cada conmutador. Dado que los PVC tienen más configuraciones, los diseñadres de redes procuran evitarlo, pero las aplicaciones que requieren conexiones de tiempo completo pueden utilizarlos.

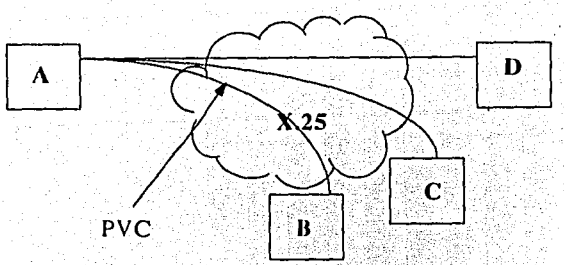


Figura 1.35. Circuito Virtual Permanente en X.25.

1.3.2.4 X.25 y el Modelo OSI

La norma X.25 definida por el CCITT se deriva directamente del modelo OSI de la ISO. En efecto ISO específicamente hace referencia a las normas CCITT para algunas capas inferiores.

La norma define las siguientes capas:

Capa de Paquetes (X.25). Se relaciona directamente con la Capa de Red. Esta capa define el direccionamiento de la Red desde el punto inicial hasta el destino de los datos. A diferencia de los protocolos de Capa 3 diseñados para LAN, la Capa de Paquetes está orientada a conexión y hace énfasis en la secuencia.

Capa de Tramas (LAPB). Corresponde con la Capa de Enlace de Datos. Esta capa provee el enlace, control, secuencia y recuperación de errores.

Capa Física (X.21, X.21 bis). Describen los requerimientos eléctricos para accesar al medio físico.

1.3.2.4.1 X.25 en la Capa 1

La recomendación original de X.25 en la Capa 1 era X.21. Esta norma define la señalización de control y características eléctricas para acceso a un adaptador de terminal TA para una red de servicios digitales integrados (ISDN). Desde que ISDN tuvo gran aceptación, el CCITT definió más tarde el X.21 bis como la norma de Capa 1 recomendada. La especificación X.21 bis incluye las normas V.24 (RS-232) y V.35 como las más ampliamente aceptadas por la mayoría de los modems y unidades de Servicio Digital (DSU).

1.3.2.4.2 X.25 en la Capa 2

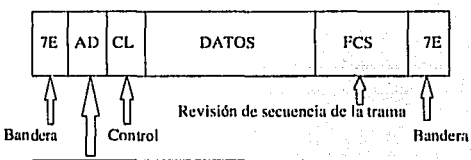
La recomendación de X.25 en la Capa 2 da a escoger dos procedimientos: El Procedimiento de Acceso de Enlace (LAP) y el Proceso de Enlace Balanceado (LAPB). En la práctica LAPB se ha convertido en la norma de facto.

El Procedimiento LAPB es un derivado del control de enlace de datos de alto nivel (HDLC).

El Procedimiento LAPB provee una relación balanceada entre dos dispositivos X.25. Esta relación permite a cada dispositivo mandar comandos o respuestas como se requiera en un ambiente de conmutación.

1.3.2.4.3 Formato de las tramas X.25

El formato para la trama del protocolo LAPB es el siguiente:
El Campo de Bandera es de 8 bit representado por el hexadecimal 7E, indica inicio o fin de cada trama. Algunos equipos pueden usar opcionalmente el campo de bandera para representar una condición de estado reposo.
El campo de dirección es de 8 bits e indica que dispositivo DCE/DTE originó la trama. Mientras que LAPB provee una comunicación punto a punto, uno debe de configurar un lado como capa 2 DTE y el otro lado como capa 2 DCE. La dirección está contenida en este campo depende del dispositivo que la mandó y si la trama contiene un comando o una respuesta.
El Campo de Control está formado por 8 o 16 bits y describe el tipo de trama.
El Campo de Datos contiene paquetes de información de capa 3, así como datos de usuario.
El Campo de Validación de Secuencia de la Trama es una suma de validación de 16 bits que asegura que se reciba íntegra toda la trama.



Dirección	Comando	Respuesta
DTE	01	03
DCE	03	01

Figura 1.36. Formato de la trama de X.25.

1.3.2.4.4 Tipos de Tramas

El protocolo LAPB define tres tipos de tramas. Éstas incluyen:
Tramas No Numeradas que proveen el establecimiento de enlace, desconexión y mantenimiento. Dado que estas tramas no son secuenciales, se les llama no numeradas.
Tramas de Información que permiten transferencia de datos de manera secuencial.
Tramas de Supervisión que aseguran el control de flujo ordenado y recuperación de errores.

1.3.2.5 X.25 en la Capa 3

La capa de paquetes en X.25 define los requerimientos de direccionamiento de punta a punta, establecimiento de la llamada, también como la secuencia.
Las direcciones usadas en X.25 proveen la información necesaria para ruteo de punta a punta. La recomendación X.121 describe los detalles de cómo esta capa 3 hace el direccionamiento.
Una dirección de X.121 tiene 14 dígitos; esto es llamado el Número de Datos Internacional (IDN). Los primeros cuatro dígitos describen el Código de Identificación de la Red de Datos (DNIC). Los tres primeros dígitos describen el país. El cuarto dígito describe el número de la red dentro del descrito país.
Los 10 dígitos restantes en la dirección X.121 describen el Número de Terminal Nacional.
Dos redes públicas de datos (PDN) pueden conectarse entre sí a través de una conexión X.75. La especificación X.75 simplemente define el procedimiento para interconexión de PDNs.

1.3.2.5.1 Formato de los paquetes X.25

Esta información está a continuación del campo de control de la capa 2. Los campos contenidos en el formato de los paquetes son los siguientes:
El Identificador de Formato General (GFI) describe los requerimientos de secuencia para el paquete. Utiliza cuatro bits.
El primer bit, llamado Q, identifica que los paquetes contengan información para el dispositivo de Ensamble/Desensamble de Paquetes Asíncrono (PAD).
El segundo bit, llamado D, es el que llama al Reconocimiento (ACK) desde la estación origen a la destino.
Los siguientes 2 bits se llaman Número de secuencia, y describen el número de secuencia utilizado en esta conexión. Puede ser módulo 8, para paquetes numerados del 0 al 7; y módulo 128 para paquetes numerados de 0 a 127.
El Identificador Lógico del Canal (LCI) identifica de manera única un canal lógico en 12 bits, entre dos estaciones sobre un circuito físico específico.
El Identificador de Tipo de Paquete define el tipo de paquete. Por ejemplo:
Solicitud de llamada, Llamada aceptada, Solicitud de desconexión, etcétera.

1.3.2.6 Transferencia de datos

Una vez que dos DTE se han puesto de acuerdo para comunicarse a través de la rutina de establecimiento de la conexión, que se explicó anteriormente, comienza la transferencia de datos. Durante la transferencia de datos, el dispositivo receptor provee reconocimiento de un paquete en particular.
El protocolo LAPB provee el control de flujo en la capa 2; esto permite a un dispositivo parar al dispositivo que envía cuando sus unidades de almacenamiento intermedio están llenas. La capa 3 provee una facilidad similar para cada conexión lógica que corre sobre la capa física. Como el protocolo de la capa 2, X.25 en la capa 3 usa paquetes Receptor no Listo (RNR) para completar este procedimiento.
Si un paquete se perdiera o llegara fuera de orden, la capa 3 usa un REJ para informar al que envía que retransmita.

Cuando una transmisión termina, cualquier DTE puede limpiar la llamada. La solicitud de limpiado de llamada se propaga hasta el otro lado de la conexión. El DTE recibe el indicador de limpiado y responde con una confirmación de limpiado, la cual regresa a través de la red al DTE que originó la solicitud de limpiado.

1.3.3 Frame Relay

1.3.3.1 Antecedentes

Frame Relay es una solución para WAN que permite interconectar LANs remotas.
Típicamente, los servicios de Frame Relay se obtienen de un proveedor público que posee el troncal o backbone de la red. Algunas compañías grandes poseen su propia red privada de Frame Relay.
Las especificaciones de Frame Relay definen:

- La interconexión de un DTE a un DCE.
- Un formato de trama establecido para transmisión de datos.
- El proceso para encapsulado multiprotocolo.
- La administración del enlace y la integridad.

Frame Relay provee ancho de banda dinámico el cual soporta tráfico intempestivo de la LAN, si se requiere más ancho de banda por una aplicación o servicio, puede ser proporcionado más ancho de banda adicional mientras no ocurra una congestión.
Frame Relay es también una interface de paquetes multiplexados. Dado que utiliza circuitos virtuales para establecer conexiones de lado a lado de la red, el DTE y el DCE son capaces de multiplexar varias conexiones sobre un medio común.
El formato de la trama está basado en el LAPD la cual define el nivel básico de la trama para transmisión y recepción.
Algunos de los beneficios que Frame Relay provee es el ancho de banda asociado con las líneas privadas pero con las ventajas de costo y flexibilidad asociado con la conmutación de paquetes de X.25.

1.3.3.2 Características de Frame Relay

Frame Relay es una tecnología de conmutación de paquetes, permitiendo que los conmutadores conmuten tramas a múltiples destinos desde una sola línea de acceso. Las características de interface son:

- Velocidad moderada de acceso de línea.
- Longitud variable de la trama.
- Sin revisión de errores entre conmutadores.
- Sin retransmisión de datos.

Frame Relay es un servicio orientado a conexión, definido por su uso de uno o más circuitos virtuales que prevén conexiones punto a punto a través de la malla o nube. El uso de circuitos virtuales es garantía de que las tramas llegarán en secuencia.
Esto ocurre porque todas las tramas de una conexión específica siguen la misma ruta desde el origen hasta el destino. En consecuencia, a diferencia de otros protocolos basados en transporte, el control de secuenciación no se requiere dentro del Frame Relay. Frame Relay también desempeña el mejor servicio de entrega. Sólo garantiza la conmutación de tramas adecuadas a su siguiente destino. Si recibe una trama con error en

la suma de verificación (Checksum) o se encuentra involucrada en una congestión de red, la trama será rechazada, y no habrá solicitud de retransmisión automática enviada de regreso al origen, por lo que la responsabilidad de una capa superior de protocolo en el origen es identificar que su paquete de información no fue reconocido, y que lo tendrá que retransmitir nuevamente.
Un aspecto importante de Frame Relay es su habilidad para identificar congestiones y notificar a los sistemas terminales (DTE) de esa condición.
La integridad de la administración de enlace permite a los dispositivos de la red identificar la condición y estado de acceso de la línea ofreciendo un muestreo de rutina.

1.3.3.3 Frame Relay y el modelo OSI

Opera dentro de la capa 1, 2 y 3 del modelo OSI.
La capa 2, enlace de datos, permite la transmisión y recepción de unidades de datos de protocolo (PDU) del origen de un DTE a un destino de DTE a través de la red conmutada.
Algunos de los componentes involucrados en esta capa son:

Las tramas LAPD.
Direccionamiento de circuitos virtuales.
Revisión de errores de encabezado para asegurar la integridad de la trama.

La capa 1, física, permite la transmisión y recepción de datos desde el DTE origen a la red de conmutación. La capa física define la interface física y eléctrica, consideraciones de tiempo, así como otros componentes involucrados en el acceso de la conexión de la línea:

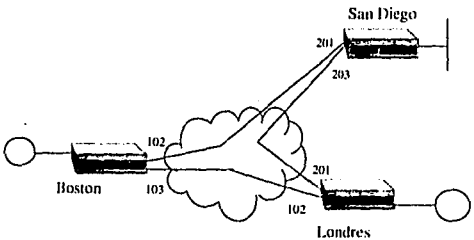
Cableado
- V.35
- RS-449
- HSSI

DSU/CSU
Línea Privada

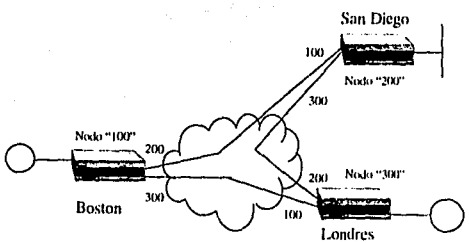
1.3.3.4 Circuitos Virtuales Permanentes

Un circuito virtual está definido como el camino a través de una red común. En Frame Relay, los circuitos virtuales se implementan estáticamente.
La gran mayoría de las aplicaciones de red que soportan circuitos virtuales inicialmente soportan conexiones estáticas o circuitos virtuales permanente (PVC).
Una PVC es creada por el proveedor de red como una interface que está configurada. Los puntos terminales del PVC son configurados estáticamente por el proveedor de la red.
Por tanto un PVC requiere recursos de red para ser previamente localizado para soportar la conexión. Como resultado, el PVC deberá estar siempre disponible para los sistemas terminales a menos de que ocurra una falla a través de la ruta.
Cada PVC está identificado por una dirección única, llamada Identificador de Conexión de Enlace de Datos. (DLCI), la cual es única para cada PVC en uso, sin embargo es sólo localmente importante entre el DTE local y el DCE. Por esto, cada DLCI puede ser reutilizado de enlace a enlace.

Típicamente las direcciones de Frame Relay y sus asignaciones son llamadas direcciones locales, porque son exclusivas únicamente para la línea de acceso local.
En algunas configuraciones de red se prefiere que un mismo sitio remoto sea identificado por los demás sitios remotos por medio del mismo DLCI. Aunque este diseño limita la disponibilidad de direccionamiento, simplifica la configuración general de la red. Este procedimiento es conocido como direccionamiento global.



Direccionamiento local (Unicast PVC'S)



Direccionamiento global (Unicast PVC's)

Figura 1.37. Direccionamiento local y global en Frame Relay.

1.3.3.5 Ancho de Banda Asignado

Dentro de cada línea de acceso, pueden ser configurados múltiples PVC. Para garantizar el desempeño de cada PVC, a cada uno de los PVC se le asigna un ancho de banda

específico, conocido como CIR (Committed Information Rate). El CIR del PVC garantiza que un PVC específico utilice una cantidad de ancho de banda determinado para su conexión.
El CIR está fijado desde el establecimiento de la línea de acceso. Un CIR no puede exceder el ancho de banda de la línea dedicada de acceso. Típicamente el CIR es mucho menor que el ancho de banda de la línea de acceso.
Para soportar los picos de tráfico en LAN, que se encuentren por encima del CIR, cada PVC tiene la habilidad de exceder su CIR, si esto ocurre la red no garantiza la entrega de estos paquetes, por lo que los paquetes pueden no llegar a su destino.

1.3.3.6 Estructura de la Trama y Campos

Las direcciones en Frame Relay son de 2, 3 o 4 bytes de longitud.
El campo Identificador de conexión de Enlace de datos (DLCI).
El tamaño del DLCI está basado en la longitud de la dirección. Identifica el canal o circuito virtual que se está utilizando.
Valida que la dirección de 2 bytes, en esté caso, este dentro del rango permitido, que es de 16 a 1007. Las demás comprendidas entre 0 a15 y 1008 a 1024 están reservadas para efectos de administración y direccionamiento múltiple.
El campo Direccionamiento Extendido (EA) es el bit que determina la terminación del formato de dirección de 2, 3 o 4 bytes; donde 0 indica que la dirección continua o 1 que indica que es el final de la dirección.
El campo Notificación de Congestión Explícita hacia Adelante (FECN).
Puede ser fijada por el conmutador de Frame Relay cuando ocurre una congestión. Cuando es puesta en 1 notifica a los nodos siguientes que ocurrió una congestión.
El campo Notificación de Congestión Explícita hacia Atrás (BECN).
Se fija de igual forma que el anterior, sólo que en este caso es para notificar a los nodos anteriores que ocurrió una congestión.
El campo Elegible para desecho provee una identificación de las tramas que son desechables si ocurre una congestión. Puede ser fijada tanto por el conmutador de Frame Relay como por los puentes o ruteadores que intervengan.
0 indica tráfico con prioridad, no es desechable; 1 indica tráfico sin prioridad, es desechable.
Si una congestión ocurre y se deben desechar tramas, las tramas sin prioridad serán las primeras que se desecharán.
El campo Comando/Respuesta (C/R) no es usado dentro de la red de Frame Relay, es transparentemente relevado de conmutador en conmutador. Este campo es fijado por el equipo DTE..

1.3.3.7 Encapsulamiento Multiprotocolo

Como un proceso de transmisión de unidades de datos de protocolos (PDU) a través de la red de Frame Relay, es responsabilidad del equipo DTE de Frame Relay encapsular cada PDU con la información de encabezado de Frame Relay que corresponda.
Como una aplicación de usuario es enviada a la interface de Frame Relay, el DTE debe identificar el tipo de datos que está contenido dentro del paquete. La solicitud de comentario (Request for Comment) o RFC 1490 define el procedimiento para el

encapsulamiento multiprotocolo. La implementación de la RFC 1490 asegura la interoperabilidad entre diferentes fabricantes.
En el encapsulamiento multiprotocolo se agrega al PDU con un encabezado que es similar en función al campo "Tipo" de la trama Ethernet versión 2.0. El encabezado identifica al DTE receptor el tipo de PDU que está contenido dentro del paquete permitiendo que el receptor sepa cómo procesar ese paquete que llega.
La RFC 1490 define el proceso de encapsulamiento para la interconexión de múltiples protocolos sobre una red de Frame Relay y así mismo el uso de un campo de Identificación de Protocolo a nivel de Red (NLPID) para el encapsulamiento de PDUs.
Los diferentes protocolos definidos por la RFC son:

Protocolo Internet: IP
Open System Interconneect: OSI
Protocolos de Acceso a la Subred: SNAP
- Appletalk

Banyan VINES
Bridging
DECnet Phase IV
Novell IPX
XNS

Proceso de Encapsulamiento de Multiprotocolos

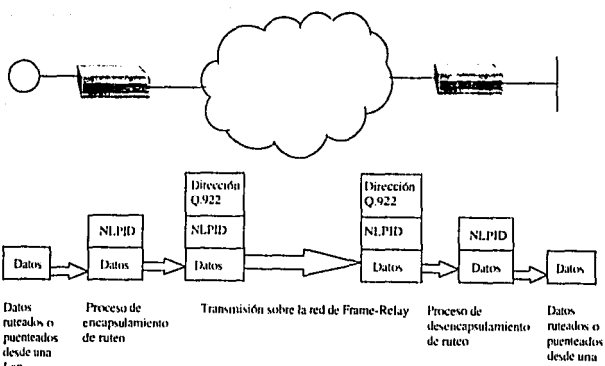


Figura 1.38. Proceso de encapsulamiento multiprotocolos.

1.3.3.7.1 Encapsulación NLPID

El NLPID es usado para protocolos normalizados Internet. Tiene dos bytes de longitud y es agregado al principio del PDU ruteado o puenteado. El encabezado Frame Relay es entonces agregado al principio del NLPID.
Los NLPIDs son administrados por el ISO y CCITT, los valores asignados para los diferentes tipos de encapsulación multiprotocolo son:

IP 0XCC
SNAP 0X80

Finalmente, el campo "Control" es fijado siempre en 0X03. Este valor es utilizado por todos los fabricantes.
Donde X puede tomar cualquier valor.

1.3.3.7.2 Encapsulamiento SNAP

SNAP es usado por los demás protocolos no asignados antes mencionados.
El encabezado SNAP agrega tres nuevos campos que el NLPID no contiene. Los campos adicionales permiten identificar el PDU dentro del paquete.
Como con el NLPID, el SNAP también empieza con un campo de Control el cual siempre está fijo en 0X03.
En seguida viene un PAD de 0X00, el cual es usado para alineación.
El Campo NLPID entonces muestra que éste es un PDU SNAP, 0X80.
Entonces dos nuevos campos son creados, estos nuevos campos permiten al receptor identificar los diferentes PDUs asignados a la encapsulación SNAP, dichos campos son:

El Identificador Único Organizacional (OUI). Identifica las organizaciones administrativas como por ejemplo: XNS/IPX, Appletalk, etc.
El Identificador de Protocolo (PID) únicamente identifica el protocolo. Por ejemplo: Novell IPX, 802.3 Bridging, Appletalk, etc.

1.3.4 Protocolo de Conmutación de Enlace de Datos (DLSw)

1.3.4.1 Antecedentes

DLSw es un protocolo propietario desarrollado por IBM con el fin de permitir la comunicación, a través de una LAN puenteada, entre dispositivos que manejan protocolos tales como NetBIOS, SNA y SDLC, simulando estar conectados directamente a un procesador de punto inicial (FEP).
DLSw es un protocolo de envío de tramas para dispositivos que se comunican por medio de protocolos específicos de IBM mencionados anteriormente. Dado que estos dispositivos utilizan la LLC2 de la IEEE802.2 para comunicarse, DLSw deberá interpretar este protocolo, el cual deberá ofrecer los siguientes servicios:
Conectividad (a través de una interconexión de red TCP/IP) entre dispositivos SNA o estaciones de NetBIOS.
Emplear mecanismos de control de flujo a nivel de la LLC2 para eliminar la terminación de enlace de datos debido al tiempo fuera de sesiones cortas.
Permitir la configuración de redes de ruteo de origen, que incluyen más de 7 saltos a lo largo de la ruta seguida.

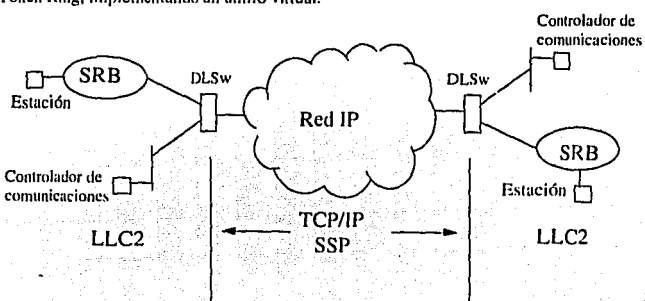
Conjuntar las direcciones de SNA y NetBIOS y utilizarlas en su momento, para optimizar la ruta de envío y reducir la cantidad de tráfico sobre la red TCP/IP.

1.3.4.2 Características de DLSw

Es un protocolo orientado a conexión.
Termina la sesión localmente, limitando los tiempos fuera de la misma y previniendo que las señales de conmutadores de recepción (RR's) atraviesen la red innecesariamente.
Ofrece una manera confiable de entrega de datos utilizando TCP.
Opera sobre cualquier circuito que soporte IP.

1.3.4.3 Dispositivos de redes utilizados por DLSw

DLSw requiere la utilización de cuatro dispositivos de red:
1. Enrutamiento de origen por puenteo:
Captura de tramas que requieran del protocolo de DLSw, para entrega o descubrimiento de rutas sobre la red TCP/IP.
Envío de tramas a redes Token Ring conectadas localmente.
2. LLC2:
Inicia sesiones a estaciones terminales, tanto locales como remotas.
Termina sesiones locales para prevenir tiempos fuera.
Previene el flujo de tráfico que no contiene información.
3. Servicios TCP/IP.
Asegura la entrega confiable de tramas de datos entre dispositivos similares a DLSw conectados a la misma red IP.
Descubre las rutas entre dispositivos similares o equivalentes a DLSw.
Permite que DLSw aparezca como una extensión de ruteo de origen del testigo de una red Token Ring, implementando un anillo virtual.



1.3.4.4 Protocolo entre conmutadores (SSP)

Es un protocolo entre conmutadores, definido por la RFC 1434 para comunicación entre conmutadores de red IBM 6611 para permitirle al protocolo DLSw terminar con sesiones locales sin perder conectividad remota y permitir el control de flujo y congestión de trafico en la red TCP/IP .
DLSw utiliza SSP para:
Desarrollar un mapeo de formatos de mensajes de tramas entre LLC2 y SSP.
Establecer, reinicializar o interrumpir cualquier circuito entre el DLSw local y cualquier dispositivo similar remoto.
Construye sus tablas de enrutamiento MAC automáticamente en el ruteador mediante la difusión de transmisiones desde estaciones terminales locales y estaciones terminales remotas .

1.3.5 Protocolo Punto a Punto o PPP

1.3.5.1 Antecedentes

Es un método común de encapsulamiento para protocolos entre enlaces punto a punto con la ventaja que permite utilizar cualquier dispositivo de interconexión, como ruteadores y computadoras, sin importar la marca o fabricante. Este tipo de protocolo nació de la imposibilidad que tuvo HDLC para cubrir las expectativas esperadas.
PPP es un protocolo de enlace de datos que permite la negociación en la capa tres del modelo OSI, con la capacidad de ofrecer un monitoreo sobre la calidad de enlace,siendo esta como su característica más importante. PPP es considerado también como una norma para el envío de información sobre las interfaces DTE/DCE como V35, T1, E1. Contiene además medidas de seguridad que evitan acceso sin autorización.
La estructura de este protocolo está contenida en el documento RFC 1311, al cual se le asocian otros documentos RFC que muestran como encapsular protocolos de capas superiores.
1332 PPP Internet Protocol Control Protocol (IPCP)
1333 PPP Link Quality Monitoring (LQM)
1334 PPP Authentication Protocols (PAP)
1336 PPP DECnet IV Protocol Control Protocol (DNCP)
1377 PPP OSI Network Layer Control Protocol (OSINLCP)
1378 PPP Apple TALK Control Protocol (ATCP)
1362 PPP Internet Packet Exchange Control Protocol (IPXCP)
PPP es full duplex y puede ser dedicado o conmutado por circuito. Se basa en HDLC, que es el más ampliamente usado en protocolos de enlace de datos síncronos.
HDLC fue creado para ser el protocolo que terminaría con todos los protocolos propietarios de los fabricantes , siendo la intención de que realizara el trabajo que actualmente PPP está destinado a realizar. Debido a sus múltiples características y posibilidades, una gran cantidad de implementaciones se han realizado, sin embargo, como el esquema de direccionamiento no fue lo suficientemente rígido, muchos fabricantes aprovecharon esta situación para fijar sus propios parámetros, resultando en una deficiente intercomunicación entre los productos de los diferentes fabricantes. HDLC

está orientado hacia manejo de bits y es el fundamento para la gran mayoría de protocolos WAN.

1.3.5.2 Familia de Protocolos HDLC

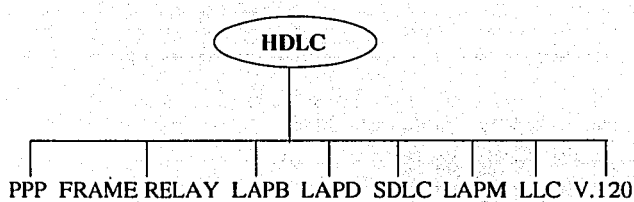


Figura 1.39. Familia de protocolos derivados de HDLC.

- **LAP B** usado para **X.25**
- **LAP D** usado para **ISDN**
- **SDLC** usado en ambiente **SNA**
- **LAPM** provee la posibilidad de **HDLC** a modems **V.24**
- **V120** es una recomendación **CCITT** para usar **ISDN** en adaptadores de terminal

1.2.4.2.1 La Trama HDLC

Bandera	Dirección	Control	Informacion	FCS	Bandera

Figura 1.40 La trama HDLC.

