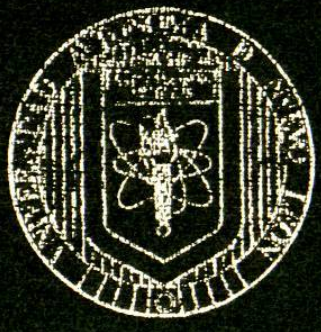
UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POST-GRADO



"REDES LOCALES Y CONECTIVIDAD"

POR

ING. CIRO CALDERON CARDENAS

T E S I S

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERIA ELECTRICA CON ESPECIALIDAD EN ELECTRONICA

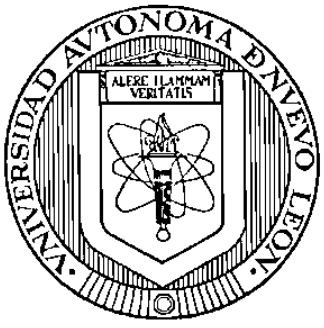
SAN NICOLAS DE LOS GARZA, N. L., JUNIO DE 1998

1998 "REDES LOCALES Y CONECTIVIDAD"

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

DIVISIÓN DE ESTUDIOS DE POST-GRADO



"REDES LOCALES Y CONECTIVIDAD"

POR

ING. CIRO CALDERÓN CÁRDENAS

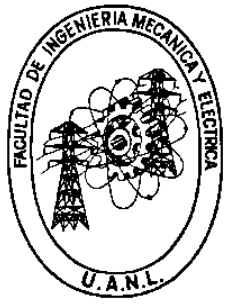
TESIS
EN OPCIÓN AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERÍA ELÉCTRICA CON ESPECIALIDAD EN ELECTRÓNICA

SAN NICOLAS DE LOS GARZA, N.L., JUNIO DE 1998

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

DIVISIÓN DE ESTUDIOS DE POST-GRADO



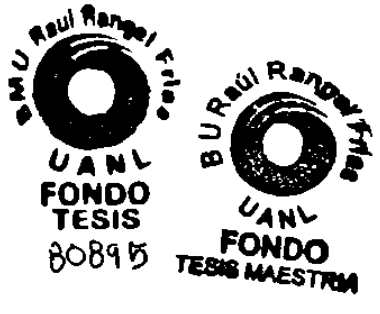
"REDES LOCALES Y CONECTIVIDAD"

POR

ING. CIRO CALDERÓN CÁRDENAS

TESIS
EN OPCIÓN AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERÍA ELÉCTRICA CON ESPECIALIDAD EN ELECTRÓNICA

SAN NICOLAS DE LOS GARZA, N.L., JUNIO DE 1998



UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA
DIVISIÓN DE ESTUDIOS DE POST-GRADO

Los miembros del comité de *tesis recomendamos que* la *tesis* **"REDES LOCALES Y CONECTIVIDAD"** realizada por el **Ing. Ciro Calderón Cárdenas**, sea aceptada para su defensa como opción al grado de **Maestro en Ciencias de la Ingeniería Eléctrica con la especialidad en Electrónica.**

El Comité de Tesis

M.C. JUAN SARABIA RAMOS
Asesor

M.C. FERNANDO ESTRADA SALAZAR
Coasesor

M.C. JOSÉ D. RIVERA MARTÍNEZ
Coasesor

M.C. ROBERTO VILLARREAL GARZA
Vo.Bo.
División de Estudios de Post-grado

San Nicolás de los Garza, N. L., Junio de 1998.

PRÓLOGO

Los sistemas de redes de computadoras tienen alrededor de 30 años y eran una curiosidad de laboratorio en aquel tiempo, hoy son herramientas utilizadas por millones de personas todos los días.

Antes de los años 80s las computadoras eran muy caras, por lo que solo unos cuantos las usaban. En 1980 con la PC se popularizó el uso, la computadora personal actualmente opera en el ambiente de Windows 95 y normalmente es utilizada por una sola persona. Cuando se conectan varias computadoras personales para formar una red de computadoras, cuyo propósito es el de compartir recursos para ahorrar dinero, trabajo, recursos tales como una impresora y archivos desde las estaciones de trabajo (computadoras personales) y estas estaciones son utilizadas por diferentes personas en horarios diferentes como en las oficinas, escuelas, empresas etc. El administrador de la red cuya función es la de mantener al servidor y a las estaciones de trabajo funcionando tiene un gran compromiso el cual no es fácil.

Lo que nos ocupa en el desarrollo de esta tesis es la formación de recursos humanos para que cuenten con conocimientos de redes de computadoras y desarrollen la habilidad para administrar dichas redes.

SÍNTESIS

Estamos viviendo en una sociedad de información. Donde ahora más que nunca, transmitir enormes cantidades de información rápidamente a través de grandes distancias es una de nuestras necesidades más urgentes. Desde esfuerzos pequeños de una persona al más grande de las corporaciones, los profesionales descubren que la única manera de tener éxito actualmente y más allá esta en comprender que la tecnología avanza rompiendo el ritmo y debemos seguir adelante. Los usuarios de todos los rincones del mundo encuentran la ventaja de conectarse al ambiente de red de computadoras. De inmediato tienen acceso a documentos y reportes que ofrecen a ellos la capacidad de incorporar un conocimiento antes inconcebible. Los usuarios en grupos de trabajo ahora pueden sostener conferencias interactivas, por ejemplo un usuario de red puede participar en una conferencia con otros, aun sin estar en la misma ciudad, y las posibilidades son interminables.

Un usuario tiene la facilidad de conversar en "tiempo real" con una persona que esta en Japón con el costo de una llamada local, o enviar un documento vía correo electrónico a un grupo de personas a diferentes partes en el mundo, las cuales critican el documento y le regresan los comentarios al autor. Este tipo de actividades es únicamente posible en redes de computadoras sin necesidad de viajar.

Incluso usuarios expertos se sorprenden cuando descubren un nuevo servicio o característica que anteriormente no existía. Una vez familiarizado con la terminología y cometiendo errores ocasionales, el proceso de aprendizaje se llevará de forma acelerada.

Las computadoras son una herramienta que nos ayuda en el trabajo de oficina, diseño y muchas otras áreas, cuando se adquiere una nueva computadora, normalmente tiene únicamente instalado el sistema operativo y el usuario de esa computadora

determina que programa de aplicación a utilizar. La nueva computadora funciona apropiadamente incluyendo la impresora conectada a esta. Si el usuario le instala nuevos programas (software) en algunas ocasiones la computadora deja de funcionar, y el usuario busca apoyo para solucionar dicho problema. Para solucionar el problema se debe tener el conocimiento del como funciona la computadora y tener la experiencia en la instalación de software. Hoy en día los usuarios normalmente conocen muy bien el programa de aplicación pero no son expertos en instalación de software por lo que ocurren estas situaciones.