Bandera. Estas indican el inicio o fin de la trama.
Dirección. Identifica las estaciones involucradas con la transmisión y recepción de la trama.
Control. Este campo contiene los comandos, respuestas y secuencia de números, así como indicar tres tipos de tramas.
Información. Contiene los datos del usuario.
FCS. Es una trama de 16 bits y cuyo campo realiza una revisión secuencial.
La bandera de cierre de una trama puede servir como la bandera de apertura de la siguiente trama.
HDLC no define una forma normalizada de aplicar las tramas en la capa de protocolos de la red, pero PPP logra esto mediante su rigidez en la que emplea las partes especificas de la trama. Para que una comunicación se lleve a cabo eficientemente sobre PPP, dos

protocolos tienen que estar bien definidos. Estos protocolos son usados para la negociaciones de la línea y las opciones de la capa de red:
Protocolo de Control de enlace (LCP)
Protocolo de Control de la Red (NCP)
LCP es usado para la apertura, configuración y ruptura de la comunicación del enlace de datos, mientras que NCP se encarga de la apertura, comunicación, y cierre la capa de protocolo de comunicaciones de la red.
Como se mencionó anteriormente, la trama PPP está basada en la trama HDLC. Esta sin embargo modificada ligeramente. El esquema de direccionamiento utilizado en PPP, así como el valor utilizado en el campo de control son muy rígidos y específicos, esto ha forzado a los fabricantes a seguir un lineamiento específico en la identificación de estaciones.
Con esto, los problemas que se encontraron en HDLC son eliminados.

1.3.5.3 La Trama PPP

Bandera	Dirección	Control	Protocolo	Información	FCS	Bandera
8 bits	8 bits	8 bits	16 bits	Variable	16 bits	8 bits

Figura 1.41. La trama de PPP.

Las diferencias entre esta trama y la de HDLC son:
El campo de dirección siempre tiene un valor de FF.
El campo de control tiene un valor de 03.
Un campo adicional es añadido justamente después del campo de control para indicar que el protocolo está encapsulado en una trama PPP.
El campo de protocolo indica valores tanto para LCP y NCP.
Todos los valores en el campo de protocolos deberán tener números impares.
Antes de que el enlace PPP pueda ser usado debe existir una negociación entre ambos lados del enlace.
El estado del enlace será reflejado por diferentes códigos contenidos en el campo de información. Mediante el uso de estos valores en este campo las estaciones que se comunican pueden informarse del éxito o del fracaso a medida que se alcanzan las diferentes fases. Existen cuatro fases involucradas en el comienzo de un enlace PPP:
Negociación LCP
Estado estable LCP
Comienzo de Protocolos de alto nivel
Flujo normal de datos en protocolos de alto nivel.

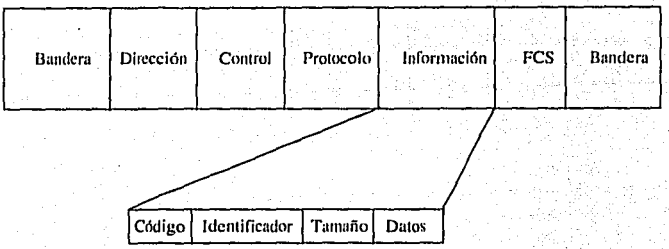


Figura 1.42. Trama PPP, con el campo de información detallado.

1.3.5.4 Sincronización de Enlaces PPP

Ningún protocolo de capa de red puede utilizar el enlace PPP sin que se alcance el paso más importante, este paso inicial es el de la fase del Protocolo de Control de Enlace, LCP.

Tres tipos de paquetes son utilizados en este paso:

Paquetes de establecimiento de enlaces.

Paquetes de mantenimiento de enlaces.

Paquetes de terminación de enlaces.

Todos los enlaces comienzan y terminan con lo que se conoce como fase muerta . Esta es una fase que indica que la capa física no se encuentra lista.

LCP tiene la responsabilidad de hacer que dos sistemas se comuniquen entre si. Durante la fase inicial entablarán una discusión acerca del tipo de paquetes que intercambiarán, posteriormente, LCP establecerá que tipo de protocolos de alto nivel deberán ser usados en el enlace. Si este es exitoso, la capa de protocolos de red podrá comenzar a utilizar el enlace.

La función de LCP continuará hasta el momento en el que se presente la fase de ruptura de enlace. LCP cumple también la tarea de monitorear la calidad del enlace.

Si esta calidad no cumple con una serie de parámetros establecidos, LCP comenzará la fase de ruptura del enlace.

Existe una fase opcional de Autenticidad que puede establecerse para el enlace. Esta fase utiliza el Protocolo de Autenticidad de Contraseña (PAP), que es un intercambio de combinaciones de textos y contraseñas.

Los paquetes LCP son cargados en el campo de información de la trama, existiendo cuatro tipos:

Petición de Configuración. (Configure-Request)

Configuración de Reconocimiento. (Configure-Ack)

Configuración de No Reconocimiento (Configure-Nack)

Configuración de Rechazo, (Configure Reject)

1.4 Comparación entre los diferentes tipos de redes

En la figura 1.43 se muestra un cuadro comparativo de las diferentes características de las redes más comunes.

	Circuito Síncrono	X.25	Frame Relay	Ethernet	Token Ring	FDDI	ATM
Trama Longitud	Rígido Fijo	Rígido Fijo	Flexible Variable	Flexible Variable	Flexible Variable	Flexible Variable	Rígido Fijo
Capacidad de ancho de banda	<45 Mbps	<64 Kbps	<2 Mbps	10 Mbps	4/16 Mbps	100 Mbps	< 2.5 Gbps
Latencia	Baja	Alta	Media	Baja	Baja	Baja	Baja
Canal Uso	Físico Dedicado	Múltiple Virtual	Múltiple Dedicado	Común Compartido	Común Compartido	Común Compartido	Múltiple Virtual
Tipo de conexión	Remoto	Remoto	Remoto	Local	Local	Local y Campus	Local y Remoto
Medio	Cobre Fibra Inalámbrico	Cobre	Cobre	Cobre Fibra Inalámbrico	Cobre Fibra	Fibra Cobre	Fibra Cobre
Servicios soportados	Voz Video Datos	Datos	Datos	Datos	Datos	Datos	Voz Video Datos
Costo	Bajo a Alto	Bajo a Medio	Bajo a Medio	Bajo	Bajo	Medio	Medio a Alto

Figura 1.43. Cuadro comparativo de características entre redes más comunes.

CAPÍTULO II

INTEGRACION LAN-WAN

CAPÍTULO II

INTEGRACIÓN LAN-WAN

2.1 Antecedentes de equipo de conexión

Las WANs se pueden conectar usando diferentes medios, algunos de ellos son:

Redes privadas o publicas con:
- Fibra óptica.
- Enlaces de microondas
- Cable coaxial
- Satélite
- O combinaciones de los anteriores.

Conectividad con portadoras comunes y/o redes de valor agregado.
Conectividad con enlaces de telefonía pública o servicios de ISDN.
Obviamente el tipo de conectividad depende de la aplicación de datos a servir y de los recursos económicos con que se cuente.
Hoy en día la tecnología ha producido una gran variedad de herramientas para crear las soluciones de interconectividad, las cuales incluyen puentes, ruteadores, repetidores y compuertas (Gateways).
Las tecnologías de conexión a analizar en el presente capitulo son conexiones por repetidores, puentes (Bridges), por conmutación (Switches), Ruteadores (Router), traducción por puenteo (Translation Bridges), puentes de encapsulamiento (Encapsulation Bridges) y puente por ruteo de origen (Source Route Bridges).

2.2 Protocolos de comunicación

Los protocolos de comunicación son formatos convencionales para transmisión entre dos dispositivos de comunicaciones. Los protocolos pueden existir en varios niveles de una red como en enlace a enlace, o usuario a conmutador.
Entre los protocolos de comunicación que dominan en el mercado tenemos TCP/IP, XNS, IPX, Appletalk, VINES Y SNA.
A continuación se presenta una breve explicación de las características de cada uno de ellos.

TCP/IP (*Transmission Control Protocol / Internet Protocol*) Protocolo de control y transmisión y protocolo de interconexión de redes. Desarrollado por el Departamento de Defensa de los Estados Unidos. Actualmente tiene una gran aplicación y éxito en los mercados internacionales, aunque no esta conforme al modelo OSI muchos usuarios lo han encontrado como una forma madura y tangible para efectuar conectividad de equipo de varios vendedores, así se adelantan a la conectividad en tanto se disponga de los productos en base a OSI.
TCP/IP a diferencia de OSI consiste de cuatro capas jerárquicas a saber:

CAPA 4	APLICACIÓN
CAPA 3	TRANSPORTE

CAPA 2	INTERCONEXIÓN
CAPA 1	INTERFACE DE RED

CAPA 1 Enruta los datos entre los dispositivos de la misma red. Esta interface en TCP/IP equivaldría a las capas 1 y 2 de OSI.

CAPA 2 Maneja el intercambio de datos entre dispositivos conectados a redes diferentes. Como en OSI el IP añade la función de direccionamiento en la red.

CAPA 3 La capa de transporte es la encargada de proveer la conexión de los datos de origen a destino entre las fuentes de datos. Esta es equivalente a la capa de transporte de OSI.

CAPA 4 Maneja las funciones de usuario requeridas para los programas. Esta corresponde a las 3 capas superiores del modelo OSI.

XNS (*Xerox Network Services Internet Transport Protocol*) Este es un protocolo desarrollado por Xerox para interconectividad y transporte en redes Ethernet. Consta de cinco capas jerárquicas únicamente:

CAPA 4	APLICACIÓN
CAPA 3	CONTROL
CAPA 2	TRANSPORTE
CAPA 1	INTERCONEXIÓN
CAPA 0	MEDIO DE TRANSMISIÓN

CAPA 0 Esta maneja el intercambio de datos entre un dispositivo y la red a la cual esta conectado. Esta capa en XNS es equivalente a las capas 1 y 2 de OSI.

CAPA 1 Maneja el intercambio de datos entre dispositivos conectados a redes diferentes. Este nivel define la forma en que se entregan los datos a través de la red. Corresponde a la capa de interconexión de TCP/IP y de OSI.

CAPA 2 La capa de transporte es la encargada de proveer la conexión de los datos de origen a destino entre las fuentes de datos. Esta es equivalente a la capa de transporte de OSI

CAPA 3 Se encarga de la presentación de los datos y del control de los recursos de los dispositivos. Este nivel correspondería a las capas de sesión y presentación de OSI.

CAPA 4 Maneja la semántica de los datos, es decir el significado de los programas. Esta corresponde a la última capa del modelo OSI.
Del XNS se derivan varios otros protocolos propietarios, el más conocido y empleado es quizá el protocolo de intercambio de paquetes en interconectividad de Novell, comúnmente conocido como IPX.

IPX Este protocolo es definido por Novell como un "Servicio" y provee aplicaciones con la posibilidad de enviar y recibir mensajes a través de una red. En varias formas es idéntico a XNS y esta basado en las mismas cinco capas, pero este permite ciertas funciones de valor agregado como es el Protocolo de

Servicio de Aviso, el cual permite a los servidores de una red transmitir su identidad e identificar los servicios ofrecidos a través de la red.

Appletalk Este provee la conectividad entre computadoras Macintosh. No maneja restricciones en cuanto al tamaño de la red, y puede soportar Ethernet y Token Ring. Este protocolo es prácticamente igual a OSI pero difiere en que combina las últimas dos capas en una sola.

VINES (*Virtual Networking System*) Sistema de redes virtuales. Se basa en UNIX y permite a las estaciones de trabajo disponer de un ambiente transparente para compartir recursos distribuidos en la red. La arquitectura de este protocolo refleja perfectamente el modelo OSI de 7 capas.
Este protocolo soporta varios estándares de IEEE como Ethernet y Token Ring y la serie 802.x, además de manejar su enlace propietario.
Soporta los estándares de la industria de X.25, TCP/IP y Appletalk.

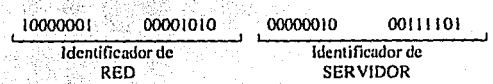
SNA IBM desarrolló este protocolo de Arquitectura de Sistemas de Redes, inicialmente para acceso remoto de grandes computadoras (Mainframes) el SNA (Systems Network Architecture) sigue evolucionando y lo mismo que OSI consta de 7 capas:

CAPA 7	SERVICIOS DE TRANSACCIÓN
CAPA 6	PRESENTACIÓN DE SERVICIOS
CAPA 5	CONTROL DE FLUJO DE DATOS
CAPA 4	CONTROL DE TRANSMISIÓN
CAPA 3	CONTROL DE RUTAS
CAPA 2	CONTROL DE ENLACE DE DATOS
CAPA 1	CONTROL FÍSICO

CONTROL FÍSICO: Describe la conexión entre dispositivos adyacentes.
CONTROL DE ENLACE: Trata de la transmisión entre equipos dentro de la misma red.
CONTROL DE RUTAS: Esta establece la conexión lógica en el mensaje entre el origen y el destino. A diferencia de OSI, en SNA no se cuenta con funciones de direccionamiento por lo cual el tráfico es puenteado y no existe posibilidad de enrutamiento.
CONTROL DE TRANSMISIONES: Esta capa es el equivalente a la capa de transporte del modelo OSI. Dentro de SNA esta capa es la responsable por establecer y mantener la sesión entre los dos dispositivos, fuente y destino.
CONTROL DE FLUJO DE DATOS: Equivalente a la capa cinco en OSI.
PRESENTACIÓN DE SERVICIOS: Describe los servicios orientados y como se presentan para conversión de datos, encripción y compresión.
SERVICIOS DE TRANSACCIONES: No tiene equivalente en OSI y básicamente tiene que ver con las caracterfsticas de administración de la red.

2.2.1 Un ejemplo de direccionamiento en IP

Las direcciones de IP se pueden utilizar para referirse a una computadora dentro de una red o bien, a un equipo de interconectividad o a una red misma.
Un ejemplo de la notación utilizada se muestra a continuación:



Que en notación decimal quedaría como:

129.10.2.61

- Por convención una dirección de red tiene al identificador de servidor en ceros.
- Un identificador de servidor con unos en su campo se refiere a todas las computadoras dentro de esa red (Transmisión simultánea o "Broadcasting")
- Las direcciones IP por facilidad se escriben en notación decimal formados siempre por cuatro enteros divididos por puntos decimales, cada entero corresponde a un byte (0-255) para así tener una dirección formada por 32 bits (4 bytes u octetos).
- Una dirección IP de 32 bits se maneja con una parte global que identifica un sitio (RED) y una parte local que identifica una computadora en el sitio (SERVIDOR).

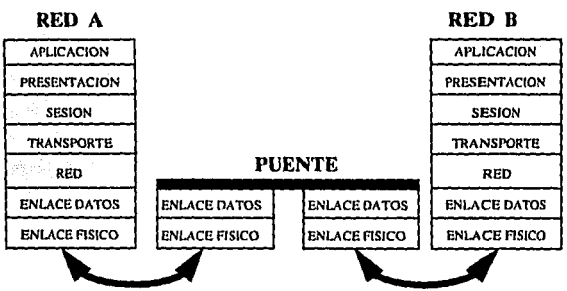


Figura 2.1. Esquema de conexión de puente conforme a modelo OSI.

2.3 Funcionamiento de puentes y ruteadores

Una vez discutidos los modelos de comunicación, así como los protocolos utilizados veamos como funcionan los dispositivos conectados para dar los servicios de conexión a las Redes de Área Local, para así formar una o varias Redes de Área Amplia.

Puentes para LAN y WAN.
Los puentes proveen como ya vimos la conexión en la capa de enlace de datos del modelo OSI, en la figura 2.1 se muestra el esquema de conexión de acuerdo al modelo OSI.
Existen varias formas de conectar los puentes a las redes, y según su función pueden ser:

2.3.1 Redes de Área Local conectadas por un puente transparente

Este tipo de conexión se utiliza cuando se tienen dos LANs que tienen exactamente el mismo protocolo, la misma capa física y de enlace de datos.
Los puentes transparentes no interactuan con los dispositivos, y a su vez los dispositivos no toman parte en la tarea de localizar la ruta o seleccionar el proceso. Desde el punto de vista de las computadoras todas las demás estaciones de trabajo se ven como si estuvieran en la misma red en forma extendida, y únicamente se identifican por tener una dirección única.
Usando la figura 2.1 diremos que el puente conectado a la **Red A** lee los datos de la capa de enlace, transmitidos por los dispositivos de esa red. Todos aquellos que tengan direcciones que no correspondan a su tabla serán desechados, es decir ignora los mensajes enviados a dispositivos en esa red.
Cuando el puente acepta los datos de algún dispositivo estos son inmediatamente transmitidos a **Red B** usando el mismo protocolo de la capa de enlace y la misma conexión física.

Lo mismo ocurre en sentido opuesto de B hacia A.

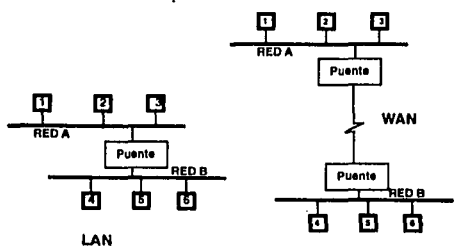


Figura 2.2. Conexión de puente en redes LAN y WAN.

Se entiende que el puente debe tener la información exacta de las direcciones y posiciones de los dispositivos conectados en ambas redes. Esta información es cargada de forma manual y/o automática según el tipo de puente usado. Muchos puentes incluso pueden aprender las direcciones de los dispositivos de forma autónoma.
La manera como el sistema aprende es a partir de la lectura que hace de la capa de enlace de datos, una vez que recibe un mensaje. Al recibir el mensaje el puente construye y actualiza su base de datos, la cual se conoce como tabla de enrutamiento. Esta tabla lista

cada uno de los dispositivos fuente, la posición del puente en donde fue recibido el mensaje y un tiempo que indica cuando se hizo la última observación.
En este tipo de puente si el dispositivo falla en encontrar una conexión, entonces entregará el mensaje a todas las conexiones que tenga, excepto donde lo recibió, a esta acción se le denomina Flooding (Inundación, en español, se refiere al envío hacia todos los puntos simultáneamente).
Si el puente encuentra una conexión entre la dirección de destino y la tabla de enrutamiento, entonces compara la conexión del puente en la cual recibió el mensaje con la conexión asociada a su tabla. Valores iguales de fuente y destino indican que el dispositivo se encuentra en el mismo segmento de la red y el ùente ignora el mensaje. En caso de no coincidir con la tabla de conexión entonces el mensaje será transmitido. según la tabla de enrutamiento. La figura 2.2 muestra la conexión típica.

2.3.2 Redes de Área Local conectadas por un puente de traducción (Translating-Bridge)

Un puente de traducción es una forma especial de puente y que puede dar servicio a redes que emplean diferentes protocolos en la capa física y de enlace de datos.
A continuación se muestra un diagrama de conexión de un puente de traducción, conectando una red Token Ring con una red Ethernet.

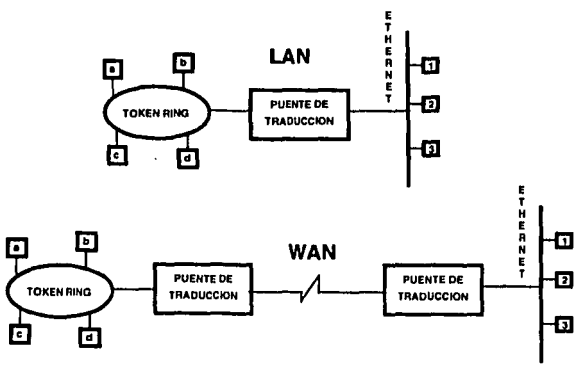


Figura 2.3. Conexión de Redes por puente de traducción.

Este puente permite tener una conectividad entre dispositivos diferentes, manejando los formatos inherentes a cada LAN. El procesamiento integro de traducción de la información es relativo, debido a que Ethernet, Token Ring y FDDI son de alguna forma similares. Sin embargo cada red envía mensajes de diferente longitud y como el puente no es capaz de fragmentar los mensajes, entonces cada red se debe configurar de forma que envíe mensajes de una longitud que se pueda soportar.

Usando la figura 2.3 veamos como opera el proceso de envío de información:

1. El puente recibe la información de las estaciones de trabajo "a, b, c, d" usando el protocolo de Token Ring, entonces lee los datos de los mensajes transmitidos por esa red.
2. El puente ignora todos los mensajes dirigidos hacia la misma red (a-b-c-d).
3. El puente acepta los mensajes para las estaciones de trabajo 1, 2, 3 y usando el protocolo de Ethernet entrega estos mensajes a dicho segmento.
4. El equipo funciona igual en el sentido opuesto Ethernet a Token Ring.

2.3.3 Redes de Área Local conectadas por un puente de encapsulamiento (Encapsulation Bridge)

Este tipo de puente se asocia con la topología de conexión llamada "Backbone", tratada a detalle en el capítulo IV. En la figura 2.4 se muestra la topología mencionada:

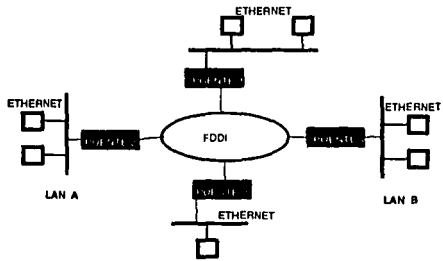


Figura 2.4 Puentes de encapsualmiento.

Como se muestra en la figura 2.4 los puentes permiten encapsular a fin de utilizar la misma capa física y el mismo protocolo (FDDI).
A diferencia del puente de traducción, el cual manipula la envoltura de datos, el de encapsulamiento pone los mensajes recibidos dentro de una envoltura especifica del backbone y enruta el mensaje ya encapsulado o otro puente, para que entonces este lo entregue al receptor.
A continuación veremos como opera esta conexión:

1. El puente 2 lee todos los datos de todos los mensajes enviados por la LAN A usando el mismo protocolo de la capa de enlace y la misma capa física de la red. Ignora todos los mensajes dirigidos a la red A.
2. El puente 2 acepta todos los mensajes dirigidos a otras redes y entonces pone estos mensajes en una envoltura propia de FDDI, los direcciona a todos los puentes (Transmisión de direccionamiento múltiple) y envía este paquete a través del anillo de FDDI.

3. Los puentes 1, 3 y 4 reciben el paquete y lo desenvuelven, los tres validan las direcciones de destino de los datos, entonces el puente 1 y el 3 los desechan por no ser direcciones locales, el puente 4 acepta los datos y utilizando la capa física y protocolo de Ethernet procede a la entrega del mensaje a su destinatario.

2.3.4 Redes de Área Local conectadas por un puente por ruteo de origen (Source Route Bridge)

Este nombre fue empleado por IBM para denominar un método de puenteo de paquetes a través de redes Token Ring. Este tipo de conexión implica que el emisor del mensaje y no el puente sea quien defina la información necesaria para la entrega de los datos a su destinatario.

En una red de este tipo los puentes no necesitan manejar tablas de enrutamiento, simplemente deciden si pasan o no los datos basados en la información contenida en la envoltura del mensaje. Para trabajar en dicho esquema cada dispositivo de datos determina inicialmente la ruta de destino de los mensajes que enviará, esto a través de un proceso especial llamado route discovery (Descubrir ruta).

Basados en el diagrama de la figura 2.5, explicaremos el funcionamiento de este tipo de dispositivos:

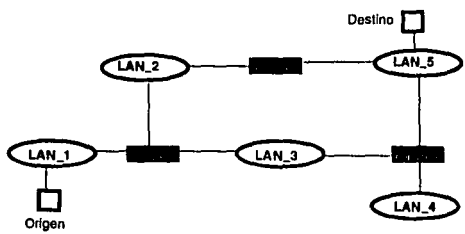


Figura 2.5. Puentes con ruteo por origen.

1. La LAN 1 necesita enviar mensajes a la LAN 5, entonces la LAN 1 envía un paquete de exploración (Explorer), el cual usa una envoltura especial que es reconocida por cualquier puente de source routing. Al recibir un puente este paquete pone en el mismo la información de por donde se conectó al puente, así como el nombre de dicho puente.
2. Entonces el puente envía el explorador a todas las otras conexiones.
3. Como consecuencia el receptor recibirá muchas copias del mismo paquete de exploración, tantas como las rutas posibles que existan entre el origen y el destino. Cada paquete contiene una lista de secuencias y rutas para la conexión del mensaje a través de la red.
4. Una vez recibido el explorador la LAN 5 decide y elige una ruta disponible y envía una respuesta al originador (LAN 1).

5. Una vez descubierta la ruta, la LAN 1 guarda esta en memoria a fin de poder enviar los mensajes necesarios para ese destino y envía el mensaje en una envoltura reconocida por todos los puentes y en la cual van las instrucciones de ruteo.

2.3.5 Redes de Área Local conectadas por Ruteadores (Routers)

A diferencia de los Puentes, los Ruteadores trabajan hasta la tercera capa del modelo OSI.

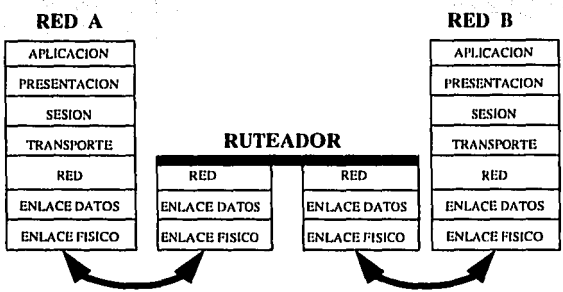


Figura 2.6 Modelo OSI para conexión de Ruteadores.

Por lo que un ruteador puede ofrecer servicios más complejos y sofisticados que un puente. Estos equipos pueden elegir una ruta de manera selectiva, entre origen y destino y además hacerlo en forma activa, basándose para esto en una selección de diversos factores, como pueden ser: Costo de transmisión, niveles de tráfico, congestión de redes, o bien distancias entre origen y destino. La distancia normalmente se mide en conteo de la cantidad de ruteadores que hay que atravesar entre origen y destino.
Los ruteadores deben ser explícitamente solicitados para que puedan ofrecer sus servicios, es decir procesan únicamente los mensajes que son enviados directamente a ellos por otro dispositivo.

La lógica de manejo de los datos en el ruteo, se basa en que cada LAN conectada al equipo tiene su dirección única (De acuerdo a la capa de red del modelo OSI) y en que cada dispositivo conectado a la LAN tiene su dirección única (De acuerdo a la capa de enlace de datos del modelo OSI).
Como ejemplificación diremos que:
Bajo el supuesto de que todas las redes están direccionadas con formato IP y de que los dispositivos direccionables en cada red van del 1 al 99, entonces tendríamos que una dirección completa se compondría de cuatro dígitos, al concatenar las direcciones de LANs con las de dispositivos. Como ejemplo tenemos que si la dirección es 150.130.128.40,

estaremos hablando del dispositivo 40 conectado en la red 150. y el 128.128.128.10 entonces será el dispositivo 10 de la LAN 128.
Dentro de un ambiente de ruteo todos los dispositivos guardan tablas básicas para enrutamiento de los mensajes. Para la mayor parte de los dispositivos en esta tabla únicamente guardan unos cuantos datos específicos acerca de las LANs y los ruteadores adyacentes.

Basados en el diagrama de la figura 2.7, trataremos de explicar el funcionamiento de este tipo de dispositivos:

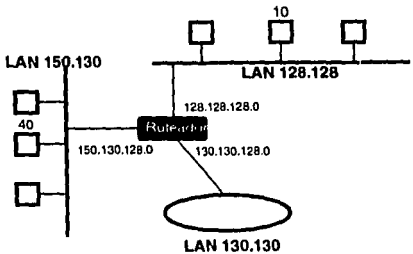


Figura 2.7. Esquema de conexión de direccionamiento.