Cuando las computadoras están en red los problemas son más, porque el usuario no tiene los conocimientos del funcionamiento de la red, entonces el apoyo solicitado requiere de una persona que tenga la experiencia en el funcionamiento, instalación y administración de redes.

Cuando se instala un nuevo programa, este puede instalarse para que se ejecute desde el servidor o desde la propia estación de trabajo. Sé tendrá que evaluar cual es la mejor opción de acuerdo a las limitaciones de espacio en disco duro en la estación, y a la velocidad deseada para correr el programa.

En el desarrollo de esta tesis comenzaremos con el propósito de redes locales y la descripción de diferentes tipos de redes así como sus sistemas operativos de red. El 80 % de las redes de computadoras en el mundo usan el protocolo Ethernet de 10 Mbps. Los sistemas operativos mas usados son Netware, UNIX, Windows 95, y Windows NT.

También se describen los protocolos mas usados y la función de los dispositivos de conectividad que forman una red local como el repetidor, el puentes, switch, y el encaminador que forma parte de los dispositivos de redes de cobertura amplia.

Cuando se presentan problemas en la red se debe analizar el porque ocurren para poder resolverlos.

Cuando las aplicaciones se corren desde el servidor y están muy lentas conviene segmentar las redes.

Una de las aplicaciones que causa problemas en la red son los videos y multimedia como con las enciclopedias que contienen un sinnúmero de animaciones y programas de realidad virtual, y existen protocolos que los soportan los cuales están empezando a ser económicamente viables.

Contenido

Capitulo 1

Introducción

1.1 Introducción

El ambiente global de las organizaciones de hoy, está orientado hacia la integración de sus Sistemas de Información, cada vez surgen nuevos productos, estándares y tecnologías, las aplicaciones de Software más modernas, las arquitecturas Cliente/Servidor más funcionales, las Bases de Datos Relacionales más potentes, y todo el Campo de la Informática, están basadas en ambientes de Comunicación de Datos.

Los distintos Sectores Industriales, los grandes Corporativos y miles de Empresas de diferentes giros, dependen ó dependerán en un futuro muy cercano, de la confiabilidad de su infraestructura de Conectividad.

La tendencia del mercado gira alrededor de necesidades como:

- La Transmisión de la Información (Datos, Voz, Vídeo) en forma segura y confiable, con la facilidad de efectuar operaciones en línea.
- La Administración y Control de cada Grupo de Trabajo y de toda la Red, en forma simple, centralizada, fluida e inteligente.
- La Conectividad hacia todas las Oficinas ó Edificios Remotos.
- La facilidad de crecimiento y migración de sus Sistemas.
- El añadir nuevas tecnologías, como quieran y cuando quieran.

La Conectividad está avanzando muy rápidamente, y el mercado actual demanda Ingenieros capacitados que puedan diseñar e instalar Infraestructuras de Información, óptimas de Sistemas de Cómputo y Dispositivos de Comunicación.

Este trabajo, es presentado en forma de Manual para facilitar su consulta. Espero pueda ayudar a los alumnos de las materias de "Electrónica para Comunicaciones" y "Sistemas de Transmisión de Datos".

1.2 Objetivo

Este trabajo ha sido desarrollado para que sea de utilidad a los estudiantes del Area de Comunicación de Datos.

El objetivo principal, es el de animar a todos los estudiantes con una fuerte inclinación hacia el Area de Comunicaciones, para que se mantengan al día con los adelantos tecnológicos que existen actualmente en este campo.

1.3 Justificación

En F.I.M.E., en el programa de la carrera de Ingeniero en Electrónica y Comunicaciones, se requiere de una estandarización de los temas del área académica que trata con la transmisión de datos.

1.4 Metodología

Este manual inicia con la descripción del funcionamiento de las redes de computadoras, que existen actualmente en el mercado, los conceptos básicos, el Modelo de Referencia OSI, y la conectividad.

Enseguida se analizan las tres tecnologías de LANs mas usadas, Ethernet, Token Ring y FDDI, describiendo su operación, topología, componentes y sus características más importantes.

Después se analizan los dispositivos actuales de conectividad, como los repetidores, concentrador ó hub, bridge, router y switch, analizando las tecnologías con que opera cada uno de ellos, sus características, funcionalidades, ventajas y desventajas.

Capitulo 2

Conceptos de Redes Locales

2.1.Conceptos Básicos.

El objetivo de las redes de Área Local (Local Area Network - LAN), es el permitir que los usuarios compartan recursos, periféricos, archivos, aplicaciones etc. Esto cambió el concepto de la Computadora Personal (PC), de ser una herramienta personal y aislada a una con acceso a una amplía variedad de recursos.
A partir de las primeras redes, la industria de la computación ha desarrollado diferentes estándares y protocolos de comunicación de datos, y también sistemas operativos de red.

Componentes Básicos

Los componentes activos básicos que definen una red de área local podrían definirse de una forma simple como el servidor de recursos, la estación de trabajo y el sistema operativo de red. Pasaremos a continuación a dar una descripción breve de las funciones de cada uno de estos componentes dentro del sistema.

Servidores y Estaciones de Trabajo

Un servidor es cualquier computadora de la red que ofrece sus recursos para que éstos sean compartidos por otras computadoras o usuarios de la red. Teóricamente el número de servidores que puede llegar a tener una red es infinito. Dado que el servidor tiene que atender las diversas peticiones de los usuarios conectados a sus recursos, deberá poseer una elevada velocidad de proceso, es decir, un CPU de alto nivel, un disco duro de gran capacidad y bajo tiempo de lectura/escritura y una gran cantidad de memoria RAM disponible.

Una estación de trabajo no ofrece sus recursos para que sean utilizados por el resto de la red, su función es beneficiarse de los recursos que ponen a su disposición los servidores. Una computadora de la red se define o configura como servidor (server) o estación de trabajo (workstation) mediante el sistema operativo de red.

Un tipo especial de servidores son los servidores de software. Lo que hace que una computadora funcione como servidor de software es su instalación en el sistema operativo de red como tal.

La función del servidor de software en conjunción con el sistema operativo de red es asegurarse de que los usuarios tengan acceso simultáneo al software compartan el recurso.

Los servidores de software proporcionan varios niveles de seguridad y control de acceso, permitiendo al administrador de la red establecer qué usuarios tienen acceso a qué recursos, por cuanto tiempo, el tipo de acceso (sólo lectura, lectura /escritura...). Por último, cabría señalar que existen distintas clases de servidores:

Servidores no-dedicados.

Trabajan para el usuario como estaciones de trabajo o como servidores de software. El rendimiento y la integridad del sistema pueden ser un riesgo a la hora de decidirse por esta solución ya que las aplicaciones y los usuarios que estén trabajando en el servidor se pueden bloquear por completo, aunque una ventaja es el ahorro de una estación de trabajo.

Servidores dedicados.

Funcionan estrictamente como servidores, no estando disponibles como estaciones de trabajo. Proporcionan mucho mejor rendimiento y seguridad e integridad del sistema que los anteriores.

Servidores de impresión.

Los sistemas operativos de red que permiten configurar una computadora como servidor de impresión.

Servidores de módem.

Estos proporcionan a todas las estaciones de la red acceso a un módem en el servidor, que puede ser una computadora con tarjeta de módem.

El Sistema Operativo de Red

Conectar todos los dispositivos de la red entre sí no significa que vayan a trabajar inmediatamente en red el uno con el otro. Para ello será necesario un programa o sistema operativo de red para una comunicación eficiente y eficaz entre los diversos dispositivos y sistemas. Una de las tareas fundamentales en un sistema operativo de red es proporcionar esta comunicación, para ello deben manejar muchos recursos y enfrentarse a situaciones muy complejas. Lo que el sistema operativo de mi computadora personal realiza normalmente para nuestra máquina, el sistema operativo de red debe realizarlo por todas las computadoras y recursos que estén conectados a él.

En las redes locales basadas en el sistema operativo MS-DOS, el sistema operativo de red funciona conjuntamente con el sistema operativo de la computadora. Cuando los comandos son locales, son procesados por el sistema operativo de la computadora. Cuando hay una petición de periférico local por parte de un usuario remoto, es decir, de red, se pasa al sistema operativo de red, para que la procese.

El sistema operativo de red debe llevar un control total de todos los accesos a los datos, estén donde estén, asignar espacio en disco, controlar los permisos de los usuarios, requerir el password del usuario, controlar la seguridad de la red.

Sistemas Operativos de Red (Network Operating System - NOS)

Las Redes no son más que herramientas para compartir recursos, para proveer "Conectividad", éstas deben soportar varios tipos de Software de Control y de Comunicación. El Sistema Operativo de Red (Network Operating System - NOS), es el componente principal y básico de la arquitectura de redes. Los sistemas operativos Soportan tanto la arquitectura igual a igual (peer to peer), y como la arquitectura Cliente / Servidor.

En una LAN con arquitectura "igual a igual", cualquier PC o estación de trabajo puede funcionar como un Servidor de archivos o de impresión.

Las Redes Cliente/Servidor permiten un alto desempeño de una PC o estación de trabajo como servidor de archivos o de impresión. Las estaciones pueden tener acceso información de este servidor. La velocidad y eficiencia de un servidor determina directamente el desempeño de la red. Muchos sistemas operativos de Redes controlan y coordinan actividades entre el o los servidores y los protocolos de transporte de red.
La siguiente sección describe los sistemas operativos de red más ampliamente usados.

Sistema Operativo Windows NT

Actualmente Windows NT de Microsoft es el sistema operativo de red más instalado, por su ambiente gráfico..

Windows NT es una de las herramientas más poderosas, disponible para aplicaciones cliente/servidor, tanto en computadoras personales como en servidores.

El papel de Windows NT

Windows NT no reemplaza al MS-DOS, al Windows 3.1 o al Windows para grupos de trabajo. Windows NT complementa y extiende la familia Windows brindando una sólida plataforma para requerimientos de aplicaciones más sofisticadas.

Windows NT ejecuta aplicaciones críticas para negocios como lo son la ingeniería de diseño, contabilidad, ordenación de datos y administración de inventarios, ligándolas con información almacenada en Mainframes, Minicomputadoras y Redes.

Los usuarios pueden accesar los recursos de la empresa utilizando la familia interfaz de Windows.

Es también una excelente solución para usuarios de computadoras personales que requieren aplicaciones sofisticadas, como lo son los desarrolladores de software y otros usuarios poderosos.

Windows NT refuerza al poder total de las plataformas sólidas basadas en arquitectura de uniprocesador, incluyendo los procesadores de Intel 80486 y Pentium, procesadores RISC de DEC y MIPS y más de 20 sistemas de multiprocesadores.

Integrando Windows NT a ambientes ya existentes

Windows NT puede ser utilizado para integrar recursos de red que compartan una variedad de plataformas dentro de una organización, incluyendo Windows 3.1, Windows para grupos de trabajo 3.1, MS-DOS, Macintosh, UNIX, OS/2 y todas las redes más conocidas, incluyendo Novell NetWare, Microsoft LAN Manager, IBM LAN Server, DEC Pathworks y Banyan VINES.

Sistema Operativo NetWare

Anteriormente el sistema operativo NetWare de Novell era el más instalado de los sistemas operativos de red. Este soporta DOS, Windows, Macintosh, OS/2 y el sistema operativo host de UNIX. La versión más actual, es la más recomendada NetWare también provee soporte para comunicación asíncrona para área amplia, permitiendo a los usuarios crear sistemas de conectividad de organización amplia. La suite de protocolos de Novell incluye Intercambio de Paquetes de Internet (Internet Packet Exchange - IPX), un datagrama de protocolo que provee conexión a estaciones de trabajo NetWare y Servidores de archivos con direccionamiento y servicios de conectividad. Intercambio de Paquetes Secuenciados (Sequenced Packet Exchange - SPX) que es un protocolo orientado a conexiones, algunas de sus funciones incluyen:

Dar conexión y control de flujo
Eliminar el envío de paquetes duplicados
Crear de un número de secuencia y número de reconocimiento para mantener confiable la transferencia de datos.

El shell de NetWare es un protocolo de servicios que controla la interacción entre las estaciones de trabajo y la red. Por ejemplo, si una estación de trabajo requiere un archivo en el disco duro local, el shell pasa la requisición al sistema operativo Host, si la estación de trabajo requiere un recurso de la red, el shell manda el requerimiento al servidor de archivos.

Sistema Operativo LAN Manager

El Sistema Operativo de Red LAN Manager de Microsoft Corporation, es fundamentalmente un sistema operativo Cliente / Servidor. Un sistema Cliente / Servidor permite Servidores poderosos para desempeñar servicios de requerimientos de archivos del cliente (como acceso a Bases de Datos) y mandar de regreso el resultado a la estación de trabajo Cliente. Esto evita tener que transmitir las Bases de Datos enteras sobre la red.