1. Supongamos que el dispositivo 40 envía un mensaje al 10.
2. El dispositivo 40 checa si la dirección 128.128.128.10 esta dentro de su misma Red, al no encontrarla va a la tabla de enrutamiento y coloca la dirección del ruteador que coincida con la de la tabla.
3. El dispositivo 40 coloca la dirección del destinatario en el mensaje lo empaqueta y lo pone así en el ruteador.
4. Al recibir el mensaje el ruteador quita los bits correspondientes a la envoltura y compara la dirección contra su tabla, la cual contiene varias direcciones correspondientes a otras LAN y otros ruteadores. Para nuestro ejemplo 3 direcciones.
5. El ruteador al comparar la dirección de destino encuentra que se equipara con la dirección de la LAN 128.128.
6. El ruteador reconoce esta como una dirección conectada directamente y entonces entrega el mensaje al destinatario utilizando el protocolo Ethernet de la capa de enlace de datos y el protocolo requerido por la conexión física.

Ahora bien, que sucede cuando el mensaje es para un dispositivo que no esta directamente conectado al ruteador, como sucede en una red de área amplia (WAN).

Como ejemplo ampliaremos la red LAN de la figura 2.7 por una WAN, y la conexión queda como se muestra en la figura 2.8.

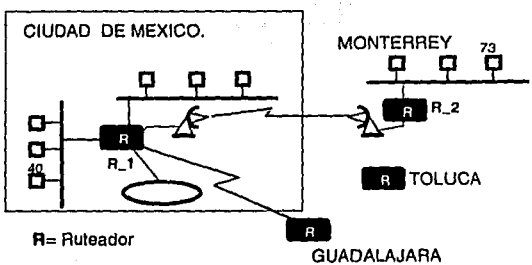


Figura 2.8. Diagrama de enlace WAN para el ejemplo.

Nuevamente el dispositivo 40 desea enviar un mensaje pero ahora al 73.

1. El dispositivo 40 verifica si la dirección se encuentra dentro de su misma Red, al no encontrarla consulta la tabla de enrutamiento y encuentra como única conexión el Ruteador 1(**R_1**)
2. Al tomar la dirección del destinatario, la coloca en el mensaje y lo empaqueta enviándolo al ruteadador.
3. Al recibir el mensaje, el ruteador quita los bits correspondientes a la envoltura y compara contra su tabla, la cual contiene varias direcciones que corresponden a otras LAN y otros ruteadores. Para nuestro ejemplo 6 direcciones.
4. El ruteador compara la dirección de destino y encuentra que no se acopla con ninguna de sus conexiones directas.
5. El ruteador consulta en su tabla y encuentra la dirección de la red de destino. Entonces procede a buscar un ruteador adyacente en la misma ruta del mensaje.
6. Encuentra el Ruteador 2 (**R_2**) y entonces el ruteador uno añade los bits necesarios para envolver el mensaje y enviarlo al ruteador 2.
7. El Ruteador 2 reconoce ésta como una dirección conectada directamente y entonces entrega el mensaje al destinatario, utilizando Ethernet de la capa de enlace de datos y el protocolo requerido por la conexión física.

Ahora analicemos otra de las funciones importantes del ruteador; que consiste en conocer la ruta óptima para envío de la información.
Basándonos en la red anterior supongamos que existiera otro enlace de comunicación entre el nodo de Monterrey y el de la Ciudad de México.(Figura 2.9)

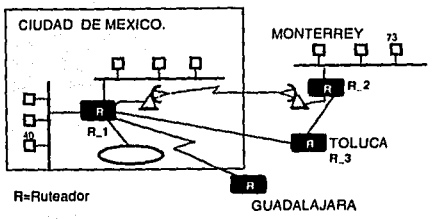


Figura 2.9. Figura del enlace para el ejemplo.

1. El proceso de envío del mensaje se seguiría igual hasta lo correspondiente al punto cuatro del ejemplo anterior, entonces:
2. El Ruteador 1 encuentra dos ruteadores adyacentes.(**R_2 y R_3**).
3. El Ruteador 1 regresa y consulta sus tablas de decisión o sus algoritmos de Ruteo y en base a estos decide el envío del mensaje por el ruteador **R_3**.

En apariencia lo ideal sería el envío directo por la misma ruta mostrada con anterioridad, sin embargo esto no necesariamente podría ser válido. Como ejemplo digamos que el enlace entre el ruteador 1 y el 2 utiliza un conexión de microondas rentada por tiempo de utilización y que la conexión entre Toluca y Monterrey, así como entre Toluca y Cd. de México, son en enlace privado digital por RDI (Red Digital de Servicios Integrados).
Para este caso sería más barato enviar el mensaje a través de la red contratada y no a través de microondas.
Como ejemplo final veamos el caso de la misma red conectada a un servicio internacional de paquetes de datos (Posiblemente con X.25).
La red del ejemplo anterior ahora añade un elemento más, una conexión a Nueva York a través de una red de datos de X.25.(Figura 2.10)
En este caso si cualquiera de las terminales y/o redes de la ciudad de México envía un mensaje para Nueva York, este seguramente se enrutaría a Monterrey como se mencionó anteriormente y entonces hacia la red de datos de X.25 para llegar a su destino final en Nueva York.
Ahora bien, el caso interesante aquí es el de la ciudad de Guadalajara, la cual tiene cuatro posibles rutas a seguir para llegar a Nueva York y Viceversa:

1. Guadalajara-México-Monterrey Nueva York.
2. Guadalajara-Toluca-Monterrey-Nueva York.
3. Guadalajara-Toluca-Mexico-Monterrey-Nueva York.
4. Guadalajara-México-Toluca-Monterrey-Nueva York.

Todas son rutas válidas y antes de hacer la conexión el ruteador tiene que hacer varios análisis para llevar a cabo la conexión de los datos.

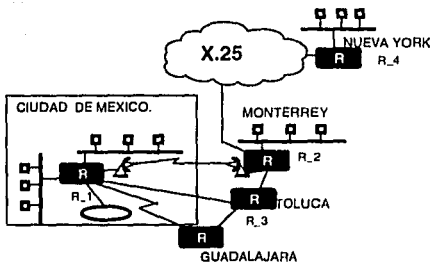


Figura 2.10. Enlace WAN a Red de paquetes.

Es interesante notar que la existencia de varias rutas para llegar a un destino hace que las redes sean más flexibles y por tanto más confiables, sin embargo no habrá que perder de vista que mientras más grandes van siendo las redes, más compleja se hace la tarea de elegir la mejor ruta para el envío de los datos.

En base a lo anterior surgen algunas interrogantes como son:

1) ¿Cómo elige el ruteador la mejor ruta cuándo existen múltiples caminos para ir hacia un destino? y
2) ¿Cómo obtiene la información acerca de los ruteadores distantes y de las redes conectadas a éstos?.

   La respuesta a ambas preguntas la da el uso de **protocolos de enrutamiento.** Debido a que los ruteadores están comunicados entre sí, pueden compartir información acerca de la red.

2.3.6 Protocolo de enrutamiento

Las funciones básicas de los protocolos de enrutamiento son:

Determinación de las rutas.
Utilización de tablas de enrutamiento.
Definición de métricas de ruta.
Algoritmo de enrutamiento.
Adaptación de rutas para intercambio de información.
Conmutación (Transporte de paquetes a través de la red)

Los protocolos de ruteo corren como software dentro del ruteador, construyendo la tabla de discriminación desde el punto de vista del ruteador.
De acuerdo a su algoritmo de funcionamiento, tenemos que los ruteadores pueden ser:

- Estático: El enrutamiento es fijo.

- Dinámico: El enrutamiento se adapta de acuerdo a la situación de la red (Tráfico, fallas en nodos y/o enlaces, etc.).
- Centralizado: Un nodo central es el que calcula todas las rutas.
- Distribuido: Cada nodo calcula sus rutas.
- Single-Path: Únicamente maneja una trayectoria para cada destino.
- Multi-Path: Puede manejar varias trayectorias para su destino.
- Estado de Enlaces: Envía actualización a tablas de enrutamiento únicamente cuando hay cambios en la red.
- Vector de distancia: Transmite tablas de actualización de rutas de manera constante y se basa en la cantidad de veces que debe pasar por un ruteador.

Entre los protocolos más utilizados se encuentran los siguientes:

EGP	(Exterior Gateway Protocol) Protocolo de compuerta exterior, enrutamiento entre dominios (Entre diferentes redes) y se utiliza en Internet. Es del tipo dinámico.
RIP	(Routing Information Protocol) Protocolo de información de ruteo, desarrollado para XNS, para IPX y TCP/IP. Es del tipo de Vector de Distancia.
OSPF	(Open Shortest Path First) Primera ruta más corta abierta, desarrollado para TCP/IP. Usa algoritmo de Estado de Enlaces.
IS-IS	(Intermediate System to Intermediate System) Sistema intermedio a Sistema intermedio, desarrollado para OSI y DECnet.
RTMP	(Routing Table Maintenance Protocol) Tabla de protocolo de ruteo y mantenimiento, utilizado por Appletalk.
BGP	(Border Gateway Protocol) Protocolo de paso por límite de compuerta.

Dentro de los algoritmos de enrutamiento las dos tecnologías que engloban a la mayor parte de los protocolos son:

1) El de vector de distancia.
2) El de estado de enlaces.

El primero es el más antiguo y un ejemplo de este es el RIP. Con este protocolo los ruteadores se encargan de actualizar y transmitir constantemente las tablas de ruteo a través de la red.
Estos protocolos permiten manejar servicios adecuados para redes pequeñas y normalmente estables, sin embargo son indeseables para redes muy grandes o en constante crecimiento. Lo anterior se debe a que la transmisión de dichas tablas en redes grandes aumenta dramáticamente el tráfico de la red y ocupa innecesariamente mayor ancho de banda.
Además este protocolo siempre utiliza la misma condición de enrutamiento, es decir la menor cantidad de ruteadores entre el origen y el destino.

El protocolo de estado de enlaces (Como IS-IS y OSPF) no actualiza constantemente las tablas, sino que envía la información únicamente cuando existe algún cambio y para notificar el nuevo estatus de los enlaces.

Adicionalmente permite manejar múltiples rutas de acceso para balancear el tráfico de datos entre nodos. Esto ofrece la ventaja al usuario de especificar tres medidas para la elección más adecuada de la ruta en base a los siguientes parámetros:

- Velocidad de transmisión.
- Capacidad de salida.
- Confiabilidad.

Lo anterior finalmente buscando el menor costo, crecimiento futuro y la mayor seguridad.

2.4 Consideraciones sobre equipos de conmutación, puentes y ruteadores

Para poder aprovechar mejor la demanda de ancho de banda, hoy día es necesario evaluar correctamente cuando usar cada una de las tecnologías

El conmutador (Switch) para LAN provee la mejor solución para ambientes locales. Si por ejemplo se van a manejar grandes cantidades de información sobre una red local Ethernet, la utilización del conmutador es la mejor opción en cuanto a precio/desempeño pues maneja conexiones punto a punto a 10 Mbps.

Los puentes son utilizados preferentemente para segmentación de redes, ya que pueden separar en grupos de tráfico compartido a usuarios que se comunican continuamente. El puente también se puede utilizar a través de WANs para enlazar segmentos remotos a una red.

Los ruteadores vienen a resolver problemas en grandes redes para comprimir la acción de cientos o miles de nodos. Sofisticados ruteadores operan dentro de la capa de red del esquema de OSI, permitiendo dividir las redes en subredes lógicas y dirigir el tráfico necesario para esas subredes.

A continuación se muestra una tabla comparativa de las tres tecnologías:

PARÁMETRO	RUTEADOR	PUENTE	CONMUTADOR.
Facilidad de instalación y configuración.	Difícil	Fácil	Fácil.
Seguridad y control de acceso	Soporta filtrado de protocolos de alto nivel.	Soporta únicamente filtrado de direccionamiento de Acceso al Medio (MAC)	Se puede prescindir de ello.
Computo de ruteo	Sofisticado con algoritmos de búsqueda de rutas óptimas.	Usa algoritmo básico de árbol expandido para evitar regresos innecesarios.	Mínimo o no existente.
Interfaces de LAN soportadas	Gran cantidad (Ethernet, Fast Ethernet, Token Ring, FDDI, ATM)	Puede no soportar interfaces de redes de alta velocidad.	Gran cantidad (Ethernet, Fast ethernet*, Token Ring* ,FDDI, ATM)
Interfaces de WAN soportadas.	Soporta prácticamente cualquiera	Puede soportar WANs de baja velocidad	Solo soporta interfaces de LAN.
Soporte de ATM	Disponible	No disponible	Disponible
Desempeño máximo de salida	225K paquetes por segundo.	280K paquetes por segundo.	240K paquetes por segundo.
Precio	Aproximadamente $2,000 dólares por puerto.	Aproximadamente $1,500 dólares por puerto.	De $350 a $1,200 dólares por puerto.

(*)Nota: Estos dos actualmente están en desarrollo.
Fuente: SynOptics, 1994.

CAPÍTULO III

GENERALIDADES DEL PROCESO PARA EL DISEÑO DE REDES

CAPÍTULO III

GENERALIDADES DEL PROCESO PARA DISEÑO DE REDES

Una red no es una entidad capaz de generar datos, sino más bien tiene como objetivo fundamental servir como medio de transferencia de la información que se haya producido en los procesos en ambos sentidos, como entrada y como salida de los elementos de computación.
Es conveniente estructurar el proceso a fin de manejar etapas controladas y así facilitar las tareas, a continuación presentamos un plan de diseño:

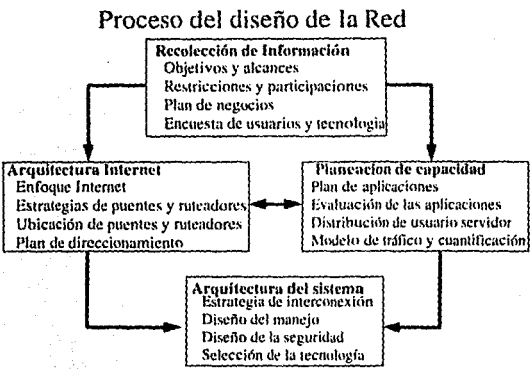


Figura 3.1. Diagrama a bloques del proceso de diseño.

Entonces antes de hacer cualquier diseño será necesario determinar las necesidades reales de transferencia de información, así como conocer los alcances de la solución a proponer y el tiempo que se requerirá para implementar la misma.

3.1 Recolección de Información

3.1.1 Objetivos y Alcance

Inicialmente se tendrá que determinar que se espera obtener de la red y cuantificar los recursos para saber que servicios se requerirán y que limitaciones se tienen o se tendrán. A esto se le denomina levantamiento de necesidades, y es utilizado para sugerir y ayudar al

cliente a decidir sobre ubicación de equipos y posibles rutas de cableado. También nos ayudará a evaluar posibles aplicaciones futuras.
Se debe tener en cuenta que el objetivo primario de una Red es la disponibilidad, es decir: Tener la posibilidad de crecimiento, el mejor rendimiento, tiempo de respuesta mínimo, facilidad de administración, costo mínimo de recuperación y adaptación a nuevas tecnologías.
Este punto nos debe dar la idea global del tipo de soluciones que podremos ofrecer. Para presentar el diseño preliminar, donde podremos definir y visualizar lo que necesitaremos en cuanto a tecnología de comunicación de datos, medios físicos de conexión, tráfico necesario por usuario, etc.

3.1.2 Restricciones y participación

Aquí se pretende determinar el tipo de equipo y de red (Si existiese), así como cuantificar los recursos de información y económicos con que se cuenta.
Esta posición nos da una clara idea de hasta donde vamos a participar. Es decir que nos delimita nuestra frontera de diseño.

Base Instalada Actual:
Es necesario partir de la premisa en la cual se encuentra la infraestructura actual, así como el saber que tipo de equipo se esta manejando (Tecnología, Fabricantes, grados de servicio actuales, aplicaciones que se están manejando)
En este punto se sugiere trabajar con una entrevista con los responsables del proyecto para responder las siguientes preguntas:

- *¿Que tipo de computadoras se están manejando?*
- *¿Poseen alguna red?, ¿De que tipo?*
  Es de suma importancia conocer el equipo que se conectará a la red para determinar las interfaces y las posibilidades de manejo de conectividad que se pueden ofrecer.
- *¿Cuantos usuarios utilizan la red?*
- *¿Que aplicaciones corren en la red?*
- *¿Cuanto tiempo en promedio accesan por usuario y por aplicación?*
- *Cantidad de datos que maneja la red hacia los dispositivos (PC's, Impresoras, etc.) en Kilobytes.*

En caso de existir más de una red LAN se requerirá información adicional como:

- *Ubicación física de las otras redes, así como tipo de redes.*
- *¿Existe algún enlace o conexión entre ellas? En caso afirmativo ¿de que tipo?*
- *¿Cuentan con medios de comunicación para enlaces (Ej. Líneas privadas, Satélite, etc.)*

Con referencia a la instalación física de los equipos y el cableado será recomendable hacer una inspección física o bien saber :

¿Que tipo de infraestructura poseen?

- Tipo de Cableado
- ¿Es estructurado su cableado?
- ¿Cuentan con concentradores? ¿De que tipo?

3.1.3 Planes Futuros

Una de las consideraciones importantes es visualizar hacia donde se esta dirigiendo la empresa, para así tener en mente que necesidades pueden llegar a tener y también cuanto se planea invertir en las soluciones. En caso contrario se puede diseñar la red con expectativas a largo plazo que nunca se cumplirán, por no ser acordes con la evolución real del negocio.

Futuras aplicaciones:
Tal vez esta es la parte más difícil de identificar tanto para los usuarios como para los diseñadores de redes, ya que es necesario presuponer las tendencias de la empresa, así como del mercado de software y hardware.
Sin embargo existen algunas cuestiones que pueden servir como auxiliares para la obtención de la información requerida, como por ejemplo:

- ¿Actualmente que tareas no se efectúan en los sistemas por falta de tiempo?
- ¿Les gustaría contar con servicios de?
  - Correo Electrónico.
  - Video Texto.
  - Fax Inter-red.
  - Video Conferencia.
  - Acceso a redes públicas de información.
  - Encripción de datos.
- ¿Tienen planeado crecer operaciones en los próximos?
  - 2 a 5 Años
  - ¿En que áreas?
- ¿Planean manejar su red de datos compartida con redes de voz?
- ¿Tienen en mente cambiar la ubicación física de sus oficinas o instalaciones?
- ¿Que porcentaje de movilidad de personal manejan?

Si existe incertidumbre sobre la información que se nos proporcione, entonces se deberá valorar a cada parámetro en escala de importancia y pensar en que ***si las probabilidades de cambios son fuertes y/o constantes deberemos proponer un equipo lo suficientemente flexible para adaptarse a estos cambios (Tecnología modular).*** En este punto es donde se deberá ser muy estricto con la elección del fabricante y considerar a aquellos que van dictando pautas tecnológicas, sobre todo es importante que tengan una representación formal en nuestro país y una base instalada lo suficientemente grande para que garantice la permanencia de la citada marca en nuestro mercado.

3.1.4 Encuesta a usuarios de la tecnología

Una política sana es el hablar con los usuarios y así conocer de ellos mismos la forma como ven los servicios que les brinda la red y más aún como les gustaría que esto funcionase.
Con lo anterior nos podríamos evitar el gastar tiempo y recursos valiosos para modificar posteriormente la red para adaptarse a cierta aplicación no considerada inicialmente, o bien que se evaluó con diferente nivel de prioridad al real.
Estas encuestas o entrevistas deben ser breves y centrarse en lo que el usuario esta trabajando actualmente, ya que asumimos que en el plan de negocios se trataron las expectativas futuras.

Se le debe preguntar acerca de que niveles de acceso tiene a otras redes y que utilidad tendría para el accesar a los otros servidores.
Se deben analizar métodos de almacenamiento y procesamiento de información, así como identificar duplicidad de tareas y/o funciones en los servidores de las redes.
Una vez propuestos los niveles de servicio a ofrecer será necesario consultar con el usuario nuevamente a fin de corroborar que el tráfico ofrecido, así como las velocidades de acceso sean los requeridos para sus aplicaciones.

3.2 Planeación de Capacidades

Aquí se hace el planteamiento de las técnicas a utilizar para el envío y recepción de la información.
Idealmente se puede manejar el siguiente modelo como guía:

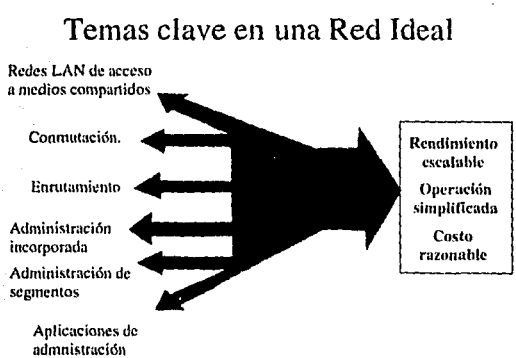


Figura 3.2. Diagrama de parámetros para diseño óptimo.

Los parámetros mostrados a la izquierda de la gráfica nos darán las base para tener una red con una Operación Simple y Rendimiento escalable a un costo razonable. En los siguientes puntos se verá como planear con dichos parámetros.

3.2.1. Planificación de las aplicaciones

Las aplicaciones de los usuarios pueden dividirse según se muestra en la tabla 3.1:
Entonces para empezar a diseñar necesitaremos determinar lo siguiente:

1. Definir que tipo de aplicaciones se utilizarán.
2. Como se implementarán dichas aplicaciones en el tiempo.
3. Las cantidades de servidores y estaciones de trabajo a utilizar.
4. Unidades para entrada y salida de datos.

5. Plataforma de operación.
6. Modos de acceso a otras redes.

APLICACIONES.	TIPO DE PROCESADOR QUE LO PUEDE MANEJAR
• Transferencia simple de datos	80286
• Manejo de archivos de gráficas y colores para usuarios.	80386
• Aplicaciones para trabajo en grupo.	80386
• Documentos gráficos y correo electrónico.	386DX
• Multimedia.	486DX
• Modelado y diseño por computadora.	486DX2, PENTIUM

Tabla 3.1.

3.2.2. Evaluación de las aplicaciones

De acuerdo a toda la recolección de información se puede dividir el análisis en dos partes principales;

1) Análisis para Redes Nuevas.
2) Análisis para Crecimiento de Redes o Modernización.

A continuación se presentan dichos análisis.

1)Para el caso en que tengamos que diseñar redes nuevas tendremos que concretar los requerimientos genéricos de acuerdo a los datos obtenidos anteriormente, principalmente en lo referente a tiempos, volúmenes y prioridades. Existe una gran libertad en la elección de la topología, por lo que será necesario que al diseñar ***considere desde las opciones básicas hacia las sofisticadas***.

Por ejemplo, si tenemos los siguientes requerimientos con un cliente que desea Token Ring:

- Velocidades de acceso menores a 250 msegs.
- Con la posibilidad de manejar 10 terminales de alta prioridad y 40 de baja prioridad.
- Manejo de gráficos y diseño automático por computadora (CAD).
- 2 terminales remotas a 1,800 metros del servidor.

Por la cantidad de terminales o estaciones de trabajo no existe restricción para Token Ring, ya que puede manejar hasta 260.

La necesidad de manejo de gráficos y diseño por PC nos plantea una demanda de tráfico alta por lo cual podría ser recomendable utilizar FDDI o Fast Ethernet a 100 Mbps. Sin embargo por el número de terminales tanto Ethernet como Token Ring pueden ser suficientes.

Además consideremos que esta tecnología nos permite una mayor facilidad para otorgar las prioridades dentro de la red.

Se manejarían dos terminales a 1,800 mts. lo que rebasa la posibilidad directa de Token Ring, entonces se requiere un enlace con repetidores para hacer dicha conexión. Otra opción podría ser una terminal por fibra óptica, la cual se puede conectar hasta a 2 Km. del servidor.

Con referencia al tipo de cableado dependerá de la elección anterior.

Otra posibilidad a analizar sería utilizando dos redes Ethernet segmentadas por puentes enlazados por fibra óptica.
Una primera red para servir principalmente a los usuarios prioritarios (10 Mbps)
Y la segunda red o segmento podría servir a los otros 40 usuarios.
También en lugar de los puentes se podría hacer el enlace con fibra óptica pudiendo poner un repetidor remoto a una distancia de 1000 metros y dos segmentos de 500 metros con repetidores locales.
Como se puede observar las posibles soluciones no siempre son simples, y lo que nos podrá ayudar para la decisión óptima será ***el costo, la confiabilidad y la versatilidad futura de nuestra elección.***
2) Para el caso de diseñar sobre crecimiento o actualización de redes tendremos entonces que concretar los requerimientos genéricos de acuerdo a los datos obtenidos anteriormente, ahora enfocándonos más bien a la base instalada actual y examinando la posibilidad de conexión entre redes. A diferencia del caso anterior no existe libertad total en la elección de la topología, ni en los protocolos de manejo, ni el ancho de banda a utilizar, por lo que será necesario elegir cuidadosamente la marca y tipos de equipo adicional que se requiera.
Los parámetros que se deberán considerar en este punto son:

-Tiempos de respuesta.

- Será necesario conocer los tiempos de acceso que requerirán los diferentes dispositivos conectados a la red, debido a que ***este parámetro es clave en la selección del tipo de tecnología de red que deberá utilizarse***, así como del tipo de medio de transmisión o transporte de encapsulamiento que se empleará. Este dato nos lo puede proporcionar el encargado de la red, o bien se podrá estimar de acuerdo a los datos obtenidos en el punto anterior.

-Volúmenes de información a transferir.

- Es importante no confundir la capacidad de almacenamiento de los dispositivos con la cantidad de datos que la red deberá transportar entre todos los dispositivos, la cual combinada con el parámetro anterior nos indicará cuales son las tecnologías que cumplen con estas condicionantes. Nuevamente este dato se puede obtener de la información anterior.
  Es conveniente analizar también las aplicaciones futuras antes de decidir la tecnología.

-Distancias a cubrir entre los dispositivos:

- Por la concepción de las redes locales se nos ofrece una limitante en cuanto a las distancias que deben de guardar las terminales de trabajo con respecto a los servidores de red. (Ver Capítulo I). Entonces de acuerdo a los datos obtenidos en la primera parte podremos ver si la red que se tiene o se está proponiendo cumple con las expectativas de distancia, de lo contrario tendrá que ser considerado el uso de repetidores, conmutadores o puentes y finalmente incluso considerar otro tipo de tecnología de cableado o red que cumpla con esos requerimientos.
- Para el caso de las distancias entre nodos remotos o configuraciones WAN. También será necesario analizar si la tecnología con que se cuente o se este proponiendo cumple con varios aspectos como serían:
  Ancho de Banda suficiente de acuerdo al tráfico.
  Medios de comunicación existentes y limitantes de interfaces físicas.

Normas de acuerdo a la tecnología actual.
Costos de renta de medios de transporte, etc.

-Número de Servicios a Soportar.

- Nos referimos a que existe la posibilidad de compartir medios de comunicación con otros servicios como podrían ser:
  Voz.
  Video
  Alarmas
  De esta forma se puede hacer más rentable la solución de comunicación al compartir el recurso, ya que muchas veces ya existen estos servicios instalados y solo se tendría que añadir el equipo adicional (Ej. Multiplexores voz/datos, Enlaces digitales E1).

-Prioridades de usuarios y aplicaciones.

- En definitiva los datos que se intercambian entre terminales de las redes no tienen el mismo nivel de importancia, entonces debemos considerar la posibilidad de dividir u organizar las aplicaciones y los usuarios a fin de optimizar los tiempos de uso de los equipos y los canales de comunicación. Con esto podemos lograr reducir el costo de inversión en la red o incluso no generar un gasto mayor en equipo para crecimiento.
  Con este parámetro, el cual nos debe definir el usuario, se puede proponer un dimensionamiento acorde a las necesidades reales.

-Privacidad y control de acceso.