El sistema operativo LAN Manager hace uso de un Lenguaje de Consulta Estructurado (Structured Query Language - SQL) en el servidor, para tomar ventaja de las aplicaciones de Base de datos SQL Cliente / Servidor.

La falta de funciones como: multitarea, Compartición de Archivos, Memoria Virtual y otras limitaciones hacen al DOS un sistema operativo Host ineficiente para trabajar en un ambiente de red; por esta razón, LAN Manager fue desarrollado para trabajar con el sistema operativo OS/2. El sistema OS/2 debe ser instalado en el servidor LAN Manager antes de instalar programas para LAN Manager. Las características de conectividad permiten que las estaciones de trabajo acceso a servidores NetWare, y Macintosh, TCP / IP, UNIX, y a Host IBM SNA. El sistema operativo de red LAN Manager ofrece un robusto soporte multi-protocolo

Protocolo TCP/IP

Además de los sistemas operativos, existen otros métodos para administrar y controlar la red estos métodos son llamados protocolos, los cuales son responsables del ruteo de datos de estación a estación, facilitando recuperación de errores, y administrando el control de flujo del tráfico. El Protocolo de Control de Transporte / Protocolo Internet (Transport Control Protocol / Internet Protocol - TCP / IP) es el Suite de Protocolos abierto más ampliamente utilizado en el mundo. Cuando se interconectan Redes que utilizan diferentes Sistemas Operativos de Red y otros protocolos, TCP / IP es una de las mejores opciones disponibles, fue diseñado para esta tarea para el Departamento de Defensa de E.E.U.U. Cuando se escoge un sistema operativo de red, se debe estudiar qué protocolos soporta.

2.2. Protocolos y Estándares.

Los Protocolos son conjuntos de reglas que especifican precisamente cómo actúan las diferentes partes de la red para permitir que los dispositivos se comuniquen con los demás. Ellos describen la información de ruteo, el cómo las direcciones de red fuente y destino, están incluidas con los datos transmitidos, para asegurar que es recibido apropiadamente por el dispositivo correcto.

Suites de Protocolos

Los protocolos están normalmente activos en una red dada simultáneamente. En muchos casos, los diferentes protocolos que existen en un ambiente de red son relativos a otros como miembros de lo que es conocido como Suite de Protocolos (conjunto de protocolos).

Algunos protocolos son propietarios; diseñados para correr sólo en los equipos producidos por los fabricantes que los definieron. Ejemplos de Protocolos propietarios y sus correspondientes fabricantes incluyen DECnet de Digital Equipment Corporation, IPX de Novell, SNA de IBM y XNS de Xerox Corporation.

En el mundo de la conectividad de hoy, estos sistemas propietarios populares han llegado a ser estándares de fábrica y son soportados por muchos fabricantes. Los Suites de Protocolos normalmente incluyen interfaces de sistemas con los estándares de Suites de Protocolos de fabricantes independientes. Hay dos estándares de Suites de Protocolos de fabricantes independientes, internacionalmente reconocidos.

- La suite Protocolo de Control de Transmisión / Protocolo Internet. Transmission Control Protocol / Internet Protocol (TCP / IP)
- La suite Interconexión de Sistema Abiertos. Open Systems Interconecct (OSI)

Ambos son estándares abiertos, lo que significa que no son propietarios. Cualquier fabricante puede ofrecer conectividad TCP / IP ó OSI en sus productos. El suite TCP /

IP ha logrado alcanzar una posición sólida en el mercado de conectividad. TCP / IP ha sido establecido por el grupo de Actividades de Internet (Internet Activities Board - IAB), el cual es un grupo de organizaciones corporativas, académicas y gubernamentales.

El otro modelo, la suite OSI está definida y aprobada por la Organización de Estándares Internacionales (International Standards Organization - ISO).

La conectividad basada en estándares, se refiere a la conectividad de sistemas basados en la Suite de Protocolos TCP/IP o en la OSI. Cada Suite puede servir como base para un fabricante independiente, resultando en ambiente de red completamente interoperable. La tabla 1-1 lista las Suites de Protocolos, mostrando la relación entre sus layers (capas). Los niveles del Modelo de Referencia OSI se discuten más adelante.

Tabla 2-1. Niveles de TCP / IP y OSI

TCP/IP	**Modelo de Referencia OSI**
Aplicación	Aplicación
	Presentación
TCP	Sesión
	Transporte
IP	Red
Subred	Capa enlace
	Física

Protocolos y Capas

Los Protocolos son reglas de comunicación de datos deben ser ejecutados en un cierto orden, usualmente de arriba hacia abajo en la transmisión y de abajo hacia arriba en la recepción.

Si hacemos una analogía entre el *Envío de una carta y los protocolos*, como se muestra en la figura 2-1, veremos como se usan las capas o niveles de los protocolos.