Así mismo como en el caso anterior es de suma importancia el disponer de los mecanismos necesarios para determinar quien va a poder accesar algo, como y en que momento.

Una forma simple de control es mediante la segmentación de redes, dando al mismo tiempo jerarquía en la selección de aplicaciones. La otra manera es mediante el software de aplicación de la red el que puede efectuar este control, presentando la ventaja de que se independiza la topología de la red con respecto al tipo de control de acceso.

-Tipos de estaciones a conectar.

Según el tipo de función que desempeñan las estaciones que se conectan a una red pueden ser:

Estaciones de trabajo.
Servidores de red
Dispositivos de comunicación
Impresoras.
Dispositivos programables (Robots, sensores, controladores de alarmas y acceso, etc., aunque son poco utilizados ya que normalmente se están trabajando en forma independiente.)

Comúnmente en ambientes de oficina se tenderá a utilizar redes de baja velocidad como Ethernet o Token Ring, sin embargo ***si existen aplicaciones de alto tráfico de información o de gran demanda de recursos de procesamiento será necesario considerar FDDI, Fast Ethernet o algún otro medio de alta***

velocidad, como ATM o Conmutador y posiblemente segmentar por aplicaciones.

-Modos de acceso a otras redes.

Este punto se debe considerar fuertemente en caso de estar diseñando libremente sin que se tenga base instalada actual, ya que una buena elección de red local puede abatir de manera dramática los costos de equipo de enlace. Esto debido a que se requerirá menos equipamiento exterior para compatibilidad con la WAN.

Si por el contrario ya se tiene base instalada (Lo cual es más frecuente) será importante entonces ***considerar que el medio de comunicación con las otras redes sea económico y que requiera menos interfaces, esto en relación a los parámetros de nuestra red actual.***

Si por ejemplo, tenemos una red Ethernet y existe la necesidad de manejar datos hacia una LAN Token Ring sería posible utilizar un Puente de Traducción, sin embargo esto nos limita a accesar solo hacia ese punto. Tal vez una opción de mayor costo inicial será un ruteador con manejo de multiprotocolo, pero nos dará la flexibilidad de crecer hacia otras aplicaciones en caso de requerir acceso futuro a otras redes

3.2.2. Distribución de Equipo Usuario-Servidor

La ubicación física de los dispositivos de terminales de trabajo, no debe representar un problema, siempre y cuando la red se encuentre estructurada (Cableado Estructurado). En caso contrario el lugar donde se coloque si deberá ser un factor determinante en la lógica de manejo de los datos, y debe ser cuidadosamente analizado, ya que de acuerdo a la cantidad de información y tipo de aplicaciones que maneje deberá ser conectada al segmento o segmentos de red que lo vayan a emplear. Para los efectos de este trabajo se considera que la red siempre es estructurada.

En cambio la ubicación de los servidores es un factor clave para el desempeño de la red, debido a que dependiendo de su posición:

1. Se afecta directamente el tiempo de respuesta.
2. Es determinante en el tamaño de la red.
3. Afecta los parámetros de diseño de aplicaciones (Distribución de datos y operaciones de cómputo)
4. Se podrá colocar la cantidad de usuarios a manejar.
5. Se podrán o no implementar buenos niveles de seguridad dentro de la red.

Es importante considerar que el 98% de las fallas producidas en una red se debe al cableado.

Como ejemplo veamos la figura 3.3, tenemos a continuación el resumen mostrado en la tabla 3.2. En donde se muestra la ruta que debe existir para que la información llegue a su destino, considerando el tiempo que recorrería un paquete a través de cada camino. En cada ruta tenemos diferentes retardos debido a la latencia de cada uno de los equipos que existen entre origen y destino:

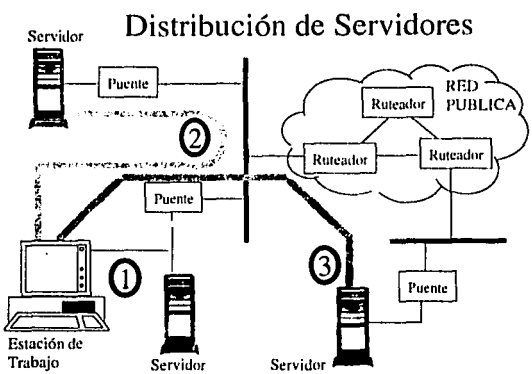


Figura 3.3. Distribución de equipo usuario-servidor.

RUTA	TIEMPO DE RESPUESTA
UNO	1.1 mseg.
DOS	1.6 mseg.
TRES	8.6 mseg.

Tabla 3.2.

De lo anterior se desprende que ***la ubicación de los servidores es un factor clave debido a que los saltos que se tienen que hacer a través de los dispositivos de conexión reducen en gran medida el desempeño de la red.*** Hay que recordar que al pasar por puentes y ruteadores existen retrasos debidos a conversiones de protocolos y verificación de datos.

3.2.3. Análisis de tráfico y presupuestos

La posibilidad de manejar grandes volúmenes de información nos lleva a considerar la mejor forma de enviar y recibir estos datos desde y hacia los servidores.
Normalmente las transacciones Cliente/Servidor son mucho más intensas para la red que las aplicaciones de Terminal/Mainframe que sustituyeron. Debido a que se requieren más transacciones para negociar el envío y recepción, entonces las redes LAN deben de funcionar a mayor velocidad (Ancho de Banda) para correr el mismo tipo de aplicaciones.
El diseñador debe tomar conciencia de la importancia de hacer un presupuesto del tráfico en la red, aunque determinar este parámetro exige mucho trabajo y conocimiento. Si agregamos la dificultad de negociar el tráfico a manejar con el ancho de banda que por lo

general es limitado, entonces determinar el rendimiento deseado de nuestra red no es algo sencillo.
El rendimiento de la red tiene dos facetas,

1. El retraso de usuarios en lo particular.
2. El retraso que se presenta al tener múltiples usuarios.

La pregunta sería ¿A que velocidad debe de funcionar la red para satisfacer ambas condiciones?
La respuesta en ocasiones no es simple, ya que puede ser que las necesidades no están bien definidas y entonces se deberá analizar en lo individual y luego pasar a lo general. A continuación presentamos un proceso que puede auxiliar en la determinación de estos parámetros.

- En caso de que exista una red habrá que hacer una medición precisa del tráfico actual. Esto se puede hacer directamente con el administrador de red.
- Determinar de acuerdo al plan de la empresa, los requerimientos de cada usuario en lo particular y de ser posible los tiempos que utiliza así como los horarios. Se podría utilizar una tabla como la 3.3, que se muestra a continuación como ejemplo:

Tabulación de tiempos de utilización de Servidor Uno.

Usuario del Recurso	Capacidad de gestión de información.	Tiempo promedio de utilización de los canales.	Tipo de transmisión.	Horario en que trabaja.
Gerencia. Informática	1 Mbps	1.0 Hora	Interactiva	9:00-12:00
Ventas.	19.2 Kbps	0.2 Hora	Batch	8:00-11:00
Compras.	9.6 Kbps	8.0 Hora	Interactiva	10:00-18:00
Ingeniería.	64 Kbps	0.1 Hora	Interactiva	14:00-19:00

Tabla 3.3.

Se debe manejar una tabla similar por cada servidor, para el caso de que existan aplicaciones compartidas.
De esta tabla se puede extraer la capacidad de canal de comunicación que requerimos por tiempo de utilización.
Se tabulan las aplicaciones y demandas por hora (Tabla de horario Tiempo de utilización),
Se añade la capacidad requerida en ese horario. Se elige el horario que tiene que manejar la mayor densidad de información, así estaremos diseñando para el peor caso.
De acuerdo al tipo de transmisión se seleccionan las tecnologías que puedan manejar dicho tráfico para interconectar los ruteadores y puentes.
Otro parámetro que es importante es el punto de donde a donde se dirige el tráfico, ya que con este dato podremos ***separar a los usuarios en segmentos para atender mejor a sus demandas, ya que puede ser necesario establecer redes lógicas diferentes de la topología física, a fin de acelerar los proceso y reducir el tráfico por segmento.***
A los datos finales se les agrega un porcentaje entre el 20 y 35% para crecimiento.

- Finalmente se suman las demandas actuales más las planeadas y se procede a colocar los datos en una tabla, que nos refleja a los usuarios con la capacidad de datos requerida y

agrupados según las necesidades en Grupos de trabajo, Estos a su vez en Departamentos, Áreas y Empresas.

- Así finalmente tenemos el presupuesto del tráfico de la red.

Como se mencionó en el punto 3.1.4 se comentan los datos obtenidos con las áreas involucradas a fin de verificar que los datos correspondan a las necesidades reales.

Con todos los datos anteriores tendremos la capacidad de manejo de los canales de conexión y siguiendo con el proceso de diseño pasamos ahora a ver la parte de Arquitectura de Conexión entre Redes (Internet)

3.3 Arquitectura Internet (Conexión entre redes)

3.3.1. Enfoque Internet

La idea de la interconexión de redes es la de poder compartir los recursos de forma independiente al área física de trabajo.

Las metas de la arquitectura de Internet son:

- Ahorro en el costo de aplicaciones y medios de enlace.
- Mayor rendimiento con el menor ancho de banda.
- Unificación del protocolo de comunicación.(Interoperabilidad)
- Confiabilidad con flexibilidad.
- Reutilización en lo posible de tecnologías heredadas.

La pregunta es ¿Cuando se necesita conexión entre redes?

Este tipo de arquitectura se requiere cuando:

- Se tienen oficinas físicamente separadas y los niveles de gestión de información superan los 4.5 Mbps.(2 E1)
- Si las estaciones terminales tienen un crecimiento promedio de 30% anual.
- Si el cableado y recableado de sus instalaciones es un problema fuerte. (Ej. Edificios viejos o plantas con ubicaciones muy distantes entre ellas mayores a los 1000 metros)
- Si los usuarios cambian de lugar frecuentemente o bien cambian de aplicaciones en forma constante.
- Los troncales principales (Backbones) necesitan más de 100 Mbps.
- Si existen servidores que manejen más de 20 Mbps.
- O se tienen aplicaciones en terminales de trabajo que requieran más de 10 Mbps.

Si es necesario arrancar hacia esta arquitectura, el primer paso será reducir los protocolos utilizados a un máximo de dos diferentes en el troncal principal. (Aplicaciones de Correo electrónico se manejarán más fácilmente)

Evalúe cuáles de los sistemas heredados no valen la pena de ser convertidos (Ej. Una red Arcnet o Token Ring, a 2 Mbps y 4Mbps respectivamente).

Plantee la estructura de cableado estructurado y concentración de recursos por piso o área.(En forma esquemática utilizando cajas negras)

Elija el equipo de conexión adecuado según sus requerimientos, mediante las estrategias de puentes y ruteadores.

3.3.2. Estrategias de puentes y ruteadores

Ahora ya sabemos que requerimos conectar nuestros recursos de cómputo, entonces la pregunta es ¿Cómo?
Por los datos anteriores ya tenemos la idea en conjunto de la forma en la cual será distribuida nuestra red y la ubicación física que tendrán los servicios de la misma, entonces requerimos elegir el tipo de equipo que se deberá colocar para unir las redes remotas y las redes segmentadas. Como ayuda para dicha elección se muestran guías de selección de equipos, las cuales al ser llenadas nos podrán indicar las características mínimas de equipo que requerimos en cada uno de los nodos de nuestra red.
Estas guías están estructuradas en forma de tablas para ejemplificar un método a seguir, aunque lo importante en sí no es la forma de la tabla, sino los conceptos que se deben conocer para la elección del equipo de interconexión.

1. Con referencia a funcionalidad.

- ¿Qué requerimientos se tienen para ruteo?

PROTOCOLOS DE COMUNICACIONES	PROTOCOLOS DE RUTEO.	SI/NO	COMENTARIO
TCP/IP	OSPF, RIP y EGP		Mucha utilización
DECnet Phase IV	DECnet Routing		Poca utilización
Novell IPX	RIP		Mucha utilización
XNS	RIP		
Appletalk	RTMP		Poca Utilización.
Banyan VINES	RTP		
OSI	ES-IS,IS-IS		Utilización Media

Tabla 3.4.

De este punto se tendrán que sacar las características de protocolo necesarias para los equipos de interconexión, hay que recordar que bajo las recomendaciones anteriores no deberemos de tener más de dos protocolos diferentes en cada troncal (Backbone) de las redes LAN y WAN.

- Cuales son los métodos requeridos para puenteo (Uno por cada nodo).

MÉTODO	COMENTARIO
Spanning Tree	No todos los puentes lo soportan.
Ruteo por Fuente	Aplicable a Token Ring.
Puente Transparente	Requiere mismos protocolos
Puente de Traducción	Es más versátil pero más caro.
Puente de Encapsulamiento	Sólo aplica a redes idénticas.

Tabla 3.5.

Con esto tenemos los tipos de puentes a manejar en cada nodo.

- Ver si se requiere soporte para otro tipo de tráfico

NODO	Puente o Ruteador.	SNA/SDLC	PBX	VIDEO
UNO	Puente	✓	✘	✘
DOS	Puente	✘	✘	✘
TRES	Ruteador	✘	✘	✓
:				
:				
N				

Tabla 3.6.

En este caso se tendrá que analizar el medio de enlace entre los nodos a fin de determinar si se requiere añadir un multiplexor antes del ruteador o puente. Este parámetro puede cambiar únicamente los requerimientos en lo referente al tipo de interface requerida, así como a tiempos de latencia y administración de la red.

- ¿Qué tipo de LAN y cuántas deben ser soportadas por cada equipo?

Como ejemplo se presenta la siguiente tabla:

NODO	Puente o ruteador.	Ethernet/ IEEE 802.3	Token Ring/ IEEE 802.5 (4 ó 16 Mbps)	FDDI	Fast Ethernet	Troncal de ATM
UNO	Puente	1	1	0	0	0
DOS	Puente	1	1	0	0	0
TRES	Ruteador	1	2	1	0	1
:						
:						
N						

Tabla 3.7.

Este parámetro es requerido para la elección de configuración en las interfaces de los equipos de conexión, esto se debe a que la gran mayoría de los equipos son configurables en cuanto a las interfaces que manejan. En el caso de ATM esto tiende a ser muy demandado.

Este dato nos servirá únicamente cuando hallamos determinado el tipo de equipo a utilizar.

- ¿Qué velocidad y cuántos circuitos de WAN debe soportar cada equipo?

Como ejemplo se presenta en la tabla 3.8:

NODO	Puente o Ruteador.	Baja Velocidad (1.2 a 64 Kbps)	Líneas E0	Líneas E1	Líneas E3
UNO	Puente	4	0	0	0
DOS	Puente	0	5	0	0
TRES	Ruteador	2	10	1	0

:					
:					
N					

Tabla 3.8.

Aquí tenemos el caso similar al punto anterior, aunque también nos ayuda a descartar muchos productos que no tienen capacidad de manejo de todas estas interfaces.

- ¿Qué capacidades de administración se deben manejar?
-

FUNCIÓN	SITUACIÓN	COMENTARIO
Capacidad de administración de nodos locales		Depende mucho de cableado estructurado.
Capacidad de administración de nodos remotos.		
Compatibilidad con SNMP		Estos son los agentes más utilizados
Soportar Base de datos MIB I y II.		
Mapa de estado de red en tiempo real.		
Capacidades de reporte de alarmas.		
Gráficas de desempeño en tiempo real.		
Configuración Centralizada de Red.		
Capacidad de manejo de reportes.		
Plataforma de software soportada		Sun, DEC, PC, etc.
Compatibilidad con otros softwares de administración de redes.		DECmcc, HP Open View, Sun Net Manager, IBM, etc.
Control redundante		Recomendable

Tabla 3.9

De acuerdo a lo presentado en la tabla 3.9 estaremos en posibilidad de elegir el software correcto o bien de requerir el cambio de algunos componentes de la red heredada. Por ejemplo, si se requiere administrar nodos remotos, se deberá verificar que los equipos que fueron elegidos o bien heredados manejen los mismos agentes SNMP, de lo contrario esta función no podrá ser soportada. En capítulo VI se tratan a fondo los detalles de la administración de la red, así como sus componentes.

- Protocolos y servicios de WAN que se deben manejar por nodo.

Como ejemplo se presenta la tabla 3.10:

NODO	Puente o ruteador.	X.25	FRAME RELAY	SMDS	PPP	ATM
UNO	Puente	SÍ	NO	NO	NO	SÍ
DOS	Ruteador	NO	SÍ	SÍ	SÍ	SÍ
TRES	Ruteador	SÍ	NO	NO	SÍ	SÍ

:						
:						
N						

Tabla 3.10.

Esta tabla nos indicará cuales son los requerimientos mínimos de software para la elección de los equipos y nos indicará la interface de conexión que se deberá equipar. También nos sirve para verificación de los datos anteriores, ya que debe existir congruencia entre los protocolos y los medios de transporte de la señal. Es decir, si se requiere manejar X.25, y anteriormente se indicó que un nodo utiliza E1, no tiene sentido, ya que X.25 maneja menos de 64 Kb de ancho de banda y la E1 2.048 Mbps. O bien si se puso que el ruteador va a manejar Voz y Datos y no se elige ATM entonces no se puede soportar la aplicación.[1]

2. Con referencia a desempeño.

Es importante para la elección del equipo el conocer qué tan rápido se deben de efectuar las funciones, esto en términos de tráfico filtrado y enrutado (Paquetes por segundo).

Se puede utilizar para el efecto una tabla como la 3.11., que se muestra a continuación:

NODO	Puente o Ruteador.	Cantidad de Estaciones de trabajo	Ancho de banda total requerido	Rutas a atender (Prioridad)	Tiempo máx. de Latencia	Es Local o remoto. (**)[2]
UNO	Puente					
DOS	Ruteador					
TRES	Ruteador					
.:						
:						
N						

Tabla 3.11.

Una vez más con los datos anteriores se deberán comparar los datos en cuanto a congruencia.

De esta tabla obtendremos básicamente la capacidad total de puertos por dispositivo, así como la velocidad mínima de proceso requerida en cada uno de ellos (Tiempo de Latencia), además se verá si los parámetros requeridos son soportados por el tipo de tecnología, o bien si es necesario dividir el tráfico para compartirlo por otras rutas.

Los datos aquí obtenidos nos dará también información valiosa para lo referente a reconfiguración de la red en caso de fallas y estimar qué procesos deberán ser desechados en caso de fallas en nodos críticos.

Así mismo el filtrado en los nodos nos permitirá manejar tráfico flexible y permitir a las aplicaciones críticas tener continuidad, así como una buena seguridad contra intrusos indeseables..

3. Con referencia a Mantenimiento y confiabilidad requeridos.

---

[1]Para mayor información refiérase al capítulo I para ver características de las tecnologías.

[2]Es importante este dato, debido a que si se requiere bajo tiempo de latencia y es un nodo local, pudiera ser mejor elección cambiar por un conmutador (Switch).

FUNCIÓN	¿REQUERIDO SI O NO?	COMENTARIO
Tiempo promedio máximo entre fallas		MTBF por sus siglas en Inglés.
Tiempo promedio máximo para reparación.		MTTR por sus siglas en Inglés.
Reconfiguración dinámica en línea		Importante para continuidad de tráfico de datos
Reemplazo en línea de tarjetas y/o componentes de interface.		Vital en nodos críticos.
Actualización en campo		
Cumplimiento de estándares		IEEE, ISO, etc. (Comparar compatibilidad de sistemas propietarios)
Homologaciones		NOM, UL.
Restricciones de tamaño.		Área disponible, considerar para mantenimiento.
Control redundante		Vital en nodos críticos.

Tabla 3.12.

Esta información nos servirá más adelante para depuración de los diferentes equipos seleccionados y así ayudar a la elección del proveedor.

Una vez completados todos los datos anteriores se tendrán las características que deberán cumplir los equipos por cada nodo.

3.3.3. Ubicación de puentes y ruteadores

En el punto 3.3.1 se trataron los procesos para elaborar el bosquejo de la red en cuanto a su estructura de ubicaciones físicas, de igual forma se tratarán en forma más extensa en el siguiente capítulo.
En el punto 3.3.2 se justificó cada nodo y se verificó si debía ser un ruteador, un puente o bien un conmutador.
Ahora bien se pueden colocar en el esquema de la red las ubicaciones tentativas de los dispositivos de conexión, la posición servirá como base para analizar el tráfico y así mismo nos permitirá visualizar la forma en que se trabajará el direccionamiento.

3.3.4. Planes de direccionamiento de información

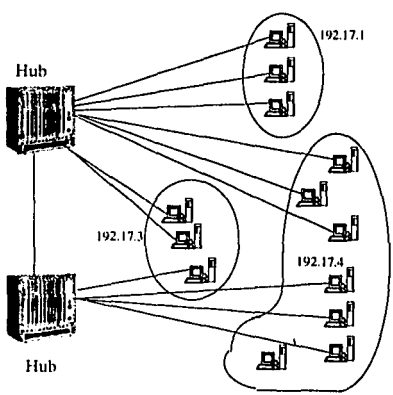
La gran ventaja de las redes es que la ubicación física no está necesariamente ligada con la aplicación que se deba de manejar. Esto nos permite tener una gran flexibilidad en lo referente al manejo de la información dentro de la empresa.
La función de determinación de ubicación lógica se efectúa utilizando el direccionamiento.
En los capítulos I y II se trataron los temas de convenciones para direcciones, por lo cual no se hace mayor referencia al respecto.
La implementación del direccionamiento se hace en:

- Segmento con el uso de las direcciones MAC.

- En la subred con la utilización de IP.

Entonces una estación o terminal podrá tener acceso a múltiples redes de área local, facilitándose así la transferencia de información en cualquier momento.
Así mismo la facilidad que tienen los dispositivos inteligentes de conexión de redes permite ir descubriendo las direcciones de los equipos conectados a la red, así nos permitirá tener la flexibilidad de cambiar de lugar una máquina (Ya sea físicamente o lógicamente) sin que se afecte su acceso a los servicios.
Es muy importante considerar que esta implementación de un plan de direccionamiento nos llevará a la utilización de múltiples concentradores para su funcionamiento.

Para dar el direccionamiento a cada uno de los equipos se utilizan las convenciones mencionadas anteriormente, las cuales básicamente nos indican a qué dispositivo de conexión está enlazada la terminal y cuál es su ubicación dentro de ese dispositivo, entonces se ubican en el plano de la red las estaciones que pertenezcan al mismo segmento lógico (Grupo de Trabajo), aunque tengan diferente ubicación física, incluso una máquina puede pertenecer a múltiples redes, siempre y cuando se direccione atrás de un puente o un ruteador.
En la figura 3.4 se muestra cómo quedaría una red típica usando la estructura de direccionamiento. En este ejemplo, se muestran claramente tres redes lógicas, la 192.17.1. la 192.17.3 y la 192.17.4. Cada concentrador tiene integrado un conmutador o bien un ruteador para el direccionamiento, y así permitir la interoperabilidad entre los segmentos.
La meta en el plan de direccionamiento es ser lo más consistente posible.
En caso de accesar a redes públicas será necesario solicitar a las autoridades correspondientes, los números de registro y dirección para la red de conexión.



FALLA DE ORIGEN

3.17

Figura 3.4 Estructura Flexible de direccionamiento..

3.4 Propuesta Arquitectónica

3.4.1. Estrategia de conexión de redes

La mejor manera de conexión es utilizando una red estructurada, para esto se emplean las siguientes arquitecturas básicas :

- Arquitectura de troncal Distribuida. Esta topología es una red segmentada con un dispositivo de interconexión localizado físicamente en cada área donde existan varias terminales.
- Arquitectura de troncal colapsada. Es una red segmentada con un puente o ruteador centralizado, el cual permite centralizar las conexiones en un solo punto.

En estos momentos no tocaremos cómo operan cada una de ellas, ya que en el siguiente capítulo se explica su operación

En la tabla 3.13. se muestra un comparativo de las diferentes arquitecturas y sus características más relevantes, para fines de elegir lo más adecuado para nuestras necesidades:

RED con troncal en:	Rendimiento	Flexibilidad para crecimiento	Facilidad de administración.	Comentarios
Red sin segmentos.	Bajo	Baja	Alta	Conectividad Básica. Facilidad de cambios. Crecimiento limitado por el ancho de banda.
Concentrador colapsado	Regular	Regular	Regular	Mayor rendimiento terminal/servidor. Centralización de administración de la red. Cambios son caros. Cada cambio afecta a ruteadores, terminales y servidores.
Concentrador paralelo	Regular	Baja	Excelente	Modularidad de administración. Cambios sin modificaciones del cableado. Reducción de administración en ruteadores. Pocas facilidades de crecimiento y segmentación.
Conmutación de tramas	Bueno	Bueno	Excelente	Reducción de problemas de distancia. Buen manejo para grupos de trabajo. Flexibilidad alta para asignar nuevos usuarios y cambios. Requiere alta compatibilidad para operar correctamente.
Conmutación de células	Excelente	Excelente	Excelente	Crecimiento sin dificultades. Uso de múltiples tecnologías en forma directa. Velocidades mayores a 100 Mbps. Integración LAN-WAN directa. Requiere equipo que opere bajo normatividad ATM.
FDDI en Hub distribuido	Regular	Baja	Baja	Alta disponibilidad de recursos. Enrutadores con redundancia por el anillo doble. Poco flexible a cambios. Limitado en capacidad de crecimiento.
FDDI/ATM	Alto	Alta	Baja	Permite evolucionar con cambios mínimos. Aumenta ancho de banda del enlace troncal. Bajo rendimiento para el usuario final. Latencia grande entre cliente y servidor.
ATM redundante	Alto	Excelente	Regular	Alta tolerancia a fallas. Alta capacidad de ancho de banda. Complejidad para administrar ruteadores.
Enlace con conmutación de células.	Excelente	Excelente	Excelente	Gran seguridad. Tráfico de ruteadores sólo a servidores remotos. Crecimiento sin límites. Velocidades superiores a los 100 Mbps. Red totalmente virtual Integración LAN-WAN transparente. Desventaja de pocos productos en mercado.

Tabla 3.13.

3.4.2 Diseño del Manejo

La mejor manera de diseñar el manejo de la red es mediante Segmentos Distribuidos. Esto se debe a que básicamente la red de la empresa podrá estar constituida en:

- Diferentes lugares y ciudades.
- Con diferentes tecnologías
- Con limitantes económicos y administrativos.
- Con alta posibilidad de necesitar proveedores diferentes de servicios

Luego entonces no es factible controlar y manejar sistemas complejos desde una visión plana total, por tanto se dividirá el control en Segmentos o grupos funcionales para poder visualizar secciones de la red y definir el punto de falla o localizar cuellos de botella.
En la figura 3.5 se muestra un esquema de lo que se pretenderá manejar:

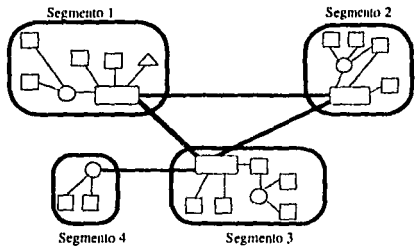


Figura 3.5 Segmentación de una red.

Qué se requiere:

- Plataforma de manejo abierta, basada en estándares SNMP[3]
- Herramientas de manejo de red distribuida.
- Software de aplicaciones efectivo, con ayudas en el momento y desplegables en pantalla.