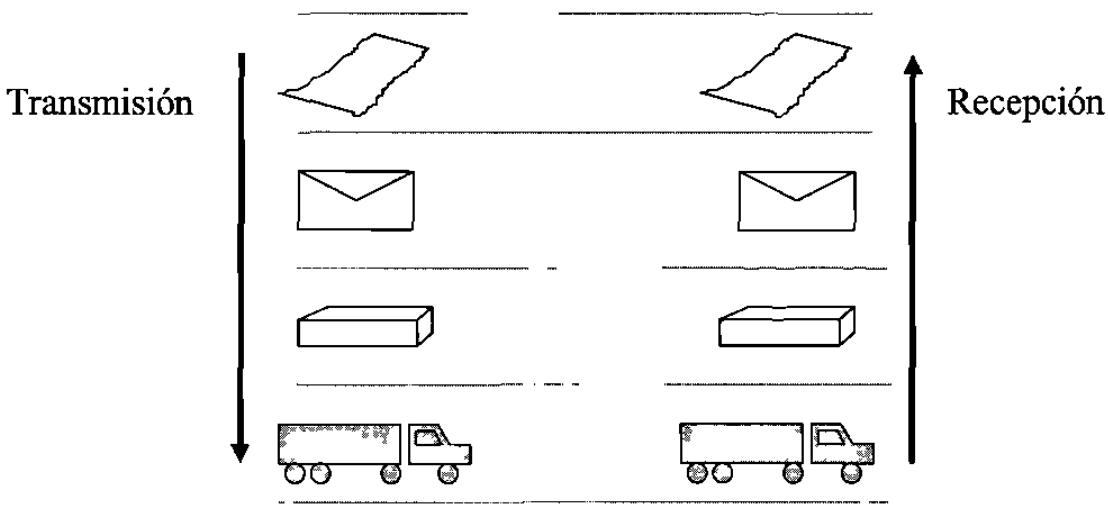


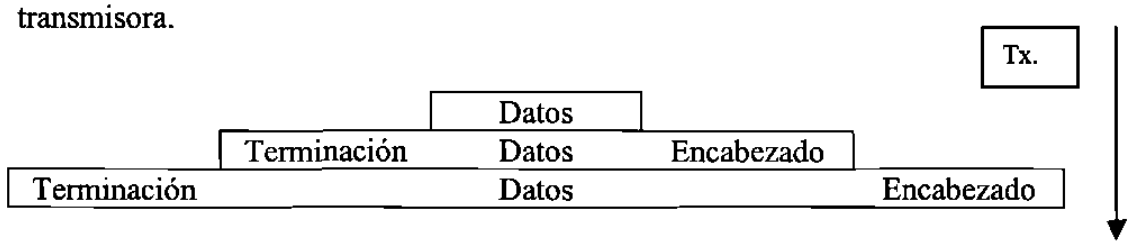
Figura 2-1 Analogía de cómo se usa cada capa en los protocolos.

1. Los datos a enviar son el mensaje escrito en la carta.
2. La carta es colocada en un sobre con la dirección del remitente, el destino, y la información de control (como primera clase, correo aéreo, urgente, etc.).
3. La carta va a la oficina de correo, donde es colocada en un caja con las otras cartas destinadas para la misma ciudad.
4. La carta es transportada a la otra ciudad.
5. Un trabajador postal en el destino, abre la caja y ordena los sobres.
6. El sobre original es entonces llevado por un cartero, donde es abierto y el mensaje es recibido.
7. Si un control especial fue solicitado (como correo certificado), el cartero es responsable de implementar el procedimiento correcto.

Los Protocolos que son usados para mandar datos a través de una red de comunicaciones operan casi de la misma manera que el correo. Los datos a enviar desde un nodo a otro son empaquetados por cada Protocolo para su transporte, como se coloca una carta dentro de un sobre, luego en una caja y finalmente en un camión.

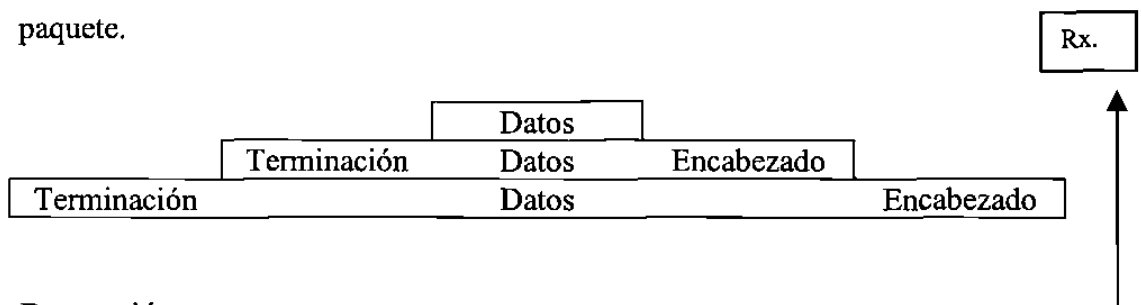
El software del Protocolo reside en la memoria de la computadora o en la memoria de un dispositivo de transmisión como una tarjeta de interfaz de red (Network Interface Card - NIC). Cuando los datos están listos para su transmisión, este software de Protocolo se ejecuta.

El software del Protocolo prepara los datos para transmisión y empieza el proceso de transmisión. El software del Protocolo en el receptor retira los datos del cable y los prepara para la computadora. quita toda la información que le adicionó la estación transmisora.



Transmisión

El proceso de transmitir los datos se logra al pasar los datos de una capa de protocolo a otra capa inferior. El protocolo de cada capa agrega información a los datos que pasan por esa capa, en forma de encabezado y terminación. El protocolo en cada capa, considera datos como la combinación de los datos de usuario y los encabezados de todas las capas anteriores. Eventualmente, los datos pasan a través de todas las capas en una familia de protocolos dada, y es transmitido en un conjunto discreto de bits llamado paquete.



Recepción

En la estación receptora, el paquete es pasado de las capas protocolos inferiores a los superiores. Al protocolo de cada capa sólo le concierne la interpretación de la información contenida en el encabezado y/o terminación. El protocolo considera que el resto del paquete son los datos que debe enviar a los protocolos de capas superiores.

2.3.Modelo de referencia OSI.

El Modelo de Referencia OSI puede ser visto como un conjunto de capas funcionales conteniendo las reglas que cada estación de una red debe seguir para intercambiar información. Un Protocolo estándar lista las reglas específicas que deben cumplir en cada capa. Cada capa es un módulo, es decir, un protocolo puede (teóricamente) ser sustituido por otro en la misma capa, sin afectar la operación de las capas superiores ni inferiores.

El Modelo de Referencia OSI es un concepto que describe cómo se realizaría la comunicación de datos. Esto provee las bases comunes para la coordinación del desarrollo de estándares para la interconexión de sistemas, mientras que permite a los estándares existentes ser colocados en perspectiva con el modelo.

La figura 2-2 muestra las siete capas del Modelo de Referencia OSI. Nótese que cada capa manda paquetes a las superiores e inferiores, pero cada capa sólo entiende la información que viene de la misma capa desde el otro extremo.

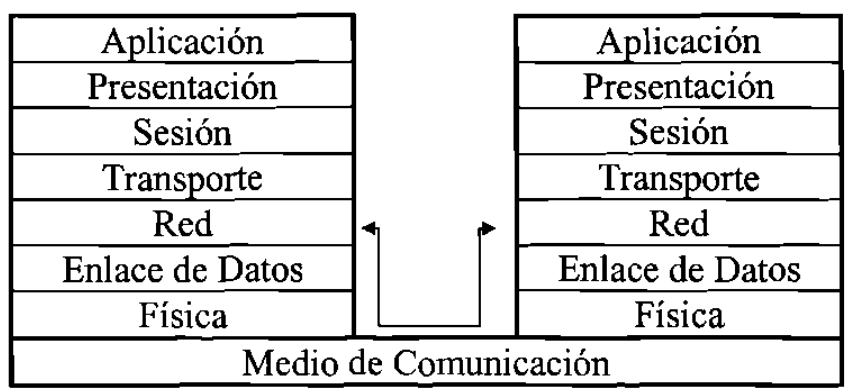


Figura 2-2. Paquetes en el Modelo de Referencia OSI.