En resumen los Segmentos deberán visualizar y controlar a las siguientes características y facilidades:

I. Manejo de circuitos (Modems, Multiplexores, portadora de comunicación).
II. Cambios de red.(Red pública conmutada, ruteador, conmutador)
III. En Red troncal principal (Puentes locales, ruteadores, distribuidor elevador, Troncales principales y conmutadores ATM)
IV. En Gabinetes de cableado (Concentradores, Interfaces usuario-servidor)
V. Entorno operativo del grupo de trabajo (Protocolos de Red y Sistema Operativo)
VI. Respaldo del software de aplicaciones estándar del servidor.
VII. Respaldo de software de aplicaciones de usuario.

[3]Se verán con amplitud estos temas en el capítulo de administración de redes.

VIII. Control en tiempo real de servicios de entrada salida (Impresoras sin papel o fuera de línea)

3.4.3 Seguridad

En los ambientes de red el administrador frecuentemente se encuentra con la problemática de definir cuándo los controles son suficientes, sin llegar a ser excesivos. Entonces hay que preguntarse y evaluar lo siguiente:

¿Qué nivel de seguridad se requiere?
¿Cuál será el costo o el impacto de una intrusión indeseable?
¿Dónde, cuándo y quién deberá obtener la información?

La seguridad comienza en los servidores, donde se deberán colocar barreras de entrada para evitar el acceso indiscriminado a los datos de la empresa.
Lo anterior se lleva a cabo asignando a cada usuario de la red una clave de identificación única (Password), la cual le permitirá accesar únicamente los servicios que el administrador le asigne, incluso se le pueden asignar los horarios y tiempos para el acceso y los lugares en los cuales podrá hacer sus respaldos de información.
Prácticamente todo el software de LAN diseñado actualmente permite manejar todo lo anterior con relativa facilidad.
Como segunda recomendación se deberán ubicar los servidores de red en lugares cerrados y protegidos con llave, esto no afecta en nada al sistema, considerando que el usuario no requiere tener acceso físico al servidor para poder trabajar.
En muchos lugares la continuidad de trabajo del servidor es fundamental para el funcionamiento de la red.
Adicionalmente se debe considerar que al seleccionar el software de red se deberán escoger aquellos productos que nos permitan manejar encripción de claves de acceso, y protecciones contra entradas ilegales al sistema, incluso algunos de ellos pueden enviar alarmas al supervisor de red en tiempo real.
Las consideraciones básicas en el diseño de la seguridad deberán contemplar:

- Procedimientos efectivos de administración (Network Manager System), es muy difícil poder tener seguridad cuando no se tiene un software, así como un hardware de administración de red confiable y poderoso.
- Definición efectiva de servicios para usuarios. Aunque representa más trabajo es necesario que se definan adecuadamente los niveles de acceso a las facilidades, para así evitar que alguien erróneamente dañe alguna información vital.
- Definición de grupos de trabajo para aumentar el nivel de control. Si el administrador tiene que analizar grandes cantidades de datos y existe un problema, es más sencillo trabajar sobre un grupo de trabajo que sobre todos los usuarios.
- Se debe crear una política o un buen sistema para mantenimiento y verificación de claves de acceso. Será necesario verificar el estado de claves y en la medida de lo posible cambiar éstas periódicamente, para evitar problemas debido a que a algún usuario le copien su clave.
- Seguridad física en servidores y equipo de interconexión. Estos equipos deberán estar ubicados fuera del alcance de gente ajena a la administración y mantenimiento de los mismos.

- Diseño controlado de aplicaciones. Con esto evitamos los problemas de que se accesen datos restringidos. Han existido casos en que por errores lógicos de aplicaciones se afectaron datos confidenciales, a esto se le conoce como "entrar por la puerta de atrás" (Back door access).
- Filtrado en los ruteadores y puentes. Con esta facilidad se puede limitar el acceso a información de servidores a los usuarios que no lo requieran, directamente desde el mismo dispositivo de conmutación. Esto representa la ventaja de que filtrando desde el equipo no se genera tráfico adicional al tratar de accesar una aplicación a la cual no tenemos derecho.

Si se requiere seguridad máxima, se tendrá que considerar adicionalmente manejar los siguientes parámetros:

- Encripción de datos transmitidos y almacenados. La ISO recomienda establecer esta protección en el nivel de presentación del modelo OSI. La justificación de esto básicamente es que si se hacen en la capa de aplicación son más vulnerables a ser desensamblados.
- Protección de copiado en los archivos del servidor (Archivos sólo de lectura). De esta forma se protege al sistema de que sean alterados datos básicos de funcionamiento o que se extraiga información del mismo.
- Poner cuando sea posible Estaciones de Trabajo sin dispositivos para discos flexibles o disquetes. Esta opción no es muy útil si la gente tiene que estar sacando datos para llevarlos a otras máquinas, además de que requiere una capacidad muy grande de almacenamiento en los servidores y las PC's. Por otro lado es una garantía para evitar que se propaguen virus en nuestra red.

Finalmente una vez que esté la red en operación, el administrador nunca deberá guardar datos esenciales en servidores no protegidos.

También es altamente recomendable establecer políticas de respaldo de la información, es decir que la información vital de los sistemas se deba respaldar por lo menos una vez al día. La información de los usuarios se puede respaldar tal vez una vez al mes, junto con toda la información adicional que no se respalda diariamente. Con los softwares actuales los respaldos se pueden programar de forma automática.

En caso de ser sistemas de alta confiabilidad se deberá contar con redundancia en lo posible y que las actualizaciones se hagan simultáneamente en los dos sistemas (Función Espejo).

3.4.4 Selección de tecnología

Una vez conjuntados todos los elementos para la elección de la tecnología requerida, lo siguiente es la selección de los equipos que cumplan con los requerimientos de nuestra red. Sobre este particular existen dos puntos de vista:

I) Uno más orientado a la solución económica:

- Evaluación de ofertas comerciales.
- Alcances máximos del presupuesto.
- Rentabilidad de la inversión.
- Aseguramiento de la capacidad de ampliación futura.
- Elección del tipo de equipo y proveedor (es)

II) Y por otro lado el punto de vista que se asocia mejor con la solución técnica:

- Elección de varios equipos basados en las características mínimas obtenidas.

- Análisis de posicionamiento de empresas en el mercado.
- Análisis de ofertas comerciales.
- Garantías de normas y soporte técnico.
- Elección de proveedor y/o equipos.

Desde un punto de vista práctico, la primera posición no es mala, sin embargo se puede descartar una mejor solución que no necesariamente es la más atractiva económicamente hablando. Entonces una posición intermedia o más bien combinada sería recomendable.
Siguiendo esta idea evaluemos la siguiente estructura:

1. Análisis cuantitativo de recursos tecnológicos y económicos disponibles actualmente. Antes de seleccionar cualquier opción de equipo se deberá conocer el presupuesto disponible, ya que de lo contrario se puede implementar la mejor solución, pero por carencia económica no ser concluida. También se tiene que proyectar el costo del equipo desde la etapa inicial del proceso hasta la etapa final, a fin de estimar posibles incrementos.
2. Definición de medios para conexión en base a disponibilidad y costos fijos de los mismos (Renta, Operación, etc.). Este punto se refiere básicamente a los recursos de comunicación existentes en cada lugar, será de suma importancia determinar el tipo de enlaces que existan y la viabilidad para reutilizarlos. Por ejemplo se puede diseñar una red que funcione muy bien para ancho de banda de RDI, y que en la zona donde se ubica parte de la red no exista infraestructura para proveer dicha conectividad, entonces se tendría que recurrir a otros medios de comunicación.
   También es importante considerar que a nivel costo puede ser más caro el medio de transporte que el equipo requerido para la conexión de la red, entonces se podría tener un costo demasiado elevado con relación a los beneficios que la red podría proveer.
3. Selección del tipo de equipo de conectividad de acuerdo a los recursos de medios de conexión o transporte. Esto va ligado del punto anterior y asume que una vez seleccionado el medio se podrá elegir la mejor interface para el mismo.
4. Selección de tipo de software de red, administrativo y de aplicaciones. Será importante considerar que el software de administración sea compatible para controlar prácticamente todos los dispositivos de la red, así mismo el software de aplicaciones deberá estar diseñado para optimizar al máximo los recursos de la red y proveer de los niveles de seguridad antes mencionados.
5. Obtención de ofertas económicas. Se deberán cotejar las ofertas económicas de diversos proveedores y establecer comparaciones funcionales con ventajas y desventajas de cada opción, pero sobre todo que se cumpla con los requisitos necesarios en el diseño de la arquitectura y del plan de negocios.
6. Análisis de ofertas en base a confiabilidad y continuidad del proveedor y del fabricante del equipo (Soporte, Servicio, Costo de ampliaciones). Una vez filtradas las opciones se deberá evaluar al fabricante, al proveedor, así como los niveles de soporte que cada uno de ellos ofrece. Así mismo evaluar y comparar los costos de crecimiento en función de precio, tiempo de implementación y costo de capacitación.

7. Pruebas piloto de enlaces de red no típicos o que aplicarán nueva tecnología. Si algunos elementos de nuestra red serán conectados con tecnología nueva o innovadora deberán ser probados antes de ponerse en operación. También será importante analizar el compromiso del fabricante para adecuar sus productos a nuevas tecnologías (Costo, tiempos, procedimientos).
8. Selección del equipo.
   Existen bastantes compañías en el mercado de la computación y las telecomunicaciones, sin embargo no todas ofrecen soluciones eficientes, y en ocasiones pueden tener un muy buen equipo pero un servicio o soporte deficiente
   Recuerde elegir tecnología orientada o adaptable a los cambios futuros.
   Luego entonces es necesario considerar otros puntos antes de decidir sobre el equipo a utilizar.

3.5 Algunas consideraciones no técnicas

Dentro del análisis que se debe de hacer sobre los proveedores de los equipos, existen algunos parámetros importantes que son importantes. A continuación presentamos los puntos a considerar:

1. Con respecto a experiencia:
   Que tengan en México personal calificado y entrenado para los modelos de equipo que ofertan.
   Que tengan unidades para evaluación.
   Cuentas de referencia en donde se hayan instalado sistemas similares.
2. En relación a Servicio y Soporte:
   Servicios de consultoría en relación a redes, tecnologías y diseño de aplicaciones.
   Capacitación técnica en administración, operación y servicio.
   Servicios de mantenimiento con pólizas de servicio, políticas de garantías, servicio en sitio, servicio remoto, soporte a usuarios vía telefónica.
3. Con respecto a la empresa:
   Estabilidad.
   Posición en el mercado (Líder o especialista en aplicaciones específicas).
   Participación en los desarrollos de tecnología relacionada a conectividad.

CAPÍTULO IV

OPCIONES DE ARQUITECTURA

CAPÍTULO IV

OPCIONES DE ARQUITECTURA

4.1 Topologías del Backbone o Troncal Principal

El Backbone es el segmento principal de la red al cual están conectados todos los dispositivos que la conforman, como son los concentradores, ruteadores, puentes, así como el equipo terminal conectado a éstos.

El Backbone debe realizar una integración óptima de los grupos de trabajo, por lo que debe cumplir con las siguientes características:

a) Conexiones a alta velocidad entre LANs, así como hacia los servidores principales.

b) Confiabilidad de la red en relación a lo crítico que pueda ser la aplicación.

c) Tener presente una posterior evolución hacia la nueva tecnología, por ejemplo la utilización de conmutadores en el caso de Fast Ethernet o ATM.

Ahora bien, considerando lo anterior y que en la actualidad el troncal principal más común es el FDDI, ya que ofrece una solución completa, a 100 Mbps, existen tres alternativas de estructuramiento del Backbone que son :

- Backbone Distribuido
- Backbone Colapsado
- Backbone Híbrido

- **Backbone Distribuido.**

Es el segmento de arquitectura de red en la que cada concentrador es designado como el Backbone de ese segmento de red. Estos segmentos están conectados a un concentrador central a través de ruteadores

El Backbone Distribuido es el más recomendado en el caso de que los segmentos de red se encuentren distribuidos en áreas alejadas unas de otras, como sucede en un Campus.

- **Backbone Colapsado.**

Es el segmento de arquitectura de red que a través de un ruteador central puede proveer un buen balance entre la capacidad distribuida de procesamiento y control centralizado.

El Backbone Colapsado es administrado en un solo punto.

- **Backbone Híbrido**

Es el segmento de arquitectura de red que comparte porciones del Backbone Colapsado unidas por medio de un Backbone Distribuido. Los tres principales son:

Backbone Paralelo en LAN

Este es otra variante del backbone colapsado en donde múltiples segmentos se encuentran distribuidos a cada gabinete de cableado, de esta manera se provee acceso a todos los segmentos de los diferentes gabinetes de cableado

Backbone Jerárquico

Este tipo de backbone contempla múltiples capas en la arquitectura general de la red, con la opción de que cada capa puede ser distribuida o colapsada.

Backbone Mixto

Es una arquitectura de backbone jerárquico conectado con partes o porciones del backbone colapsado de la red mediante un backbone distribuido.

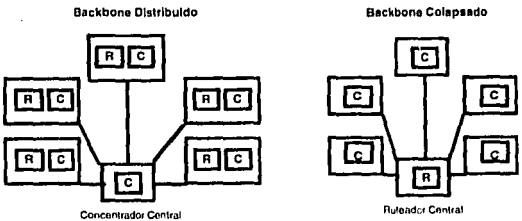


Figura 4.1. Backbone distribuido y Backbone colapsado

En la tabla 4.1 se muestra un comparativo entre el Backbone Distribuido y Backbone Colapsado:

	Backbone Distribuido	Backbone Colapsado
Características	El Backbone de alta velocidad llega a cada concentrador.	El Backbone de alta velocidad sólo está presente en el centro de red.
	El enrutamiento se distribuye a los diferentes concentradores.	El enrutamiento se realiza en el centro de red.
	En las redes LAN actualmente el Backbone es FDDI.	El ruteador sirve de Backbone.
	Los servidores están unidos al Backbone.	Los servidores están en cada segmento.
Ventajas	Estructura de cableado más sencillo.	Topología más sencilla. Las conexiones llegan a un solo punto.
	Migración sencilla hacia procesos de alta velocidad.	Al emplearse ruteadores más poderosos, pueden obtenerse ventajas en desempeño.
	Alta confiabilidad inherente a la arquitectura distribuida.	El Backbone es independiente de lo que se conecte a los concentradores.
	Adición sencilla de redes en el futuro.	Se requieren menos ruteadores.
	Aplicable en entornos geográficos grandes.	Bajo costo para instalaciones de alta densidad.
Desventajas	Se requieren más ruteadores.	Las instalaciones reales requieren de cierta distribución.
		Es un punto de falla único.

Tabla 4.1. Cuadro comparativo de Backbone distribuido y Backbone colapsado.

Es necesario definir los conceptos de gabinete de cableado y centro de red, ya que a través de éstos analizaremos diferentes posibilidades de conexión:

- **Gabinete de cableado.**

En el gabinete de cableado es donde convergen las conexiones de los dispositivos terminales de la red y donde se sitúan generalmente los concentradores y ruteadores. Estos gabinetes simplemente son un punto de concentración intermedia, para luego dirigirse hacia el centro de red.

- **Centro de red**

El centro de red es el punto donde convergen las conexiones provenientes de los gabinetes de cableado. Este punto es donde se encuentran además de otros concentradores y ruteadores, los servicios os principales.

4.1.1 Ejemplos de Topologías de Backbone aplicados a diferentes tipos de redes

Existen diferentes tipos de topologías para el Backbone. Entre las más comunes se encuentran las siguientes:

4.1.1.1 Backbone Distribuido de Ethernet

En esta topología un segmento de red de cada gabinete de cableado es conectado al Backbone de la red, el cual a su vez está conectado al centro de red. En consecuencia se provee de acceso directo al Backbone en cada gabinete de cableado.

Una topología de Backbone distribuido provee un óptimo flujo del tráfico, debido a que los dispositivos de interconexión están instalados en los concentradores locales en lugar de que estén en el centro de red.

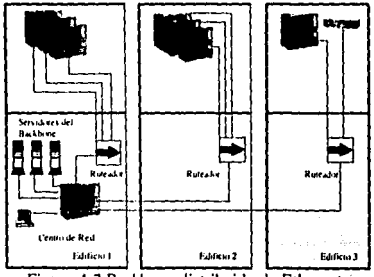


Figura 4.2 Backbone distribuido de Ethernet.

4.1.1.2 Backbone Colapsado de Ethernet

En esta topología los recursos son localizados y controlados desde un punto central y todos los usuarios están conectados a este mismo punto. Los recursos importantes como son servidores, ruteadores y concentradores están localizados en el centro de red. Cada canal en el Concentrador sirve a un grupo de trabajo y provee conectividad para esta centralización de recursos.

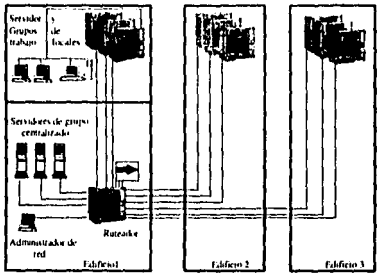


Figura 4.3. Backbone colapsado de Ethernet.

4.1.1.3 Backbone Distribuido en Token Ring

En esta topología los anillos locales están conectados al Concentrador principal que realiza la función del Backbone y el anillo de cada uno de los pisos que trabaja a 4 Mbps o 16 Mbps, conectado a un Puente local instalado en el gabinete de cableado de cada piso.

Por lo que la conexión de estos anillos es mediante puentes y concentradores que se comunican a lo largo de los ductos de canalización de los edificios.

El anillo backbone corre en el concentrador central.

Los servidores centrales pueden conectarse directamente al Backbone por medio del concentrador central o bien pueden estar distribuidos.

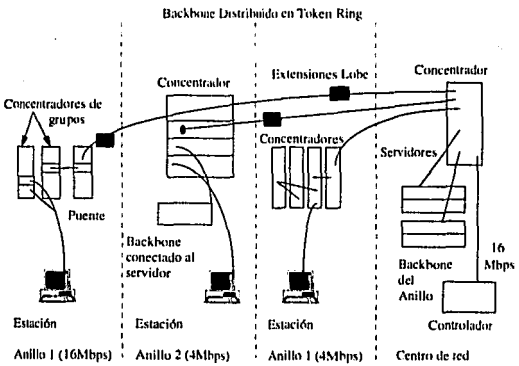


Figura 4.4. Backbone distribuido en Token Ring.

4.1.1.4 Backbone Colapsado en Token Ring

En esta configuración, los recursos están controlados desde un punto centralizado (centro de Red) y todos los usuarios están conectados a esta red común, también localizada en el centro de red. La conexión de las estaciones al anillo se efectúan con cable UTP o STP. Entre el concentrador principal y los pisos individuales generalmente se utiliza fibra óptica. Esta topología es una solución flexible para sitios que no requieren de enlaces directos de los pisos hacia el Backbone y para aquellos sitios donde se desee que todos los puentes estén localizados centralmente.

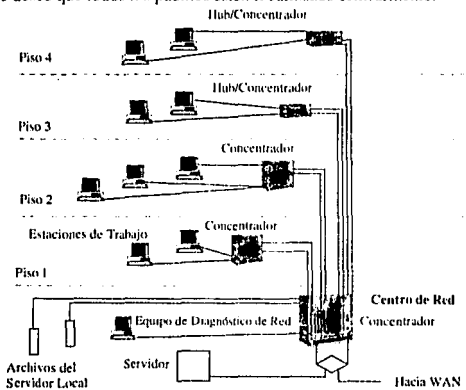


Figura 4.5. Backbone colapsado en Token Ring.

4.1.1.5 FDDI con conexión dual

Es esta configuración tanto los nodos (DAS) como los concentradores (DAC) están conectados directamente a los anillos primario y secundario de la red FDDI. Tal dispositivo frecuentemente es referido como una estación raíz o un concentrador raíz.

En una configuración de doble conexión, un nodo (DAS) o concentrador (DAC) tendrá ambos puertos en un estado activo de ser posible. Cuando ambos puertos de un dispositivo raíz están activos, el dispositivo estará en configuración THRU que quiere decir que la información entra en un puerto A y sale en el otro puerto B.

Si cualquier conexión de un dispositivo raíz falla, el DAC o el DAS se colapsan quedando los anillos primario y secundario lógicamente interconectados. El mecanismo de colapso permite a un dispositivo raíz mantener un anillo lógico en presencia de una falla de enlace.

Se puede lograr una mayor confiabilidad del Troncal principal empleando una Topologfa FDDI de conexión dual y árbol en los cuales los Ruteadores del Anillo se conducen en forma dual a los Concentradores.

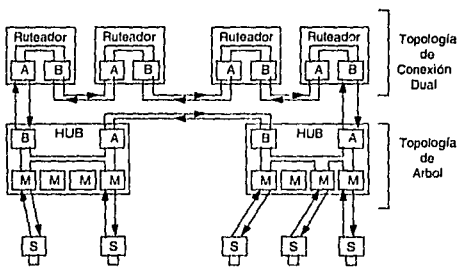


Figura 4.6. FDDI con conexión dual.

4.1.1.6 FDDI Dual Homing

Un DAC o un DAS está en Dual Homing cuando sus puertos A o B están conectados a los puertos (M) de otro concentrador. Cuando estos dispositivos están en Dual Homing existe una conexión primaria entre los puertos B y M y una conexión en reposo entre los puertos A y M. La norma FDDI establece que la conexión primaria del puerto B a M es una conexión activa, mientras que la conexión del puerto A a M puede permanecer deshabilitada o en constante contacto físico mediante el protocolo de administración de la capa física (PCM). Los dos dispositivos mantendrán una limitada comunicación a través del medio sin activar el enlace de reposo.

Si la conexión primaria de la estación conectada en Dual Homing (Entre B y M) se interrumpiera, entonces el enlace entre A y M se activa, sin embargo el PCM seguirá manteniendo comunicación a través de la conexión primaria ya, que si ésta regresara a su estado activo, el nodo entre A y M volvería a su estado de reposo.

Cuando se tiene una conexión sencilla, de un puerto S a un puerto M de un concentrador en caso de falla; tanto el puerto S como el Puerto M se aíslan de la red

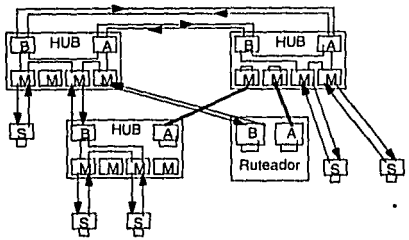


Figura 4.7. FDDI en conexión Dual Homing.

4.2 Opciones de cableado

La selección del cable va en relación directa del tipo de red que se esté instalando y es importante determinar la categoría y tipo de cable requerido de acuerdo a lo mostrado en la tabla 4.2.

Medio	Tipo de red	Distancia	Aplicaciones
UTP Categoría 3	Ethernet y Token Ring hasta de 10 Mbps	100m	Horizontales
UTP Categoría 5	**Ethernet, Token Ring, FDDI de 10 a 100 Mbps, ATM de 155 Mbps* *En desarrollo**	**100 m**	**Horizontales**
STP tipo 1	Token Ring, CDDI, ATM de 155 Mbps	100 m	Horizontales, Troncal principal en Token Ring
Fibra Multimodo	**Ethernet, Token Ring, FDDI de 10 a 100 Mbps, ATM de 155 Mbps, ATM de 622 Mbps (horizontal)**	**2 km.**	**Horizontales, Troncal principal, Campus**
Fibra Monomodo	FDDI, ATM de 155 y 622 Mbps	10 a 40 km.	Campus y Red de área metropolitana. (MAN)

Tabla 4.2. Selección de cables.

Físicamente el cableado se hará interconectando los concentradores, ruteadores y demás equipo que se requiera hacia los gabinetes de cableado y de ahí al centro de red.
El cableado se maneja en 3 topologías básicas que son: estrella, bus y anillo, aunque en realidad con el uso de los concentradores el más empleado es el de estrella.

4.3 Flujo de tráfico en redes LAN y WAN

Para el análisis de arquitecturas es muy importante conocer el flujo de tráfico que se da o debe manejarse a través de los distintos componentes de la red, así como la mejor forma en que se debe transportar de acuerdo a la topología que usemos.

Normalmente se deberán conocer ciertos parámetros antes de estructurar la red o definir su arquitectura según se mencionó en el capítulo III.

Los conceptos importantes de acuerdo al tráfico y que se mencionarán frecuentemente son:

Latencia:	Es el tiempo que se tarda la información al pasar a través de un dispositivo de red.
Demora:	Es tiempo que tardan los datos en llegar de un dispositivo a otro a través de un medio físico.
Cuenta de puertos:	(Hops, Brinco en Inglés) Será la cantidad de dispositivos que tiene que atravesar un dato antes de llegar a su destino.
Ancho de banda agregado:	Que será el tamaño del canal que teóricamente se requeriría para transmitir el dato de forma inmediata.

Grupos de trabajo interconectados por enlace troncal.

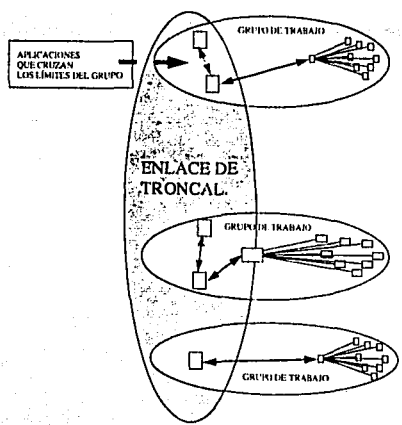


Figura 4.8. Esquema tráfico de aplicaciones.

Desde el punto de vista del empleo de Backbone o troncales como medio de enlaces se deben hacer ciertas consideraciones de dimensionamiento para elegir la estructura de

acuerdo al tráfico de usuarios y demoras: Para explicar este punto nos referiremos a la figura 4.8.

1) Como primer punto se calcula el volumen de usuarios por aplicación que soporta la arquitectura del grupo de trabajo. Es decir cuántos usuarios de cualquier grupo de trabajo pueden realmente atravesar el enlace de troncal para hacer uso de sus aplicaciones. Sin reducir notablemente el rendimiento de la red.
2) Calcular la cantidad de usuarios que soporta el enlace troncal de acuerdo a la arquitectura.
3) Estimar la cantidad de grupos de trabajo que puede soportar la troncal de acuerdo a los dos parámetros anteriores.
4) La demora será el tiempo promedio de todas las aplicaciones que pasen a través del troncal.

Una vez determinado lo anterior podemos saber cuál red y en qué topología soporta las aplicaciones.

Aquí se puede considerar que la variación de la tecnología utilizada en el Backbone o troncal nos dará la posibilidad de reconfigurar nuestra red para otras aplicaciones. Entonces si se requiere soportar a más usuarios, deberá aumentar el ancho de banda, sin embargo al hacer esto se estarán reduciendo las posibilidades de crecer en la red.

Como conclusión tenemos que un mayor tráfico de aplicaciones en el backbone reducirá la posibilidad de incrementar el número de usuarios. Esto opera como una balanza, si se aumenta el tráfico, se reduce el número de usuarios y viceversa.

Por lo anterior se ve la importancia del acomodo de los recursos en la red para reducir el tráfico entre los usuarios y los servidores a través de los concentradores.

Esto se tratará en el siguiente punto con más detalle.

Otra consideración importante es que la tecnología de conmutación puede solucionar mejor, situaciones de alto tráfico en comparación con la de troncal. Lo cual trataremos al final de este capítulo.

En relación a la manera en que se conecte o configure el cableado de la red, podremos tener diferentes tipos de backbone para solucionar mejor el tráfico. A continuación se presenta una tabla 4.3 a modo de ejemplo, la cual nos muestra lo recomendado por un fabricante ("*SynOptics*") para el manejo de los datos en función del tráfico, tanto en los grupos de trabajo (Local), así como en la troncal principal.