Capa Física

La Capa Física transmite un tren de bits sobre el medio físico, y describe la interfaz funcional, mecánica y eléctrica de la portadora. Es la Capa Física la que lleva la señal para todas las capas superiores. RS-232 es un ejemplo de un estándar de Capa física. La Capa Física incluye:

- Bits en forma de voltajes.
- Interfaz entre medio y medio.
- Modo de transmisión (Full o Half dúplex).
- Asignaciones de los Pins.

En la analogía del envío de carta por el correo de la figura 2-1, el camión y la autopista proveen los servicios de la Capa Física.

Capa de Enlace de Datos

El propósito principal de la capa de Enlace de Datos es el de asegurar una transmisión de información libre de errores entre dos terminales conectadas al mismo cable físico. Esto permite a la siguiente capa superior suponer virtualmente, una transmisión libre de errores sobre la capa física. Ethernet, Token Ring, y FDDI son protocolos que operan en esta capa.

La Capa de Enlace de Datos es responsable de empaquetar y colocar los datos en el cable de red. Administra el flujo de las cadenas de bits de datos hacia adentro y afuera de cada nodo de la red. Las siguientes son funciones de La Capa de Enlace de Datos:

- Crea y reconoce los límites de las tramas
- Comprueba los mensajes recibidos para su integridad.
- Administra el acceso a canales y controla el flujo.
- Asegura la secuencia correcta de los datos transmitidos.
- Detecta y corrige posibles errores que ocurran en la Capa Física.
- Provee técnicas de control de flujo para asegurar que la capacidad del buffer del enlace no se exceda.

En analogía con la figura 1-1, la Capa de Enlace de Datos carga a los camiones de correo, manda cada camión hacia la autopista, y se asegura que lleguen en forma segura.

Capa de Red

La Capa de Red controla la operación de las redes o subredes. Esta capa decide qué camino físico deben seguir los datos basada en las condiciones de la red, prioridades del servicio y otros factores.

El software de Capa de Red residente en cada estación de usuario debe construir el paquete de datos en forma que el software de Capa de Red residente en los dispositivos de ruteo de la red puedan reconocerlos y enrutar los datos a la Dirección Destino correcta.

La Capa de Red releva a las capas superiores de la necesidad de conocer todo acerca de la transmisión de datos usadas para conectar sistemas. Es responsable de establecer, mantener y terminar las conexiones usando las facilidades de comunicaciones. El Protocolo Internet (IP de TCP / IP) es un ejemplo de un Protocolo que opera en esta capa. El Intercambio de Paquetes Internos de la Red (Internetwork Packet Exchange - IPX) de Novell son otros ejemplo. Las tareas de esta Capa de Red incluyen:

- Direccionar mensajes.
- Ambientar el camino entre los nodos de comunicación en las posibles redes diferentes.
- Rutear mensajes a la red.
- Controlar la congestión si hay muchos paquetes en la red.
- Traducir direcciones lógicas, o nombres, a direcciones físicas.
- Usar funciones de conteo para contar los paquetes o bits enviados por los usuarios para producir información de cuentas.

En nuestra analogía de la figura 2-1, la Capa de Red actúa como los centros de distribución de correos regionales a través del país. Los camiones llevan dirección hacia los centros y son ruteados a lo largo de los mejores caminos hacia sus destinos finales.

Capa de Transporte

La Capa 4 y las superiores del Modelo de Referencia OSI son generalmente llamadas capas altas. Los Protocolos a esos niveles son extremo a extremo, y no les conciernen los detalles de las facilidades de comunicación de capas de bajo nivel.
La Capa de Transporte forma la interfaz entre estas capas superiores orientadas a aplicaciones y las subyacentes capas dependientes de Protocolos de la red. Esto provee a la Capa de Sesión, las facilidades de una transferencia confiable de mensajes, y también ofrece transferencia transparente de datos entre terminales, corrección de errores y control de flujo.

En la analogía de la figura 2-1. Las funciones de la Capa de Transporte son ilustradas por el despachador del camión de correos que toma el control si existe un accidente en carretera.

Capa de Sesión

Los Protocolos arriba de la Capa de Transporte *no están críticamente envueltos en el* proceso de conectividad, por lo que sólo se mencionan para propósitos de información.

La Capa de Sesión provee los medios para que dos entidades de Capas de Aplicación sincronicen y administren su intercambio de datos. Esta capa establece un canal de comunicación entre dos entidades de Capas de Aplicación o Presentación por la duración de la transacción de red, administra la comunicación, y termina la conexión. Esto es conocido como una Sesión.

Capa de Presentación

La Capa de Presentación formatea los datos que serán presentados en la Capa de Aplicación. Puede ser visto como un traductor para la red. La Capa de Presentación provee una representación común para los datos que puedan ser usados entre los procesos de aplicaciones. La Capa de Presentación releva a las entidades de aplicación de ocuparse de la representación de datos, por lo que provee independencia de sintaxis. Algunas de las funciones de la Capa de Presentación incluyen:

- Codificación de datos (enteros, Punto flotante, ASCII, EBCDIC etc.)
- Compresión de datos para reducir el número de bits transmitidos
- Codificación de datos para privacía y autentificación.

En la analogía, la Capa de Presentación funciona como un traductor que interpreta una carta recibida, de Francés a Español.

Capa de Aplicación

La Capa de Aplicación sirve como una ventana para el proceso de aplicación para tener acceso al ambiente de red. Esta capa representa a los servicios que directamente soporta a los usuarios y a las tareas de aplicación. La capa de Aplicación contiene una variedad de Protocolos que son comúnmente usados para:

- Terminales virtuales de red
- Transferencia de archivos
- Acceso a remoto a archivos
- Correo electrónico
- Administración de red

En la analogía con la figura 2-1, la Capa de aplicación funciona como la persona que escribe o lee a carta.

Resumen del Modelo de Referencia OSI

La tabla 2-2 contiene un resumen de las funciones de cada capa.

Tabla 2-2. Resumen del Modelo de Referencia OSI.

Capa	Función	Descripción
7	Aplicación	Selecciona los servicios apropiados para la aplicación (Interfaz de usuario)
6	Presentación	Provee conversión de códigos y reformateo de datos
5	Sesión	Coordina la interacción entre los procesos de aplicaciones de extremo a extremo
4	Transporte	Provee integridad de datos de extremo a extremo y calidad de servicio
3	Red	Conmuta y rutea la información hacia cualquier nodo
2	Enlace de Datos	Transfiere unidades de información hacia el otro extremo del enlace físico
1	Física	Desempeña transmisión / recepción en el medio de comunicación de la red

2.4.Definición de Conectividad.