En esta tabla nos dan los lineamientos de cómo se debe estructurar y conectar el troncal principal o backbone, de acuerdo a la topología utilizada, para así no tener mayores problemas con el tráfico.

Esta tabla está orientada a la solución de troncal principal con FDDI, sin embargo existen ya otras posibilidades como Fast Ethernet con conmutadores, o bien ATM, las cuales no se deben de descartar.

A continuación, a manera de ejemplo presentamos la tabla 4.4, con los resultados de una simulación[1] en una red, empleando las diferentes tecnologías y bajo los siguientes parámetros:

[1]Fuente Northeast Consulting Resources, Inc.
Boston, Massachusetts

Protocolo:	TCP/IP
Máxima demora en servidores y terminales:	3 seg.
Ubicaciones de grupos de trabajo:	De acuerdo a la topología.

Que utilizar para manejar el tráfico adecuadamente en redes WAN.

Arquitectura / Tipo de tráfico	CENTRO DE RED.	GABINETE DE CABLEADO
TRAFICO DE DATOS LOCAL	FDDI para Servidor a Servidor Concentrador para Aplicaciones locales Ruteadores entre FDDI, redes Ethernet y Token Ring	Concentrador Ethernet para hacer segmentos multiples Concentrador Ethernet conectado a servidores locales Entregar FDDI o 4 10/16 Mbps hacia cada nodo
TRAFICO EN BACKBONE	Centros de cableado Concentradores de Enrutamiento Backbone de FDDI distribuido Servidores conectados a FDDI	Ruteador distribuido a backbone de FDDI a redes Ethernet y Token Ring

Tabla 4.4. Tráfico. Cuadro comparativo.

Red utilizada➡ / Parámetro⬇	Ethernet Sin backbone.	Ethernet con backbone colapsado o distribuido	Backbone con FDDI	Backbone con ATM
Creación de imágenes.	20 Usuarios 3 segundos	28 Usuarios 3 segundos	180 Usuarios. 3 segundos	Más de 10,000 en 3 seg.
Consultas	100 Usuarios 0.8 segundos	500 Usuarios 0.8 segundos	1500 Usuarios 0.8 segundos	Más de 10,000 en 0.8 seg.
Video.	2 Usuarios 0.05 segundos	80 Usuarios 0.05 segundos	90 Usuarios 0.05 segundos	5,000 Usuarios en 0.05
Correo electrónico	700 Usuarios 0.25 segundos	1500 Usuarios 0.25 segundos	9000 Usuarios 0.25 segundos	Más de 10,000 en 0.25 seg.
Velocidad. de acceso Vs. Ethernet.	Igual	2.31 Veces más rápido en promedio	12.98 Veces más rápido en promedio.	22.43 veces más rápido en promedio.

Tabla 4.4. Tabla de resultados de simulación.

Es importante notar que las ventajas de utilizar segmentación pueden reducirse dramáticamente si la aplicación primaria de la red tiene que ver con creación de imágenes. Los resultados nos muestran las ventajas de manejar un backbone de alta velocidad, como se puede observar en el ejemplo FDDI es casi 13 veces más rápido que la red sin segmentar y seis veces más rápido que el backbone colapsado utilizando ruteadores y concentradores. Sin embargo hay que observar que si la aplicación mayoritaria fuera a ser utilizando video, FDDI casi no ofrece ventaja sobre la arquitectura convencional de backbone colapsado.

Por otro lado, la tecnología de conmutación ATM, presenta ventajas importantes en todas las aplicaciones y ofrece prácticamente el doble de rendimiento que FDDI en casi todo, y es realmente muy poderosa al manejar video. Esta es una de las razones por las que la tecnología de conmutación puede desplazar rápidamente a FDDI de la arquitectura de redes.

4.4 Arquitectura de Conmutación

Como se mencionó anteriormente, los conmutadores son dispositivos que han revolucionado el manejo de información en redes, mejorando su desempeño, capacidad de crecimiento y escalabilidad, así como las ventajas que ofrece la administración de redes virtuales.

La tecnología de conmutación se puede clasificar en dos categorías: conmutación de células y conmutación de tramas. El tipo de categoría utilizada y hasta que punto de aplicación se llegue, estará basado en las necesidades de los clientes y usuarios que tendrán que evaluar el costo de estas tecnologías para subsanar el costo de la inversión.

4.4.1 Conmutación de Tramas

Este tipo de conmutación se basa en el tamaño de las tramas usadas en las redes LAN, cuando éstas son recibidas por la red, siguen una ruta predeterminada a través de la misma desde su estación de origen hasta su destino.

Este es un proceso semejante al puenteo, con la excepción de que la transmisión múltiple de tráfico a varios puntos se maneja de manera diferente, es decir, que aquí el tráfico es direccionado únicamente a miembros de la misma *red lógica* y no a todos los puertos cómo en el caso del puenteo normal.

El tráfico entre redes lógicas es manejado por ruteadores que han sido configurados para establecer las políticas de comunicación deseadas entre redes.

Un ejemplo de conmutación de tramas es la conmutación de Ethernet (Ethernet Switching) que puede soportar conexiones compartidas o dedicadas de 10 y 100 Mbps, administración de múltiples redes lógicas, enlaces redundantes y paralelos así como conectividad a ruteadores ya existentes.

Algo realmente importante es que esta mejora en el desempeño requiere una mínima inversión, debido a que no se requerirán tarjetas nuevas de red en las estaciones para la mayoría de los usuarios, sino solo aquellas que se integren a 100 Mbps.

Las ventajas del costo/desempeño entre conmutación de tramas contra ruteo se muestra en la tabla 4.5.

Desempeño y Costo	Ruteo	Conmutación de tramas Ethernet
Rango de Desempeño (tecnología de punta)	.3-.8 Gbps	1-2 Gbps
Precio por cada interface de 10 Mbps	$3,000-5,000	$ 500 por puerto
Precio por cada interface de 100 Mbps	aprox. $15,000	aprox. $800

Tabla 4.5. Tabla comparativa de desempeño y costo de ruteo vs. conmutación. (Precios en U.S. Dólares)

La conmutación de tramas, al igual que la tecnología del medio compartido, en la cual se

basa, no es orientada a conexión. La información necesaria para el direccionamiento de las tramas está contenida dentro de la trama misma (dirección MAC).

4.4.2 Conmutación de Células

Como se mencionó con anterioridad, ATM opera sobre células de longitud fija en las cuales todas las formas de comunicación pueden ser encapsuladas (video, datos, voz etc.). ATM presenta un mayor nivel de crecimiento y escalabilidad que la conmutación de tramas, ya que además de soportar servicios como multimedia, fue diseñada con el fin de interconectar redes LAN y WAN.

Debido a que ATM puede soportar servicios orientados a conexión punto a punto, se podrán alcanzar nuevos niveles de desempeño, confiabilidad, seguridad y administración en redes.

4.4.3 Ventajas de la Conmutación

Las principales ventajas ofrecidas por estas dos maneras de conmutación se reflejan en el ancho de banda incremental que poseen, además de contar con las facilidades y características de la administración de redes virtuales.

4.4.4 Ancho de Banda Dedicado e Incremental

El ancho de banda dedicado se utiliza principalmente para servidores y dispositivos que requieren enviar gran cantidad de tráfico, y esto mejora substancialmente el desempeño y administración de una red.

La conmutación provee un ancho de banda dedicado y en caso de que más dispositivos sean conectados a la red ofrecerá un mayor ancho de banda para acomodar el incremento de tráfico. Esto mejora en gran medida las capacidades de manejo del tráfico, particularmente cuando se está acoplado a una red virtual.

4.4.5 Redes Virtuales

Una de las características más importantes de la conmutación es la posibilidad de manejar redes virtuales, también conocidas como LANs virtuales (VLANs).

Las redes virtuales separan la topología lógica de la LAN de la topología física.

Las estaciones que forman parte de una red virtual pueden estar distribuidas a todo lo largo de un campus pero siguen interactuando como si estuvieran conectadas a un mismo segmento de red.

El beneficio principal de esto es la posibilidad de administrar el tráfico, el crecimiento y en sí, la red de manera más flexible, que la que se presenta en las redes LAN de medios compartidos a base de ruteadores y puentes.

4.4.6 LANs Conmutadas

La gran ventaja de este tipo de conexión sobre la de medios compartidos se puede ver claramente al comparar el funcionamiento de la red con conmutación ATM contra la de FDDI, según se vio en un ejemplo anterior.

La forma en que esto funciona es mediante un envío directo al destino sin perder tiempo en analizar la información, entonces podremos conectar varios enlaces entre dos conmutadores a fin de aumentar el ancho de banda según sea requerido. Como ejemplo, podremos decir que si manejamos la conexión de 4 enlaces entre dos redes Ethernet de 10 Mbps, por cada

uno de ellos se podrán manejar los 10 Mbps de manera simultánea y bidireccional, pudiendo entonces conectar en el mismo tiempo a ocho estaciones de trabajo. Esto equivaldría a decir que tenemos un ancho de banda de 40 Mbps.
A este tipo de conexión se le conoce como "Multilíneas".

4.4.7 Microsegmentación

Es un método para mejorar el desempeño de una red en el cual se va dividiendo una LAN en múltiples segmentos, dedicando cada segmento a un sólo usuario o estación terminal.
La microsegmentación mejora el desempeño al permitir comunicaciones simultáneas en cada segmento, es decir comunicaciones paralelas múltiples, reduciendo a su vez el tiempo de acceso a la red.
La microsegmentación implica un cuidadoso estudio para conectar las estaciones a los segmentos adecuados aislando la mayoría del tráfico a segmentos específicos, sin embargo, surge la necesidad de interconectar los microsegmentos para casos en donde dos estaciones de microsegmentos diferentes se tuvieran que comunicar.
Una conexión por ruteadores no es recomendable ya que sería muy difícil para éstos manejar todo el tráfico agregado de las estaciones, comunicándose simultáneamente si se contempla en un ambiente de gran escala y geográficamente disperso.

4.4.8 Una Alternativa por Conmutación

La conmutación ofrece una solución a los problemas de administración y desempeño del ruteo de microsegmentación mediante la implementación de sistemas flexibles de alta velocidad, creando rutas directas a través de conmutadores que con la utilización de las direcciones MAC entregan los datos a la estación final indicada.
Los conmutadores generan múltiples conexiones a la vez, permitiendo la comunicación paralela de los múltiples usuarios. Estas conexiones de alta velocidad pueden destinarse a servidores o a dispositivos conectados al backbone, mejorando de manera importante el desempeño de la red.
La tecnología de conmutación puede utilizarse para resolver muchas de las limitaciones operativas generadas por los ruteadores:
La red conmutada puede ser administrada para crear redes lógicas interconectando usuarios por medio de software de acuerdo con las necesidades inmediatas de comunicación que se tengan, independiente del lugar físico dónde se encuentre la estación o usuario. Dispositivos como servidores, compuertas o equipo de prueba pueden asignarse a las redes lógicas de la misma manera.

4.5 Conmutación de células ATM

Como se dijo en el capítulo I, ATM está basado en la conmutación de células y es una tecnología de conmutación orientada a conexión y es utilizada en redes de área local y amplia. ATM es escalable y permite virtualmente un número ilimitado de usuarios con un ancho de banda dedicado y de alta velocidad, hacia los demás usuarios o hacia los servidores principales.
ATM ofrece ventajas significativas sobre las soluciones existentes en casos tanto de Backbone en un campus como configuraciones de oficina:

- La velocidad de ATM es mayor que la del Backbone distribuido basado en FDDI y el Backbone colapsado basado en ruteadores.
- ATM provee un significativo incremento en el ancho de banda disponible para los usuarios, debido a su característica de ancho de banda dedicado.
- Las velocidades de los enlaces entre nodos de conmutación pueden ser escalables para alcanzar requerimientos de tráfico específico.
- ATM permite la integración de ambientes LAN-WAN, esto debido a que el esquema de direccionamiento y formato de las células en ambos ambientes es la misma.
- ATM soporta simultáneamente tráfico de video, audio y datos.

4.5.1 Comunicación entre conmutación Ethernet y conmutación ATM

ATM es utilizado principalmente en conexiones a servidores. Las conexiones de gran ancho de banda de ATM a servidores, pueden ser compartidas con usuarios en Ethernet de menor ancho de banda conectados a una red ATM con un conmutador Ethernet. Esto permite, a servidores ATM comunicarse con clientes Ethernet para interactuar como si estuvieran ambos en una Ethernet.

4.5.2 Diferencias entre ATM y las LANs convencionales

La diferencia más importante entre la tecnología ATM y la tecnología del medio compartido, (utilizada por FDDI, Ethernet y Token Ring) es el uso, en ATM, del canal dedicado, longitud fija de la célula y orientación hacia conexión.

- ATM usa conexiones dedicadas que corren en paralelo. En contraste, las redes con el medio compartido, usan la operación en serie, donde los usuarios tienen que esperar para tener acceso al medio de transmisión y sólo una transmisión se puede hacer al mismo tiempo. Con ATM, se pueden tener varias conversaciones simultáneas a través del mismo conmutador, por lo cual la velocidad de transmisión real de cada nodo permanece constante, aunque se incremente el número de estaciones en la red.
- ATM toma los paquetes de longitud variable usados en comunicaciones convencionales y mapea estos paquetes en células de longitud fija. Los datos segmentados son rearmados en el destino, simplemente concatenando cada célula. Las células de longitud fija, permiten la entrega simultánea de datos e información sensibles a la latencia, como voz y video, utilizados en aplicaciones multimedia.
- La naturaleza de ATM orientada a conexión significa que los canales virtuales proveen rutas dinámicas múltiples entre fuentes y destinos, garantizando así un ancho de banda determinado.

4.6 Tendencias en redes LAN y WAN

Es claro en este momento, que la tendencia de la tecnología se orientan a soluciones en ATM. Esto es debido a las ventajas que ofrece esta tecnología comparada con las demás como se trató anteriormente.

En el futuro será una solución común la integración de ATM en el Backbone, así también proveer conectividad con servidores de grupos de trabajo virtuales.

Así mismo integrando clientes virtuales en LAN con 10BASE-T con servidores en 100BASE-T a 155 Mbps, a través de una infraestructura de LAN virtual.

Lo anterior se muestra en la figura 4.5.

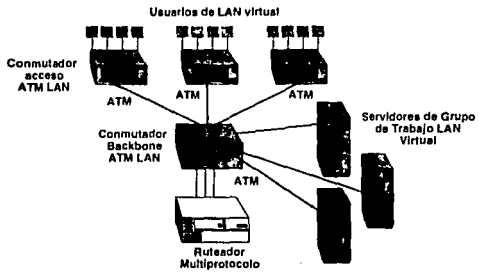


Figura 4.5. Red LAN basada en un Backbone de ATM.

Dado que ATM también tiene la capacidad de conexión a WAN, es claro que al tratarse de una tecnología que soporta ambos ambientes, LAN y WAN, será utilizado para soluciones en WAN.
Una aplicación típica (ver figura 4.6) sería para la integración de voz, datos y video sobre un Backbone WAN ya sea público o privado.

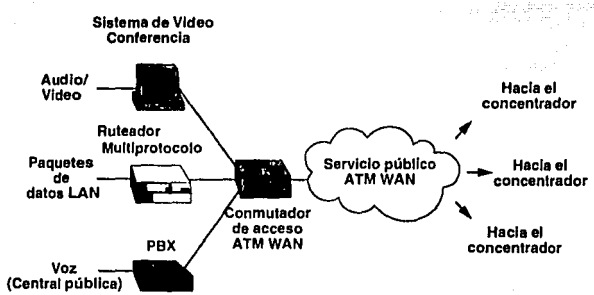


Figura 4.6. Integración de Datos, Voz y Video sobre una red pública de ATM.

También se prevé su uso para la conexión LAN a alta velocidad entre ruteadores, a través de la WAN de ATM.
Lo anterior está representado en la figura 4.7.

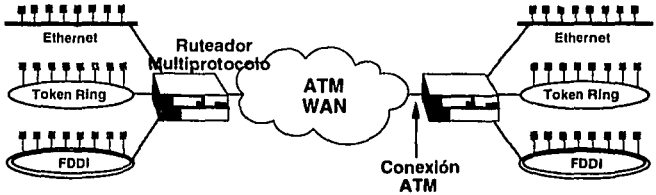


Figura 4.7. Conexión LAN de alta velocidad entre ruteadores usando ATM.

CAPÍTULO V

CASOS REALES.

CAPITULO V

CASOS REALES

5.1 CASO 1.- Organización Universitaria

Dentro de una Universidad se necesita integrar una red para dar servicio aproximadamente a 2000 usuarios, los trabajos que se realizan dentro de esta organización están enfocados a la investigación. El campus se compone de 5 edificios con 6 pisos cada uno, conteniendo computadoras personales IBM, estaciones de trabajo UNIX y computadoras Macintosh que se encuentran en redes LAN Ethernet por piso y en dos ambientes, también hay algunos ruteadores y puentes.

La figura 5.1. nos muestra una vista aérea de dicho campus.

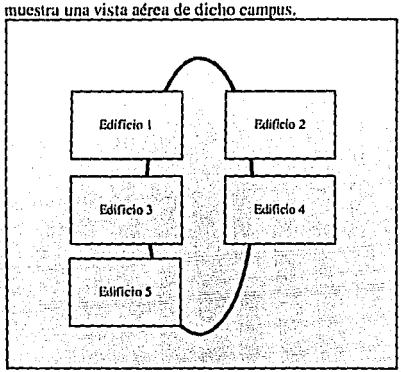


Figura 5.1 Red de campus Universitario.

Un requerimiento en esta red, es que se tenga control de acceso a la misma y que sea segura.

5.1.1 Desarrollo

En este caso la red que se pretende instalar o adecuar debe estar enfocada al proceso de Investigación, controlando el acceso y que su utilización sea segura.

5.1.2 Recolección de Información

En el campus se alojan Estaciones de trabajo, Risk 6000, Computadoras personales IBM y Computadoras Macintosh. La red actual instalada se compone de redes LAN ubicadas en cada uno de los pisos teniendo por separado a la LAN para las computadoras Macintosh.

La capacidad que se requiere cubrir es de 2000 usuarios, utilizando aplicaciones como bases de datos, programas de simulación, graficadores, diseño, etc. donde el tiempo de

utilización de los usuarios por aplicación es Alto, así como los datos que tiene que manejar la red hacia los dispositivos.
El enlace existente entre las redes de cada edificio es por medio de Ruteadores y Puentes, y el cableado instalado es UTP categoría 5, según se muestra la figura 5.2.
En la nueva red también se desea que se pueda implementar el uso de otros servicios como Correo Electrónico, Fax, conexión a otros Centros de cómputo y que además esta red pueda expandir su capacidad en un 20% en 2 años.

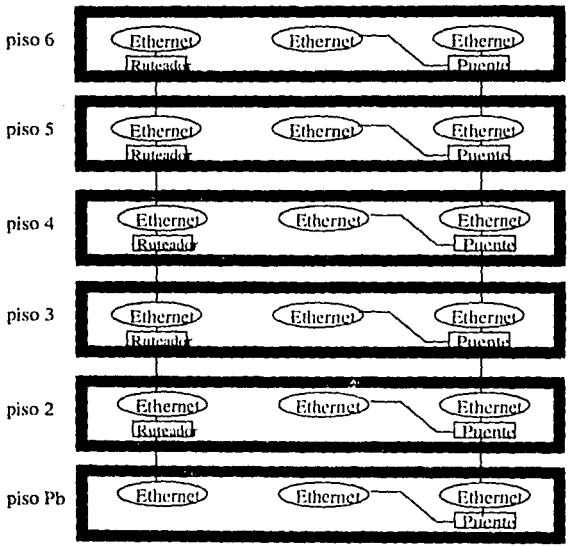


Figura 5.2 Red de Campus actual.

5.1.3 Planteamiento

Como esta es una red de alta densidad y se desea integrar a cada LAN Ethernet de cada piso con los demás edificios; se propone lo siguiente:

En cada edificio.- Se emplearían 4 conmutadores Ethernet que formarían la parte de control de cada uno de los edificios. La estructura de estos conmutadores sería de la siguiente forma:

- Los primeros 2 conmutadores interconectarían a los pisos Planta Baja, Tercero y Quinto.
- Los conmutadores 3 y 4 integrarían a los pisos Segundo, Cuarto y Sexto.

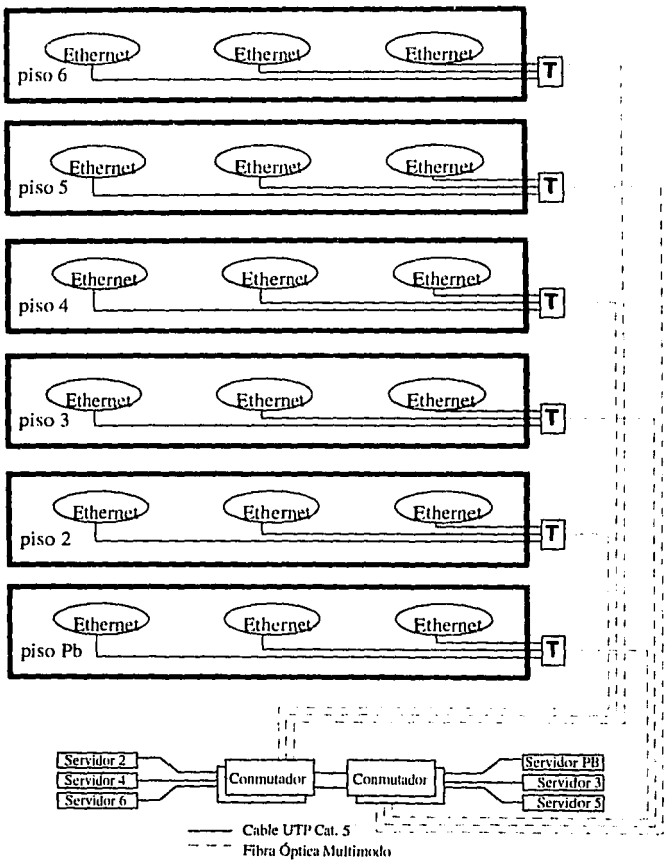


Figura 5.3 Diagrama de solución para campus Universitario.

La razón de tener los conmutadores Ethernet por pares es para lograr la seguridad que se desea en la red, ya que sólo uno de estos conmutadores se encontrará activo, mientras que el otro se encontrará en estado de reposo, si ocurriera alguna falla en el conmutador activo, el otro se activaría y tomaría la carga (Redundancia en los Conmutadores).
Como en cada piso se encuentran 3 LAN cada conmutador redundante integraría a 3 pisos, el número de LANs que soportaría cada Conmutador redundante sería de 9 segmentos; además de 3 Servidores (uno para cada piso). La conexión de los segmentos de LAN a los Conmutadores sería en Estrella (Ver figura 5.3).
La topología en estrella se emplea para tener control de cada uno de los segmentos de LAN, ya que todas pasan por un punto único; además que en caso de presentarse una falla de algún segmento, sólo se aísle el segmento que presenta el problema.
Los 2 conmutadores redundantes (4 conmutadores) por edificio se interconectarían entre ellos y con un ruteador, a través de puertos dedicados en los conmutadores y con esto se garantiza que el ancho de banda disponible sería del orden de cientos de Mbps, esto se puede apreciar si se observa la figura 5.4.
El empleo del ruteador es para realizar la interconexión de cada edificio al conjunto.

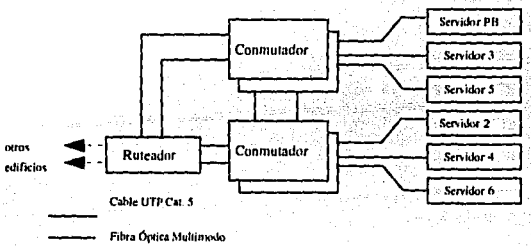


Figura 5.4. Diagrama de conexión de entre Conmutadores Ethernet y Ruteador

Para el Campus de los 5 edificios.- Como se menciona anteriormente los edificios estarán interconectados por medio de un ruteador en cada uno de los cinco edificios que componen el campus utilizando una topología de anillo doble FDDI, esta topología nos proporciona seguridad en su conexión, y el soporte de respaldo requerido.
El cableado que emplearíamos sería el siguiente:

- Para las LAN Ethernet cable UTP Categoría 5
- Para el cableado entre las LAN Ethernet y los Conmutadores redundantes sería fibra óptica multimodo y esta sería doble; ya que un cable va al conmutador activo y el otro al redundante, por lo que en caso de falla en alguno de los conmutadores o en el cableado ningún punto quedaría aislado.
- El cableado entre los conmutadores redundantes y el ruteador seria por medio de fibra óptica multimodo.
- Los ruteadores del anillo doble FDDI serían conectados con fibra óptica multimodo.
- El empleo de estos tipos de cable y fibra óptica se puede corroborar en la tabla 4.2.

Para realizar la interconexión entre el cableado de Fibra óptica multimodo horizontal de los edificios y el cable UTP categoría 5 en los segmentos LAN se emplearía el uso de transceptores UTP-FOIRL.

5.1.4 Ubicación de los Servidores

Los servidores estarán alojados en la misma sala donde se encuentren ubicados los conmutadores e interconectados al conmutador que le corresponda, pudiendo ser esta conexión por medio de puertos dedicados.

5.1.5 Administración

Para la administración de la red se debe tener presente que tipo de plataforma tiene implementada, y en este caso son UNIX y DOS.

5.1.6 Equipamiento

Los equipos a emplearse son los siguientes:
Por Edificio:

ÍTEM	EQUIPO	CANTIDAD
01	Conmutador Ethernet	4 pzas
02	Servidor	3 pzas
03	Transceptor	48 pzas
04	Ruteador	1 pza
05	Cable UTP 5	60000 m
06	Fibra óptica multimodo en edificios	10000 m
07	Fibra óptica multimodo en anillo	4000 m
08	Bastidor	8 pzas
09	Pánel de parcheo de 36 puertos	18 pzas
10	Pánel LIU	2 pzas
11	Plataforma de Administración	1 paquete

Gastos de Instalación y Puesta en Servicio

Concepto	Costo en base al total de equipo empleado en el Proyecto
Administración del Proyecto	2.0%
Canalización entre edificios	10.0%
Canalización de edificios	20.0%
Conectores y Material de instalación	2.5%
Instalación y puesta en operación	10.0%

Los cálculos de las cantidades fueron hechas en base a los siguientes criterios:

- Empleo de 1 bastidor, 1 transceptor, 3 paneles de parcheo (36 puertos) por cada piso, además de dos gabinetes adicionales para los conmutadores,servidores y 2 páneles LIU

- Se considera una distancia de 30 mts de cable UTP Cat. 5 por terminal, 2000 mts. de fibra óptica por troncal de cada edificio y 4000 mts adicionales para el anillo doble FDDI
- En la parte de gastos de instalación y puesta en servicio, los porcentajes que aparecen por dichos conceptos, representan el costo adicional que tendrán en base al valor del equipo.

Ejemplo: Si el total del equipo a instalar es de N$10,000, por concepto de instalación y puesta en servicio se cobraría una cantidad de N$1,000.

5.2 CASO 2.- Institución Bancaria

Dos edificios principales de 4 pisos que se encuentran ubicados en una cuidad, están enlazados a un centro de datos fuera del área metropolitana y también están interconectados con 25 oficinas filiales que se encuentran en diversas partes del mundo.

Quieren implementar un nuevo cableado estructurado dentro de los edificios, que les pueda ofrecer un mejor control de su sistema, además de tener presente una migración hacia ATM.

También requieren que se centralicen los Servidores, así como la segmentación de las redes LAN.

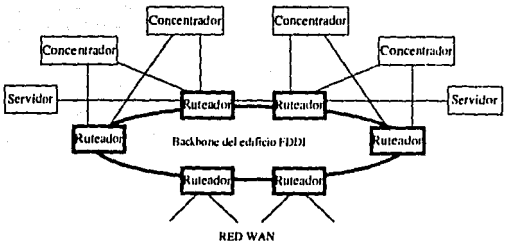


Figura 5.5. Estructura de Red Actual de Institución Bancaria

Como se observa en la figura 5.5 el edificio tiene un backbone de anillo FDDI y por medio de ruteadores interconecta a los servidores y concentradores por medio de enlaces duplicados, así como enlances de E1 hacia una red WAN.

Dentro de los concentradores, se encuentran conectados los diferentes segmentos Ethernet LAN.

5.2.1 Desarrollo

En este caso se tiene que cumplir con los siguientes objetivos:

- Mejor control de su sistema
- Implementación de cableado estructurado
- Centralización de Servidores
- Segmentación de las Redes LAN existentes

- Migración hacia ATM

5.2.2 Solución

El backbone del complejo tendría una topología FDDI Anillo/Árbol, esto quiere decir que la conexión entre los dos edificios será mediante dos anillos duales (Topología FDDI).
Para interconectar este anillo se emplearían enlaces dobles a cada uno de los ruteadores ubicados en cada piso y éstos a su vez se conectarían a un concentrador (Gabinete de cableado), si tomamos como referencia cualquiera de los dos conmutadores del edificio, se puede apreciar que el backbone (sin considerar el anillo dual FDDI) estaría en una configuración de árbol, lo cual se puede apreciar en la figura 5.6.

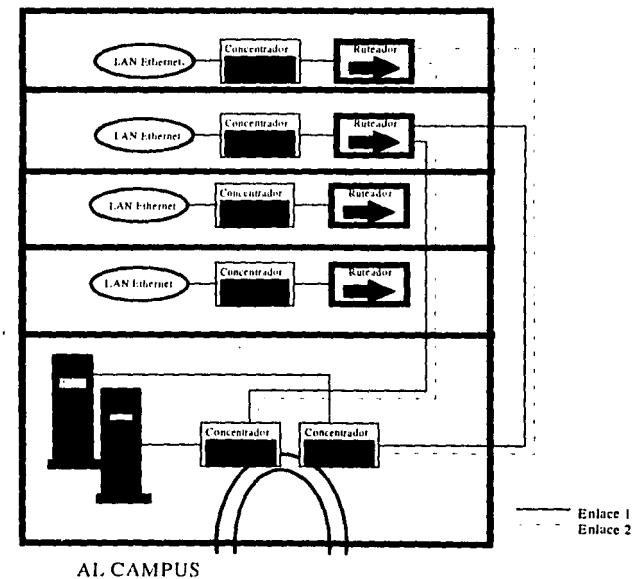


Figura 5.6. Diagrama de solución del Backbone.

Para cada edificio la topología del Backbone sería Distribuida, esto quiere decir que los segmentos de redes LAN irán conectados a un concentrador ubicado en cada piso (Gabinete

de Cableado) con un Ruteador de FDDI que se interconectará con el doble enlace de cada uno de los dos concentradores del anillo doble FDDI que se mantiene entre los dos edificios.

El cableado requiere ser de tal forma que se pueda implementar en segmentos de red Ethernet, Token Ring y FDDI , además debe estar preparado para migrar hacia ATM.
Si observamos la tabla 4.2, observamos que recomienda lo siguiente:

- Para el cableado horizontal, el empleo de UTP categoría 5 entre las LAN y los Gabinetes de Cableado.
- Para el cableado vertical y horizontal en este campus, el empleo de fibra óptica multimodo.
- Para el cableado de redes MAN, el empleo de. de enlaces E1.

(ver figura 5.7)

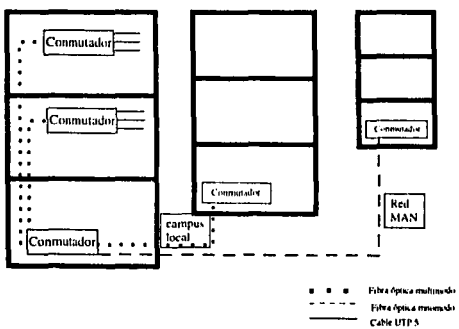


Figura 5.7 Solución de cableado estructurado

Para este caso se emplearía un Servidor para cada piso.
La administración seria de un modo centralizado .

5.2.3 Equipamiento

Por los dos edificios:

Enlace con base de Datos

ÍTEM	EQUIPO	CANTIDAD
01	Concentrador	6 pzas
02	Servidor	4 pzas
03	Ruteador	1 pza
04	Cable UTP 5	** m
05	Fibra óptica multimodo en edificios	16000 m
06	Fibra óptica multimodo en anillo	4000 m
07	Bastidor	12 pzas
08	Panel de parcheo de 36 puertos	24 pzas
09	Panel LIU	2 pzas
10	Plataforma de Administración	1

** En este caso no se conoce el numero de terminales, por lo que no se puede estimar este dato.

Gastos de Instalación y Puesta en Servicio

Concepto	Costo en base al total de equipo empleado en el Proyecto
Administración del Proyecto	2.0%
Canalización entre edificios	10.0%
Canalización de edificios	20.0%
Conectores y Material de instalación	2.5%
Instalación y puesta en operación	+10.0%

Los cálculos de las cantidades fueron hechos en base a los siguientes criterios:

Empleo de 1 bastidor, 3 páneles de parcheo (36 puertos) por cada piso, además de 1 bastidor por piso y 2 paneles LIU

Se consideran 2000 mts. de fibra óptica por troncal de cada edificio y 4000 mts adicionales para el anillo doble FDDI

En la parte de gastos de instalación y puesta en servicio, los porcentajes que aparecen por dichos conceptos representan el costo adicional que tendrán en base al valor del equipo. Ejemplo: si el total del equipo a instalar es de 10,000 Nuevos pesos, por concepto de Instalación y puesta en servicio se cobraría una cantidad de 1,000 Nuevos pesos

5.2.4 Alternativa futura

Como se tiene implementado un cableado estructurado, el cual esta preparado para ATM, el ejercicio se podría resolver sustituyendo los equipos de la siguiente forma:

Para cada uno de los pisos.- Tanto los concentradores, como los ruteadores se sustituirían por conmutadores ATM, así mismo los que conformaban el backbone también, se cambiarían por conmutadores. Siendo que la conexión entre cada Conmutador de piso hacia los conmutadores principales estaría duplicado. Por último estos dos concentradores estarían conectados a un ruteador multiprotocolos, por lo que si observáramos el backbone este tendría una topología colapsada. La cual se repetiría en cada uno de los edificios y cada ruteador multiprotocolo se conectaría a traves de los enlaces E1 hacia el edificio de la base de datos (WAN), donde se ubicaría otro ruteador multiprotocolos y otro conmutador redundante ATM. Según se muestra en las figuras 5.8. y 5.9.

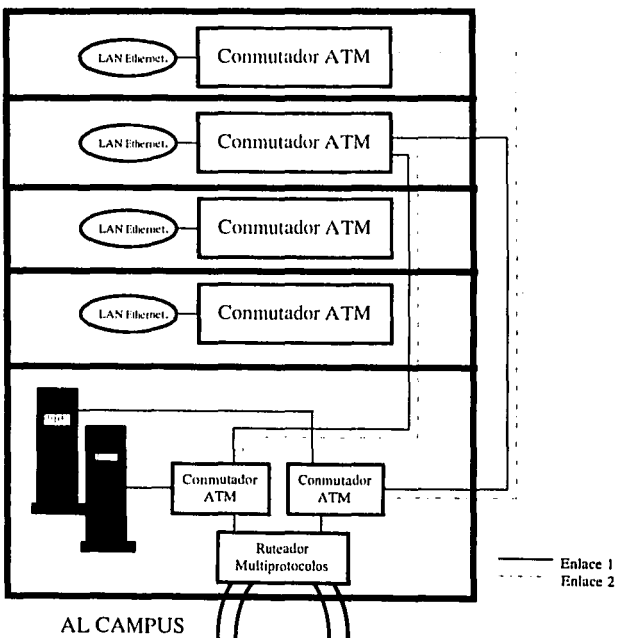


Figura 5.8 Solución con Conmutadores ATM

Con el empleo de conmutadores en cada uno de los pisos el enrutamiento y concentración de los segmentos se encuentra integrado y esto reduce los tiempos de latencia. Como en ATM cada equipo que se encuentra conectado al conmutador se transporta usando el máximo ancho de banda, no es necesario realizar conexiones dedicadas a puertos como sucede al emplear Conmutadores de Ethernet.

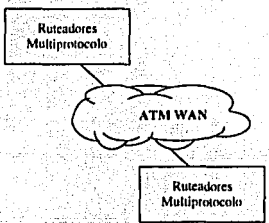


Figura 5.9 Comunicación WAN entre Edificio principal y Edificio Base de Datos

CAPÍTULO VI

ADMINISTRACION DE REDES

CAPITULO VI

ADMINISTRACIÓN DE REDES

6.1 Introducción a la administración de redes

Hoy en día los ambientes de red en los negocios y en la industria llegan a ser extremadamente complejos. El progreso se da a partir de las primeras redes de área local sencillas, las cuales se han extendido hasta formar WANs.

El 75% de todo el cableado reside ahora en los concentradores inteligentes. Los ruteadores conectan a las LANs a oficinas remotas y los superconcentradores reciben toda esta información. El monitoreo y la reconfiguración de estos sistemas, sin mencionar la solución de problemas, pueden llegar a ser muy complejos y difíciles en estos sistemas.

Los sistemas de administración de redes se desarrollaron para ofrecer una solución a los problemas de manejo y supervisión de las redes.

Con estos sistemas el administrador de la red esta en posiblidad de prevenir, más que corregir las posibles fallas del sistema, además de representar una poderosa herramienta para el diseño e implementación de la red.

Antes de implantar un software para la administración de la red, es importante examinar las plataformas y sistemas con que se cuenta actualmente, y entonces definir una serie de pasos y criterios que nos permitan elegir un sistema de administración de red que maneje efectivamente el control y mantenimiento de los sistemas complejos de LANs.

Para tener una administración adecuada de red se debe utilizar una combinación apropiada de hardware y software, lo cual proporcionará un manejo eficiente de redes a un bajo costo.

Así mismo se debe considerar que el administrador de redes pueda manejar diferentes topologías, permitiendo reducir los tiempos empleados en la solución de problemas en comparación de los que se presentan con una administración manual.

Para lograr una óptima administración en redes muy grandes, se deberá distribuir la administración mediante el uso de concentradores inteligentes que dividirán a la red en segmentos, como podría ser un departamento, una zona geográfica o bien un grupo de usuarios.

La administración inteligente esta distribuida en forma de agentes y aplicaciones de administración, las cuales trabajan en forma residente en los concentradores, servidores, tarjetas de red, ruteadores y demás equipo de la red, preparado para este fin. Esto se logra con módulos insertados en los concentradores o hardware de cada equuipo que es llamado Módulo de Administración de Red. (NMM).

Los agentes administran la recolección de información dentro del concentrador, el cual reduce las aplicaciones y tráfico del administrador central, mejorando el desempeño de la red. Una vez recolectados los datos son enviados al administrador central, en donde un software despliega el estado de la red mediante el uso de gráficas.

Debido a que la recolección, análisis y condensación de los datos se efectúa en los concentradores inteligentes, estos sólo envían la información relevante hacia el administrador central evitando generar gran cantidad de tráfico sólo para señales de control.

Podemos mencionar cuatro áreas de administración de redes:

a. *Administración*: Contempla todas las funciones necesarias para regular el desempeño de la red, como serían, mantenimiento, actualización de usuarios y de la configuración, retener información acerca de los nodos, estadísticas de tiempos de uso por usuarios, así como de la recolección y presentación de datos estadísticos sobre el desempeño general de la red.

b. *Mantenimiento*: Esta función examina y lleva el historial de errores y fallas ocurridas en la red; permite localizar puntos de falla en líneas, nodos o subredes y en caso necesario, se activa una alarma para que personal capacitado intervenga en la reparación de la falla.

c. *Control*: Este incluye control de acceso y direcciones de canales, entre otras funciones de control de la red. Por ejemplo, se puede manejar la seguridad de la red e incluir restricciones de acceso a ciertos usuarios a determinados archivos o programas residentes. Se puede restringir el acceso a porciones de la red para un usuario que no esté autorizado.

Otro aspecto del control son las prioridades para el acceso a la red, normalmente en sistemas distribuidos todos tienen la misma oportunidad de acceso, sin embargo algunas estaciones, usuarios, mensajes o servicios pueden tener alto grado de prioridad, y así utilizar los canales de enlace con preferencia sobre los demas.

d. *Manejo y administración de redes virtuales*. Este tipo de administración también es manejado por cieros concentradores y consiste en asignar a uno o varios usuarios a los recursos de otro segmento o subred.

Todas las funciones de administración de red son ejecutadas en una computadora de la red llamada NMS(Network Management Station), la cual utiliza un software sobre alguna plataforma de cualquier sistema operativo, incluso algunos de estos sistemas de administración son muy sencillos de operar.

Si la estación de administración presenta una falla, se puede afectar negativamente la operación de la red, entonces se recomienda en sistemas distribuidos eficientes tener un segundo dispositivo de administración que debe ser incorporado para obtener redundancia. En el caso de que falle el primero, el segundo administrador de red (respaldo) toma el control del sistema.

6.2. Funcionalidad y características de los sistemas de administración de redes

Lo primero que se debe de saber son las necesidades de administración que se requieren. En el capítulo III se trató el tema de la forma de recolectar la información.

Las necesidades en una red como podrían ser: la detección de fallas del cableado estructurado, un mayor control, establecimiento de la seguridad, detección de funcionamiento incorrecto del hardware o bien simplemente poder hacer un cambio en los direccionamientos. Lo que nos lleva a que la administración de red deberá encargarse de facilitar todos estos trabajos.

Existen algunas consideraciones importantes cuando seleccionamos un sistema de administración de redes:

1. *Fallas del cableado estructurado*: Los administradores de red deben identificar fallas en el cableado y pérdidas de la comunicación en todo el

sistema. Con la identificación y aislamiento de esas fallas de comunicación los problemas podrán ser resueltos fácilmente.

2. *Control*: Los administradores de red deberán controlar la red desde un punto central, ya que se recibe toda la información desde los concentradores indicando el estado de cada uno de los equipo.

3. *Fallas en el hardware*: Cuando un ruteador de un nodo crítico llega a fallar, todo el sistema podría fallar también. El administrador de red debe dar la facilidad de sonar una alarma. Esto es primordial para asegurar el funcionamiento de la red.

4. *Seguridad*: Algunos paquetes de administración de redes permiten especificar cuales servidores pueden ser accesados y cuales estaciones de trabajo pueden conectarse a ellos. El aseguramiento en las puertas de acceso a los concentradores y equipo central es lo primero que se debe de hacer para mantener alejado al personal no autorizado.

5. *Reorganización de la distribución*: El saber donde van a estar los concentradores, puentes, ruteadores, estaciones de trabajo y servidores debe ser importante. El reorganizar la distribución permite a los sistemas de administración dibujar un mapa de todos los dispositivos.

6. *Soporte técnico eficiente*: El 80% de las fallas pueden ser resueltas en un par de minutos con una administración de red y casi 20% restante pueden ser resueltos en algunos minutos. La administración de la red da la habilidad de ver inmediatamente al sistema entero y así determinar el origen y posiblemente la naturaleza de la falla sea de hardware o software.

6.2.1 Interface gráfica en la administración de redes

Una eficiente administración de redes debe proveer una manera sencilla de trabajar y una interface altamente visible. Un sistema basado en gráficas provee una funcionalidad amigable, permitiendo ver la red desde una vista global hasta una vista particular de un terminal de trabajo.

La administración de redes utiliza el protocolo SNMP (Single Network Management Protocol). Este estándar de administración ofrece muchas formas de ver los sistemas de redes, incluyendo una vista global, una vista intermedia de un anillo o un segmento en particular hasta llegar incluso a una vista de un elemento de la red.

a. *Vista Global*: Es una representación de como está construida la red. Esta nos permite ver donde están conectados los ruteadores, anillos, segmentos y puentes.

b. *Vista intermedia*: Es una representación de donde están localizadas la estaciones de trabajo, los concentradores inteligentes, ruteadores y puentes en cada anillo o segmento en particular.

c. *Vista de un elemento de red*: Es una vista gráfica expandida del dispositivo administrado como puede ser un concentrador, un puente o un ruteador. Si este es un sistema en servicio puede proveer una vista del estado del dispositivo.

6.2.1.1 Creación manual del mapa de la red

Un mapa representa a toda la red dividiéndola en diferentes figuras, cada una de las figuras representa un segmento de la red, por ejemplo cada figura puede representar el departamento de contabilidad de una compañía grande.
Para crear un mapa se realiza en primer lugar un dibujo llamado dibujo superior (Top picture), éste es usado como base para enlazarlo a otras figuras llamadas dibujos inferiores (Subpictures). El dibujo superior es el más extenso y da una visón total de la red.
Cada uno de los dibujos es un símbolo que representa un segmento, estaciones, componentes y cables para toda la red, debiendo estar cada uno de estos etiquetados con un texto que permita identificarlos, describirlos o moverlos a un lugar distinto de la red.
De esta forma el mapa de toda la red es creada por una persona la cual le dice a la computadora administradora toda la configuración de la red.
Se pueden. crear múltiples mapas dentro de una red por ejemplo, una geográfica o física y otra lógica.
El mapa físico o geográfico describe una vista global en su figura superior separada en otras subcapas como son país, estado, ciudad, edificio, piso, etc.
La representación lógica puede mostrar los departamentos de ingeniería, contabilidad y comercialización de una empresa como entidades separadas, donde se ven todos los componentes de la subred sin importar la localización física.

6.2.1.2 Creación automática del mapa de la red

Cuando se tiene una red muy extensa y complicada se debe de tomar en cuenta un programa de administración que maneje una utilería que nos permita crear un mapa de la red en forma automática. Esto se logra gracias a la utilización de la información de las direcciones TCP/IP, el sistema es capaz de buscar éstas desde los módulos NMM y de los puentes basados en el protocolo SNMP. Existe una gran diferencia entre los mapas creados manualmente y éstos, ya que organiza el mapa en diferentes vistas
Para que funcione la configuración automática se debe cumplir con los siguientes requisitos:

1. Contar con agentes avanzados SNMP en los equipos de interconexión, para que puedan ser manejados por la estación NMS.
2. Configurar el módulo de un puente o ruteador con una dirección IP. En caso de requerir incorporar segmentos o redes nuevas se tendrá que actualizar la base de datos.

Existen dos tipos de vistas una estática y una dinámica.
La vista estática es usada para organizar a los componentes de la red por tipos. Por ejemplo: ruteadores en una vista y todos los puentes en otras.
Si algunos de los dispositivos no son administrables a través del programa de administración se pueden crear iconos de estos, teniendo entonces una vista estática de ellos.
La vista dinámica es creada automáticamente por el programa de administración y se puede administrar desde ésta, ya que se tiene una información en tiempo real del estado de toda la red.
Una característica importante que debe tener una buena administración es el que contemple las vistas dinámicas.

6.2.2. Aplicaciones del programa de administración

El programa que se instale debe de permitir una serie de aplicaciones como son: monitoreo, administración de la base de datos MIB, emulación de terminal y pruebas del acceso a distintos puntos de la red.

6.2.2.1 Monitoreo de la red

Esta aplicación es conocida como administración de medición y recolecta automáticamente datos para desplegarlos en el medidor o graficador. Estos valores de objetos MIB son calculados por fórmulas definidas por la persona que administra la red para después ser desplegados. Las mediciones que realiza son de utilización del canal, errores, colisiones, y funcionamiennto correcto de una gran variedad de dispositivos. Esto puede ser realizado en cualquier punto de la red desde segmentos enteros hasta puertos individuales.

Deben de tener varias herramientas que permitan evaluar el estado de la red. Herramientas de diagnóstico, tales como, análisis de actividad y opciones de grabación, las cuales permitirán ver el tráfico de la red en tiempo real ya sea de un anillo o segmento, de un módulo o bien de un puerto.

Así mismo será conveniente que cuente con reportes de eventos, grabando sólo aquellos que rebasen el límite preestablecido por las políticas de administración.

La información de este evento puede ser utilizada para tomar acciones y reparar la operación de la red cuando se ha detectado una falla.

Por ejemplo, cuando un puente empieza a trabajar por debajo del desempeño preestablecido, automáticamente se puede hacer una partición automática del resto de la red, aislando así el puente hasta que pueda ser investigado el problema.

Los errores en una vista global de la red deben ser reportados a través de alarmas por diversos mecanismos.

Como ejemplo tenemos:

1. El cambio de color de los íconos en el mapa de la red.

   El verde significa que el nodo o el componente está en buen estado.

   El naranja o amarillo significa precaución y que una condición no crítica se esta presentando, como sería que se esta excediendo el umbral programado.

   El rojo significa una falla crítica indicando que un nodo o dispositivo está deshabilitado y que no existe comunicación con la red.

   El azul puede representar un estado indeterminado es decir que no se sabe de un nodo o componente ya que éste no reporta su estado o bien que el mapa ha cambiado y el estado no se ha reportado todavía.

   El magenta que existe una falla de bajo nivel en su rama.

   El azul turquesa significa que un puente se encuentra en modo de espera en una configuración "Spanning tree".

2. A través de un mecanismo de alarma basado en "traps"(agentes para situaciones de alarma)

3 O a través de alguna facilidad de alarma del software propietario (sunet manager, netview 6000, H.P. openview)

El monitoreo de red en tiempo real permite al administrador de red evaluar el estado de los dispositivos en una red Ethernet o Token Ring, por lo que es una característica importante con la que debe contar el software. El proveer la información en formato gráfico y

estadístico de varios niveles incluyendo el global, el plano (flat), el segmento y el expandido es altamente deseable.

6.2.2.2 Administración de la base de datos MIB

Esta aplicación permitirá recuperar, desplegar, registrar y modificar continuamente los valores de los objetos MIB recolectados de los dispositivos compatibles con SNMP.

6.2.2.3 Emulación de terminal

Esta aplicación permitirá la administración de una gran variedad de dispositivos que particularmente no soportan agentes SNMP pero si soportan Telnet.

6.2.2.4 Prueba de acceso a distintos puntos de la red

Esta es una característica de gran ayuda y que deberá ser tomada en cuenta para la selección del software de administración, ya que con ella se puede verificar la conectividad a distintos dispositivos de la red.
En esta aplicación se utiliza el programa PING (Packet InterNet Group) para probar el acceso de los destinos. Una solicitud de eco ICMP es enviada a una dirección IP de destino a través de la red y espera un momento, si éste regresa completamente al punto de origen, significará que el destino se encuentra disponible. Entonces el protocolo de ICMP envía un comando ECHO_REQUEST y se obtiene una respuesta en la forma ECHO_RESPONSE de algún host o concentrador en particular.
El PING es soportado tanto para Token Ring como para Ethernet, así como por cualquier dispositivo que soporte TCP/IP.

6.3.Conectividad de un sistema administrador de red

Los sistemas de administración de redes deben tener la capacidad de trabajar con una gran variedad de sistemas operativos, administradores SNMP y plataformas de estaciones de trabajo. Esto se debe a que una organización no puede ser construida para soportar un cierto tipo de estación de trabajo o sistema operativo y seleccionar un solo sistema que le permitirá trabajar y realizar todas las tareas requeridas a su total potencial. Sin embargo, es importante considerar que una gran parte de los softwares de administración de redes se realizan sobre el sistema operativo UNIX.
Las principales plataformas de hardware con las que se cuentan en mercado son:
-Equipo SUN.
-Equipo HP.
-Equipo IBM.
-PC's y compatibles.
Las plataformas más comunes de sistemas operativos son:
-Sistema operativo UNIX
-Sistema operativo DOS
Y por último tenemos la plataforma de los softwares propietarios de administración:

1. Para sistema operativo UNIX:
   -SunNet manager para equipo SUN
   -NetView/6000 para equipo IBM
   -OpenView/UNIX para HP.

2. Para sistema operativo DOS:
   -OpenView/dos
   -NMS(NetWare Managment System) para ambiente Novell.

Un programa de administración debe de ir colocado sobre todas las plataformas antes vistas, como se muestra en la figura 6.1, y por lo tanto debe estar basado en éstas, entonces es importante saber el equipo y plataformas que se tienen antes de escoger el programa de administración.

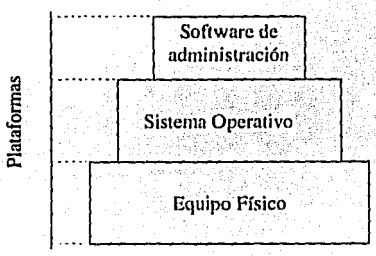


Figura 6.1. Plataformas necesarias para administración.

Los sistemas de administración de redes proveen productos adicionales que permiten soportar alguna otra base distinta. Estos productos pueden incluir paquetes de administración para dispositivos de distintos proveedores basados en SNMP, tales como puentes o ruteadores. Otros paquetes incluyen herramientas como monitor de ayuda y puntos críticos de datos que ayudan a encontrar fallas y errores.

6.3.1. Requerimientos para la implantación de un programa de administración

- **Requerimientos de hardware.**

Estos se refieren al tipo de computadora y capacidad que se requiere para poder instalar el software de administración y que posteriormente tenga la capacidad suficiente para desempeñar todas sus funciones. Normalmente el fabricante del software da una serie de requerimientos mínimos para la instalación de su producto.
Dentro de estas características como ejemplo están :
-Clase o tipo de computadora. Por ejemplo: PC 486 o 100% compatible.
-Capacidad de memoria RAM. Por ejemplo: 8MB mínimo, 16MB recomendados.
-Tipo de monitor. Por ejemplo: VGA o SVGA.
-Dispositivos de ayuda. Por ejemplo: Mouse.

- **Requerimientos de software.**

Este punto se refiere a la plataforma de software que debe de tener instalada la red, para que funcione el programa administrador. Normalmente el fabricante indicará los requerimientos mínimos para su instalación:
-Sistema operativo. Por ejemplo: MS-DOS 5.0 o mas alto y Windows 3.1 o mayor.

-Software propietario de administración. Por ejemplo:H. P. OpenView/DOS

6.4 FUNCIONAMIENTO DE UN SISTEMA ADMINISTRADOR DE RED

6.4.1. El protocolo SNMP

Como se mencionó anteriormente, los administradores de red usan el SNMP para controlar y monitorear redes heterogéneas. Este protocolo esta dentro de la norma TCP/IP por lo que para entenderlo primero se deben ver los orígenes; normatividad y estructura de TCP/IP.
SNMP puede administrar todas las redes heterogéneas o diferentes en un sistema de administración de red.
Algunos de los objetivos de diseño de las especificaciones del SNMP fueron:

a. *Administración integral de la red*: La capacidad para administrar redes incorporando elementos que vienen de una gran variedad de fabricantes con una aplicación sencilla.
b. *Conectividad*: La capacidad para tener un dispositivo de un proveedor administrado desde cualquier otro vendido por un proveedor diferente.
c. *Normas*: Métodos de comunicación comunes y estructura de datos que en redes no similares puedan ser integrados y administrados.