Los sistemas computacionales son una mezcla de computación, y comunicaciones con equipos de diferentes fabricantes que tienen características diferentes. La conectividad enlaza conjuntamente diferentes LANs y WANs a través de diferentes lugares.
La conectividad es asegurar la transmisión de datos sin importar el protocolo o los medios.

Durante la década de los 80s, las Redes proliferaron y llegó a ser necesario interconectarlas. El correo electrónico fue la aplicación que estimuló la necesidad de interconexión de los 90s. Entonces otras aplicaciones empezaron a ser uso de la computación distribuida, la tendencia hacia la conectividad continuó.

Inter-redes Locales y de Area Amplia. (Internetworks)

Los dos tipos fundamentales de Inter-redes son las Locales y las de Area Amplia.

Inter-redes Locales	Conectan redes que están geográficamente cercanas, por ejemplo, una Inter-red local conecta todas las Redes dentro de un gran edificio de oficinas.

Inter-redes de Area Amplia:	Conecta a redes distantes geográficamente como en diferentes ciudades. La Inter-red de un gran Corporativo puede combinar un gran número de Inter-redes Locales.

Aunque la definición más simple de una Inter-red (Internetwork) es una red de redes, las Inter-redes son mucho más complejas que una simple red. Esta complejidad surge porque deben soportar típicamente:

- Numerosas Topologías e híbridos

- *Muchos Protocolos*
- Diferentes Medios de transmisión
- Un gran número de Dispositivos

Cuando las Inter-redes crecen, es necesario segmentarlas en sub-redes más pequeñas y más administrables. Esto se hace utilizando dispositivos de conectividad tales como Repetidores, Bridges, Routers y Gateways.

Dispositivos de Conectividad

El modelo de referencia OSI provee una representación simple de como se mueve la información a través de una red. Esto puede servir como una base para entender y describir una estrategia completa de conectividad. La relación de los diferentes dispositivos de conectividad con el Modelo de Referencia OSI se muestra en la figura 2-3.

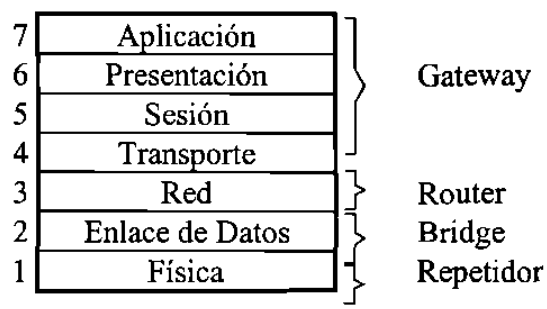


Figura 2-3 Dispositivos de Conectividad y el Modelo de Referencia OSI.

Gateway	Dispositivo que opera en las capas de Sesión y Aplicación. Conecta ambientes de red diferentes o no relacionados, como los protocolos SNA y DECnet. Un convertidor de protocolo puede ser usado como parte de un Gateway para traducir datos de un conjunto de protocolos a otro. Los gateways se relacionan con aplicaciones específicas y configuraciones de red.
Router	Dispositivo que opera en la capa de Red, conecta redes a Inter-redes que están físicamente unificadas, pero en las cuáles cada red retiene su identidad como un segmento separado de red. El propósito primario es encontrar el mejor camino de una red a otra y enviar paquetes entre ellos. Los Routers son visibles a las estaciones.
Bridge	Dispositivo que opera en la capa de Enlace de Datos. Usualmente conecta redes de tipos similares (Ethernet, FDDI, Token Ring) en Inter-redes lógica y físicamente sencillas. Recientemente, sin embargo, los Bridges de traducción han sido desarrollados para conectar diferentes tipos de LANs. Los Bridges almacenan y reenvían los datos en paquetes; y son transparentes a las estaciones al igual que los Repetidores.
Repetidor	Dispositivo que opera en la capa Física. Recibe una transmisión (bits) de un segmento de LAN y regenera los bits para ayudar a una señal degradada y para extender la longitud de los segmentos de LANs. No son técnicamente dispositivos de conectividad porque sólo extienden un segmento lógico de LAN, pero se dice que es uno.

Administración de Red

Como las redes e Inter-redes se han hecho vitales para la operación continua de una empresa, la Administración de las Redes e Inter-redes se ha hecho críticamente importante. Este campo se ha visto rápidamente en evolución y en desarrollo y los beneficios que ofrece son muy grandes; no obstante que los fabricantes han estado luchando por satisfacer los requerimientos vagamente definidos por los usuarios.

Los Bridges, los Routers, y otros dispositivos de conectividad deben ofrecer un buen rango de funcionalidad de Administración de Red, con mucho énfasis en Fallas, Configuración, Desempeño y Seguridad.

- La administración de Fallas es un sistema automático que provee detección de fallas, diagnósticos, corrección y administración.
- La administración de Configuración identifica, configura y controla los dispositivos en la red, incluyendo dispositivos remotos.
- La administración del Desempeño evalúa la confiabilidad del sistema y el nivel de desempeño, esto ocasiona la recolección, almacenamiento y reporte de estadísticas de desempeño, y el uso de sistemas expertos para analizar y ofrecer sugerencias para mejorarlo.
- La administración de la Seguridad ofrece herramientas para proveer autorización y autentificación del acceso a los recursos de la red.

Uno de los Protocolos de Administración más comúnmente implementados es el Protocolo Simple de Administración de Red (Simple Network Management Protocol - SNMP). Este Protocolo fue desarrollado para proveer una estructura de Administración de Red en redes TCP/IP. Otro protocolo estándar de administración de red es usado por la Suite de Protocolos Interconexión de Sistemas Abiertos (Open Systems Interconection- OSI). Como el estándar OSI es relativamente complejo. Sin embargo, IBM, AT&T, y otros grandes fabricantes de administración de red soportan el estándar OSI. Como se están fabricando muchos productos OSI, el uso de protocolos OSI han llegado a ser más común.

Beneficios de Redes Basadas en Estándares

Para implementar una solución de conectividad, existe una vasta clasificación de equipos de conectividad disponibles de varios fabricantes.

Es importante que todos los dispositivos de conectividad comprados sean Interoperables (conectividad sin importar la marca). Un equipo Interoperable se dice que opera bajo las mismas reglas, porque los equipos Interoperables están basados en estándares, sin importar la marca y trabajan fácilmente desde el principio, simplificando las tareas de incorporar equipos heterogéneos en un ambiente unificado. Esto permite a los administradores de red seleccionar el equipo correcto para el trabajo, en lugar de empezar sujeto a una solución propietaria disponible de un fabricante independiente.