El SNMP fue diseñado para que fuera tan sencillo como fuera posible y está basado en dos elementos:

1. *Estaciones de administración de red*: Son responsables de correr las aplicaciones de administración que controlan y monitorean los elementos de red.
2. *Elementos de red*: Son concentradores inteligentes, ruteadores, puentes y NICs que tienen agentes dentro de ellos. Estos agentes SNMP son responsables del desempeño de las funciones solicitadas por las estaciones administradoras de la red.

El protocolo SNMP es el medio por el cual se comunican la estación administradora y los elementos de la red. Es un simple protocolo que permite a la persona encargada de administrar la red inspeccionar o cambiar variables sobre los elementos de la red, desde una estación de administración remota.
La transmisión del SNMP se realiza confiablemente en el protocolo UDP (Universal Datagram Prptocol) del frame TCP/IP para enviar la información. El protocolo UDP permite a los agentes de administración SNMP ser representados por un solo paquete. De esta manera el SNMP requiere del mínimo de rendimiento y tienen muy poca interferencia con las otras funciones de la red.
Todo el monitoreo SNMP es efectuado por los sistemas de administración de la red, los cuales preguntan a los elementos de red la información requerida o bien los cambios de variables.
En este punto se incorporan tres conceptos de manejo en administración de SNMP:

Gets: Encuestas y cambios
Sets: Las variables que se pueden modificar para producir un cambio en la red
Traps. Cuando una red inicializa comunicaciones (sólo bajo circunstancias inusuales)o existe una condición de alarma por algún mal funcionamiento.

Los elementos de red utilizan un sistema de comunicación llamados agentes Proxy SNMP, estos proveen una comunicación especializada entre las estaciones administradoras y los elementos de red y son usados junto con otros elementos administrados.

Otros protocolos de administración son: SMTP (Simple Mail Transfer Protocol), DNS (Domain Name Service Protocol), FTP (File Transfer Protocol) y el Telnet.

6.4.2. Funcionamiento de una estación administradora de red

Las estaciones de administración SNMP son un conjunto de aplicaciones y base de datos que controlan a un grupo de agentes.

Consta de los siguientes componentes:

. Interface de usuario: Habilita al operador para introducir comandos de administración y recibe mas tarde la respuesta de los agentes, ya sea solicitada o no. Esto se puede realizar en formato de texto o bajo alguna interface gráfica de usuario (GUI o Graphic User Interface).

. Aplicaciones de Administración: Ayudan en el análisis y procesamiento de la información obtenida de los agentes, reduciendo la recolección de datos y extrayendo únicamente la información relevante para ser enviada a la estación de administración.

. La base de datos: Contiene todos los nombres, configuraciones, desempeño, topología y demás datos detectados en la red. Esta base de datos se separa en categorías, entre las que se incluyen:

- Base de datos de la información administrada (MIB).
- Base de datos de los elementos de red.
- Base de datos de las aplicaciones de administración.

La categoría mas importante es la MIB, ya que ésta contiene definición de objetos actuales y que están siendo administrados en ambientes SNMP. Actualmente hay cerca de 1000 dispositivos registrados como miembros de la norma de MIB.

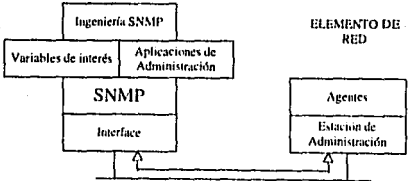


Figura 6.2. Comunicación entre NMS y NMM.

6.4.3 Administración por monitoreo remoto

El protocolo SNMP ofrece gran funcionalidad, sin embargo, su habilidad para monitorear la red es deficiente. Para remediar este problema en 1992 se propuso crear una nueva versión del SNMP. Esta nueva versión llamada SNMPv2 incorpora un monitoreo remoto del MIB (RMON remote monitor) y refuerza los procedimientos de seguridad.

Las especificaciones RMON definen la norma para el funcionamiento del monitoreo de red y las interfaces para comunicarse entre los dispositivos basados en SNMP. El RMON da a las redes la capacidad para proporcionar una eficiente y efectiva vía para monitorear grandes subredes reduciendo así el tráfico y el trabajo sobre otros agentes y estaciones de administración.

Los MIB RMON usan un dispositivo agente, conectado a una red distribuida, para la recolección de estadísticas de tráfico, también se realizan cálculos directamente en el agente y no sobre el administrador, para ciertas funciones. Típicamente, un agente es únicamente responsable de la información administrable que realiza sobre el propio componente.

Para tener efectividad en la administración, una estación de administración RMON debe ser conectada a la LAN. Los agentes RMON están residentes en cada dispositivo que monitorea cada subred. Los monitoreos incluyen operación fuera de línea, detección y reportes de problemas, soporte de múltiples administradores.

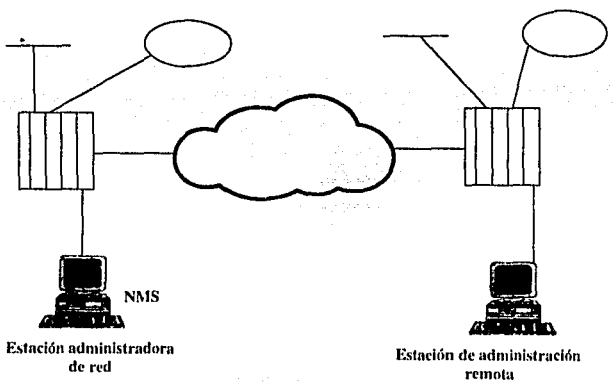


Figura 6.3. Administración remota.

El SNMP y el SNMPv2 no pueden interactuar y no son compatibles, pero en un paquete de aplicaciones SNMP pueden incorporarse ambas arquitecturas o componentes dentro de una aplicación muy grande de administración de red.

6.5. El proceso de inicialización (booting)

Los elementos de red pueden ser configurados y cargados con la información de inicialización utilizando el protocolo BOOTP (Bootstrap Protocol). Este permite que los NMM (Network Management Module) soliciten la información de configuración durante la instalación inicial y las caídas subsecuentes de los NMMs.

El mecanismo para la transferencia del envío de la configuración y el archivo imagen del NMS al NMM es mediante el protocolo TFTP(Trivial File Transfer Protocol).

El archivo de configuración contiene la siguiente información:

- *Llave para los agentes avanzados*: Esta habilita el uso de los agentes avanzados en los módulos de administración NMM y consiste en 8 dígitos que deben concordar con el número dado por el proveedor como licencia de uso.
- *Información de la dirección IP para los ruteadores.*
- *Password común para acceso a las aplicaciones SNMP.*
- *Parámetro para comunicación fuera de banda*: Especifica un teléfono para ser marcado a través de un módem y establecer comunicación por este medio.

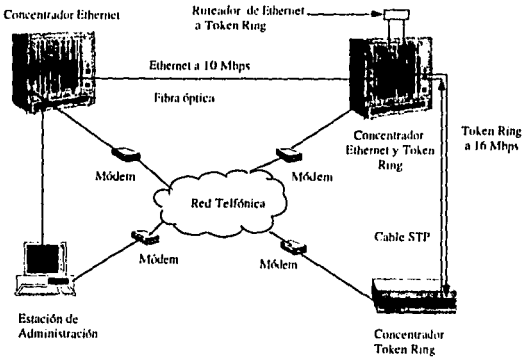


Figura 6.4. Comunicación fuera de banda.

- *Seguridad*: Facilidades como son nodos permitidos y una lista de componentes a los que les será permitido entrar a la red. Éstos están definidos en este parámetro.

El archivo imagen es cargado en los dispositivos NMM desde el NMS y como ya se mencionó utilizando el protocolo TFTP durante el proceso de inicialización (Boot processing).

El archivo imagen es cargado y almacenado en la memoria RAM del NMM y por lo tanto es volátil, es decir, permanecerá mientras no se apague, se reinicie o exista una pérdida en la energía eléctrica. Para volver a recargar la imagen el proceso de inicialización debe ser repetido.

El BOOTP es un proceso que configura y carga los archivos de configuración y de imagen en los NMM, los puentes remotos, los ruteadores, la terminal del servidor y cualquier otro componente que utilice este protocolo para cargar el software. Cuando inicia el modo BOOTP, los NMM envían una trama solicitando información a través de este protocolo.
El servidor BOOTP el servidor TFTP y la NMS con el software de administración pueden ser la misma máquina o puede estar en diferentes computadoras de la red, configuradas para soportar el BOOTP y el TFTP. En algunos casos la configuración del BOOTP y los archivos imagen deben ser instalados en el servidor. Los parámetros para configurar el BOOTP son:

- Dirección IP de los NMM.
- Dirección IP del servidor que contiene el BOOTP
- Dirección inicial de los ruteadores.
- Nombre del archivo de configuración.

Una vez que ésta ha terminado el NMM solicita UDP BOOTP y el servidor BOOTP envía su dirección IP y el nombre de archivo. El NMM pregunta al servidor TFTP por los archivos de configuración y de imagen, regresando este los archivos completando la carga de datos en el NMM.

6.5.1. Inicialización a través de un ruteador

Si el NMM y la NMS están separadas por un ruteador la configuración debe de tener:

- Dirección IP del NMM.
- Nombre del archivo de configuración.
- Localización de la configuración en la NMS.
- Dirección IP del rutedor.

6.6. Software disponible y principales características

Existen en el mercado diferentes marcas, niveles y tipos de programas para administración de redes, los cuales se deben de escoger de acuerdo a una serie de necesidades y requerimientos.
Los hay para funcionar con el sistema operativo DOS y OS/2, son sencillos de instalar, para redes Token Ring y Ethernet.
Otros están basados en plataformas UNIX para IBM, HP y SUN microsystems y son sistemas de administración distribuidos para redes grandes de vendedores múltiples Ethernet, Token Ring y FDDI.
Por último existen programas para implementar control de red distribuido delegando procesos de administración a través de la red.

6.6.1. Software para sistema operativo DOS

En la tabla 6.1 se muestran a manera de ejemplo tres programas distintos y sus características.
Se habla aquí únicamente de algunos productos comunes y sus características aunque en el mercado existe una gran cantidad de éstos
En resumen:

Las aplicaciones SNMP en realidad están basadas en la norma TCP/IP. Este se sitúa en la capa de aplicación del modelo OSI y utiliza UDP como método de transmisión, dándole una comunicación con una metodología de baja utilización del ancho de banda.
Los administradores de red pueden soportar productos de distintos proveedores con interfaces de textos y gráficas, adicionalmente de ofrecer paquetes extra para ayuda en la solución de problemas y mantenimiento de las redes LAN y WAN.

Facilidad	Lattis EZ-View	Optivity para HP Open View/DOS	Optivity para NMS
Administración Ethernet	SI	SI	SI
Administración Token Ring	SI	SI	SI
Administración SNMP a través de ruteadores	SI	SI	SI
Vista expandida del concentrador	SI	SI	SI
Administración a nivel puerto	SI	SI	SI
Estadísticas de la capa MAC	SI	SI	SI
Clave para control de acceso		SI	
SNMP de dispositivos de distintos fabricantes		SI	
Apilamiento doble IP/IPX	SI		SI
Descubrimiento de Internet			SI
Descubrimiento automático de IPX			SI
Administración Telnet		SI	
Registro de datos relativos al funcionamiento de la red		SI	

Tabla 6.1. Comparativo de softwares comerciales.

CONCLUSIONES

CONCLUSIONES

El mundo de las redes hoy en día es tan amplio que es difícil evaluar cual es o será la mejor opción, intervienen tantos factores y existen tantos productos y tecnologías que un diseñador de redes se puede ver envuelto en un laberinto de soluciones.
El presente trabajo fue desarrollado buscando auxiliar a las gentes que se quieran dedicar al desarrollo de soluciones LAN-WAN, así como para las gentes que requieran conocer que parámetros tienen que evaluar antes de resolver sus necesidades de conectividad.
A continuación presentamos las conclusiones obtenidas del material desarrollado:

GENERALES

- Debido a los cambios tan rápidos en la tecnología no se ha podido establecer una norma a nivel mundial. En definitiva la tendencia parece firme en ir hacia ATM, pero la pregunta será ¿Con cual de sus variantes?, eso nadie lo puede contestar por ahora. Lo mejor entonces será buscar a aquellos fabricantes que están tratando de regir la norma y en su caso ver la posibilidad de acuerdos sobre actualizaciones futuras de tecnología, una vez que se conozca la norma.
- Servicio y Soporte son los puntos que más deberán cuidar los proveedores de equipo de redes, ya que cada vez se vuelve mas sutil la línea que les divide con la competencia.
- Será necesario que las empresas inviertan más en la capacitación de su personal de sistemas y de comunicaciones, ya que el éxito o fracaso de una red LAN-WAN depende en gran medida de los responsables de la administración de la red, así como de las herramientas que tenga para dicha función.
- El mercado para los productos de red es aún tremendamente atractivo, si consideramos que únicamente el 18% de las PC's que existen en nuestro país están conectadas en red, veremos que la potencialidad es enorme.
  Incluso la compañía 3COM asegura que las inversiones en este campo en los próximos 3 años serán considerables, ellos pronostican que en 1996 la base instalada de equipos llegará a los 65 millones de nodos.
- Por otro lado TELMEX planea tener el 70% de su red digitalizada para 1995, lo que abre una gama muy interesante de posibilidades de conexión para redes LAN, MAN y WAN.

TECNOLOGÍA

- FDDI tiene grandes posibilidades de desaparecer del mercado, esto debido a que la tecnología de Conmutación y Fast Ethernet es mucho más económica. Por otro lado con el surgimiento de ATM se ven limitadas las aplicaciones de FDDI en el futuro inmediato.
- La tendencia de la tecnología se esta orientando fuertemente hacia el manejo de la conmutación de información; luego entonces esta tecnología en ambientes de LAN esta siendo muy demandada. Por otro lado en el ambiente LAN-WAN, la tecnología ATM estará ganando terreno rápidamente en los próximos años y como consecuencia en un tiempo medio los ruteadores tendrán que ceder su lugar en las redes actuales para dar paso a los dispositivos de conmutación.

- El cableado estructurado tiende a convertirse en una norma de trabajo para las empresas que planean permanecer fuertemente comunicadas.
  Según estadísticas de los fabricantes de equipo de redes, se estima que entre el 70 y 80% de las fallas de una red son provocadas por el cableado, entonces es fácil entender la necesidad que tendrán las empresas de invertir en esta tecnología.
- Los materiales que están marcando la pauta para lo referente al cableado son: El UTP nivel cinco y la fibra óptica, esta última ha ido reduciendo su precio de mercado y no sería extraño que en breve sea casi tan barata como el cable de cobre.
- La tendencia y demanda del mercado es hacia conectividad universal, pudiéndose manejar simultáneamente y por el mismo medio voz, datos e imagen. Esta es una de las fuertes razones por las que ATM puede ganar adeptos rápidamente.
- A pesar de la tendencia hacia ATM, en nuestro país los proveedores de servicios públicos de transmisión de datos no están planeando invertir en este tipo de tecnología hasta que se halla definido la norma internacional. Por desgracia esto podría llevar algunos años y entonces será difícil que ATM se implante en México en el corto plazo.
- Una opción al problema del punto anterior podría ser la entrada en 1996 de las compañías extranjeras, para proveer en sociedad con empresas nacionales, los servicios de portadoras públicas de datos así como los servicios de larga distancia.

DISEÑO

- Consideramos que como primer punto la gente de diseño debe conocer claramente el funcionamiento de los dispositivos y normas relacionados con las Redes LAN y WAN, para así tener las herramientas para encontrar la mejor solución.
- Quienes se diquen tanto al diseño como a la asesoría de redes tienen un gran campo de acción en el corto y largo plazo en nuestro país.
- La demanda de aplicaciones que existen hoy en día hace que el diseño de las redes deba ser sumamente versátil en cuanto a crecimiento y servicios se refiere.
- Los anchos de banda que están demandando las aplicaciones actuales han forzado a los fabricantes de equipo a implementar nueva tecnología para obtener mejores rendimientos con las muy populares Ethernet y Token Ring, logrando continuar su uso en el mediano plazo y posiblemente hasta unos 10 años más.
- No existe ninguna fórmula para hacer un diseño confiable de red, entonces la experiencia y una buena visión global son características vitales para el diseñador de redes.
- Los factores clave a cumplir en los diseños serán:
  En desempeño: Baja latencia.
  Conectividad directa para usuarios.
  Capacidad de manejo de un ancho de banda amplio.
  En flexibilidad: Posibilidad de expansión.
  Aplicaciones que permitan mantener el desempeño.
  Costo bajo: Tanto en instalación como en administración de la red.
- Uno de los aspectos más peligrosos para el diseñador es dejarse llevar por condiciones de mercado de precios. Será de suma importancia plantear las limitaciones que se pueden tener con la adquisición de una red sin el desempeño adecuado debido a falta de recursos.

Los diseños deberán mantener en la medida de lo posible la homogeneidad en lo referente a equipos de comunicación, ya que esto aumenta la confiabilidad de servicio y así reduce la posibilidad de fallas debidas a incompatibilidad.

- La administración de redes es un requerimiento para cualquiera que quiera controlar y monitorear sus LANs y WANs. Existe una gran variedad de productos nuevos diseñados para trabajar como sistemas de red integrados y bien organizados, sin embargo podría rápidamente existir una desorganización masiva de dispositivos operando independientemente, por lo que se deben implementar aplicaciones de administración de red, basados en el protocolo SNMP, para solucionar este problema.

GLOSARIO

Glosario de Términos y Siglas

Términos o Siglas	Significado de las Siglas en Inglés	Significado en Español
ANSI	American National Standards Institute	Instituto Nacional Americano de Normalización
ASCII	American Standard Code For Information Interchange	Código Estándar Americano para Intercambio de Información
ATM	Asinchronous Transfer Mode	Modo de Transferencia Asíncrona
B-ICI	Broadband Interexchange Carrier Interface	Interface Transportadora de Intercambio de Banda Ancha
Backbone		Troncal Principal
BGP	Border Gateway Protocol	Protocolo de Compuerta Gateway
BISDN	Broadband Integrated Services for Digital Networks	Red Digital de Servicios Integrados de Banda Ancha
Bridge		Puente
BSI	British Standards Institute	Instituto de Estándares Británicos
CAD	Computer Application Design	Diseño de Aplicaciones por Computadora
CCITT	Consultive Comitee for International Telegraphy and Telephony	Comité Consultivo Internacional Telegráfico y Telefónico
CIR	Commited Information Rate	Relación de Datos Dedicados
CSMA/CD	Carrier Sense Multiple Access/Collision Detection	Acceso Múltiple por Detección de Portadora
DAC	Dual Attached Concentrator	Concentrador con Doble Conexión, una por anillo.
DAS	Dual Attached Station	Estación con Doble Conexión, una por anillo
DCE	Data Comunication Equipment	Equipo de Comunicación de Datos
DLCI	Data Link Conection Identifier	Identificador de Conexión de Enlace de Datos
DLSw	Data Link Switching	Conmutación de Enlace de Datos
DNIC	Data Network Identification Code	Código de Identificación de Red de Datos
DSU	Data Service Unit	Unidad de Servicio Digital
DTE	Data Terminal Equipment	Equipo Terminal de Datos
DUAL HOMING		Método de conexión de dispositivos con redundancia
E1		Enlace Digital Norma CCITTG703

Términos o Siglas	Significado de las Siglas en Inglés	Significado en Español
EGP	Exterior Gateway Protocol	Protocolo de Compuerta Exterior llamada Gateway
EIA	Electronic Industries Association	Asociación de Industrias Electrónicas
Ethernet		Medio de acceso de red basado en la norma IEEE802.3
ETR	Early Token Release	Liberación Temprana del Testigo.
FDDI	Fiber Distribution Data Interface	Interface de Datos por Distribución de Fibra óptica, medio de acceso de red establecido por la ANSI
FEP	Front End Procesor	Procesador de Primera Línea
Flooding		Método de envío de información simultánea
FOIRL	Fiber Optic Inter Repeater Link	Repetidor de enlace a través de fibra óptica
FRAME RELAY		Protocolo de Conmutación de Tramas
FRAME SWITCH		Conmutador de Tramas
Gateway		Compuerta de enlace
Gbps		Gigabits por segundo
HDLC	High Data Link Control	Control de Alto Nivel de Enlace de Datos
HUB		Concentrador
IDN	International Data Number	Número de Datos Internacional
IEEE	Institute of Electric and Electronic Engineers	Instituto de Ingenieros Eléctricos y Electrónicos
IP	Internet Protocol	Protocolo de interconexión de redes
IPX		Protocolo para redes Novell
IS-IS	Intermediate System to Intermediate System	Sistema Intermedio a Sistema Intermedio
ISO	International Standards Organization	Organización Internacional de Normalización
ITU	International Telecomuncation Union	Unión Internacional de Telecomunicaciones.
Kbps		Kilobits por segundo
LAN	Local Area Network	Red de Área Local
LAP	Link Access Procedure	Procedimiento de Acceso al Enlace
LAPB	Link Access Procedure, Balanced	Procedimiento Balanceado de Acceso a Enlace
LAPD	Link Access Procedure, Direct	Procedimiento Directo de Acceso a Enlace

Términos o Siglas	Significado de las Siglas en Inglés	Significado en Español
Lobe		Tramo de cable que interconecta un dispositivo de red Token Ring a una unidad de acceso
LLC	Logic Link Control	Control de Enlace Lógico
MAC	Media Access Control	Control de Acceso al Medio
Mainframe		Computadora Central
MAN	Metropolitan Area Network	Red de Área Metropolitana
MAU	Multiaceses Attachment Unit	Unidad de Acceso Multiestación
Mbps		Mega bits por segundo
MIB	Managment Information Base	Base de datos de Información para la Administración
MMF	Mult Mode Fiber	Fibra multimodo
MTBF	Medium Time Between Failures	Tiempo Medio Entre Fallas
MTTR	Maximum Time to Repair	Tiempo Máximo Para Reparación de Fallas
Multimedia		Manejo de información en voz video video y datos
MW	MicroWave	Microonda
NAUN	Nearest Available Upstream Neighbor	Notificación de Vecino Activo Anterior más Próximo o Cercano
NIC	Network Interface Card	Tarjeta de Interface Controladora de Red, también conocida como adapatador.
NLPID	Network Link Protocol Identifier	Identificador de Protocolo a Nivel de Red
NMM	Network Management Module	Módulo de Administración de Red
NMS	Network Management System	Sistema de Administración de Red
NMS	Network Management Station	Estación de Administración de Red
NNI	Network Node Interface	Interface nodo de red
NNP	Neighbor Notification Process	Proceso de notificación de vecino
NOM		Norma Oficial Mexicana
OSI	Open System Interconnection	Interconexión de Sistema Abierto
PBX		Central Telefónica Pública
PCMCIA	Personal Computer Memory Card International Association	Asociación Internacional de Tarjetas de Memoria de Computadoras Personales

Términos o Siglas	Significado de las Siglas en Inglés	Significado en Español
PDU	Protocol Data Unit	Unidad De Datos de Protocolo
PHY	Physical	Capa de protocolo físico
PLP	Package Link Protocol	Protocolo de Enlace de Paquetes
PMD	Physical Media Dependent	Capa Física Dependiente del Medio
PPP	Point to Point Protocol	Protocolo Punto a Punto
PVC	Permanent Virtual Circuit	Circuito Virtual Permanente
RDI		Red Digital Integrada
RFC	Request For Coment	Solicitud de Comentario
RIP	Routing Information Protocol	Protocolo de Entubamiento de Información
RMON	Remote Monitor	Monitor Remoto
SAC	Single Attached Concentrator	Concentrador de Conexión Sencilla
SAP	Service Accsess Point	Punto de Acceseso al Servicio
SAS	Single Attached Station	Estación de una Sola Conexión
SDLC	Synchronous Data Link Control	Control de Enlace de Datos Síncrono
SMDS	Switched Multi-Megabit Data Services	Servicio de Conmutación de Datos De Múltiples megabits
SMF	Single Mode Fiber	Fibra Monomodo
SMT	Station Management	Administración de Estación
SNA	Systems Network Architecture	Arquitectura de Redes de Sistemas
SNMP	Simple Network Management Protocol	Protocolo de Administración de Red Sencilla
Spanning Tree		Árbol Expandido
STP	Shielded Twisted Pair	Par Trenzado Blindado
Switch		Conmutador
TCP	Transmission Control Protocol	Protocolo de Control de Transmisión
TCP/IP	Transmission Control Protocol/ Internet Protocol	Protocolo de Control de Transmisión/Protocolo de Interconexión de Redes
Token		Testigo
Token Ring		Método de Acceso de Red basado en la norma IEEE802.5
TP	Twisted Pair	Par Trenzado
UNI	User Network Interface	Interface Usuario Red
UTP	Unshielded Twisted Pair	Par Trenzado sin Blindaje
WAN	Wide Area Network	Red de Área Amplia

Términos o Siglas	Significado de las Siglas en Inglés	Significado en Español
X.21		Protocolo de Capa Física que define las interfaces físicas y eléctricas entre la red y las estaciones
X.25		Conjunto de normas y regulaciones que definen una red de área amplia utilizando conmutación de paquetes
XNS	Xerox Network Services	Servicios de Red Xerox

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Libros Consultados:

Andrew s Tanenbaum
Redes de ordenadores
Prentice-hall hispano americana
Primera edición, México 1991

Justo Carracedo Gallardo
"Redes Locales en la Industria "
Serie Productica, Editorial Marcombo
España, 1988

Roger L. Freeman
Telecommunication System Engineering
Wiley-Interscience Publication, John Wiley & Sons
Segunda Edición U.S.A., 1989

Uylles Black
"Redes de Computadoras Protocolos, Normas e Interfaces"
Prentice Hall, Inc. 1987

Revistas consultadas:

Bor Ryan
"El intermanejo de las redes un panorama a largo plazo"
Revista Byte, México, Septiembre de 1994

Francisco Villarreal
"Redes de área local de alta velocidad: ¿Salto cuantitativo o cualitativo al futuro?" Parte II
Revista red, México Abril de 1994

Ing. José I. Chavez Páez
"Atm, la llave de la comunicación digital"
Revista red, México Marzo de 1994

Jon Bryan
"Conmutación de las redes"
Revista Byte, México, Septiembre de 1994

Lic. Laura Mayo Guzmán
"Topologías de red, tendencias en la selección de redes"
Revista red, México, Mayo de 1994

Marcelino Gómez
"El ruteador en extinción"
Revista red, México, Noviembre de 1994

Información Técnica:

A guide to SNMP Network Management
Anixter, Technology ,U.S.A. 1994

IBM 8250 Ethernet Products

IBM Networking Systems 1993
Integrating SNA and Multiprotocol LAN Networks
Wellfleet Communications, Inc., U.S.A. Junio 1993
LAN/ATM
SynOptics Communications, Inc U.S.A. 1994
PC LAN Networking
Wellfleet Communications, Inc., U.S.A. 1993
Preparación de la red para soportar los requisitos de negocios emergentes
SynOptics Communications, Inc U.S.A. Febrero 1994
Seminario de Tecnología de Puentes/Enrutadores
Kb/Tel México D.F. Febrero de 1992
Simplifiying LAN-WAN Integration
Wellfleet Communications, Inc., U.S.A. 1993
SynOptics Pocket Guide
SynOptics Communications, Inc U.S.A. Febrero 1994
Technical reference pocket guide Q3,1994
SynOptics, U.S.A. Julio 1994
Token Ring Connectivity Certification
SynOptics Communications, Inc U.S.A. 1994

Folletería de características técnicas de productos:

Wellfleet Communications, Inc
SynOptics
I.B.M.
Newbridge
Cysco
Anyxter