Capitulo 3

Protocolos de Redes Locales

3.1 Introducción

En este capítulo analizaremos los tres protocolos de redes locales más comunes y estos están definidos en la Capa Física y de Enlace de Datos. Los dos estándares más populares definidos por el Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronic Engineers - IEEE). El IEEE 802.3 describe el estándar Ethernet, el IEEE 802.5 describe el estándar derivado de la tecnología Token Ring de IBM. La tercera, Interfaz de Distribución de Datos por Fibra (Fiber Data Distribuited Interface - FDDI) es otro protocolo de red definido por el Instituto Nacional de Estándares Americanos (American National Standards Institute - ANSI)

3.2 Estándar IEEE.

El estándar IEEE divide la capa de Enlace de Datos de OSI en dos subcapas:

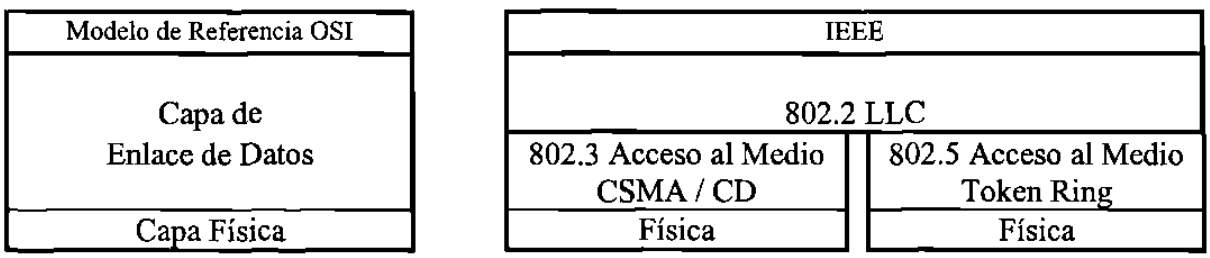
La Capa de Control de Acceso al Medio (Media Access Control - MAC) la cual trata con las técnicas de Acceso al Medio para un Medio físico compartido. Un Medio compartido divide el ancho de banda entre los dispositivos individuales bajo el principio de "uno por uno".

La Capa de Control de Enlace Lógico (Logical Link Control - LLC) extiende la capa de Enlace de datos tradicional, proveyendo la habilidad de soportar una o más conexiones lógicas en un solo medio.

Las dos subcapas trabajan juntas para proveer comunicaciones libres de error entre los nodos de red. La subcapa MAC gana el acceso al Medio de la red. La subcapa LLC provee servicios "extremo a extremo" (end to end), tales como el establecimiento

de la conexión, el control de flujo, la recuperación de errores, y secuencia del "frame" (paquete de bits).

Todas las LAN IEEE tienen la misma capa LLC, como se define por el estándar 802.2, esto permite que los mecanismos de las capas superiores sean los mismos sin importar el tipo de hardware de red. La figura 3-1 ilustra la relación entre el estándar IEEE 802 y el Modelo de Referencia OSI.



La figura 3-1 Relación entre el Modelo de Referencia OSI y el Estándar IEEE

3.3 Ethernet - IEEE 802.3

El diseño de la red Ethernet fue creado a mediados de 1970 como resultado de un trabajo experimental desarrollado por Xerox Corporation en su Centro de Investigación en Palo Alto (Palo Alto Research Center - PARC). La primera LAN Ethernet se extendió a una distancia de 1 kilómetro, soportando 100 estaciones y alcanzando rangos de 2.94 Mbps.

Ethernet llegó a ser tan popular que se convirtió en una estándar de fábrica. Digital Equipment Corporation (DEC), Intel Corporation, y Xerox propusieron la adopción de Ethernet como un estándar IEEE 802. La propuesta Ethernet fue renombrada IEEE 802.3.

Topología.-

La Topología básica de las redes Ethernet tradicionales es un bus. La configuración de bus utiliza uniones en T (taps) para conectar todas las estaciones al mismo cable. Cada estación tienen una dirección única y lee todos los mensajes que

atraviesan la red. La estación toma acción sólo en los mensajes especialmente direccionados a ella.

La figura 3-2 ilustra una topología de bus.

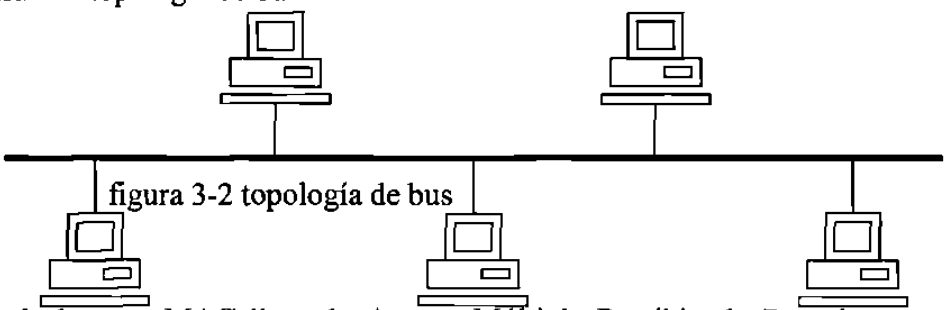


figura 3-2 topología de bus

Operación.-

El método de la capa MAC llamado Acceso Múltiple Percibiendo Portadoras, con Detección de Colisiones (Carrier Sense Multiple Access with Collision Detection - CSMA/CD) es el método de acceso Ethernet. Este determina cuando los datos son transmitidos y recibidos.

Antes de que una terminal Ethernet transmita, se pone primero en estado de "escucha", para determinar si alguna otra terminal ya está transmitiendo. A la presencia de una transmisión se le llama Portadora (carrier).

Si la terminal detecta una portadora, esperará un mínimo de 9.6 microsegundos después de que pase el último bit del paquete o frame antes de volver a transmitir. Si la estación trata de transmitir cuando una portadora está presente, o cuando dos estaciones empiezan a transmitir simultáneamente, resulta una transmisión alterada, a la cuál se le llama Colisión.

La figura 3-3 ilustra lo que sucede cuando dos estaciones tratan de transmitir al mismo tiempo.

1. La estación A transmite un "frame" (paquete) de datos.
2. La estación B empieza a transmitir antes de que el frame de la estación A alcance a la estación B.
3. Ocurre una colisión.
4. Tanto la estación A y la B detectan la colisión, y ambas abortan sus transmisiones y esperarán un momento para volver a intentar transmitir.

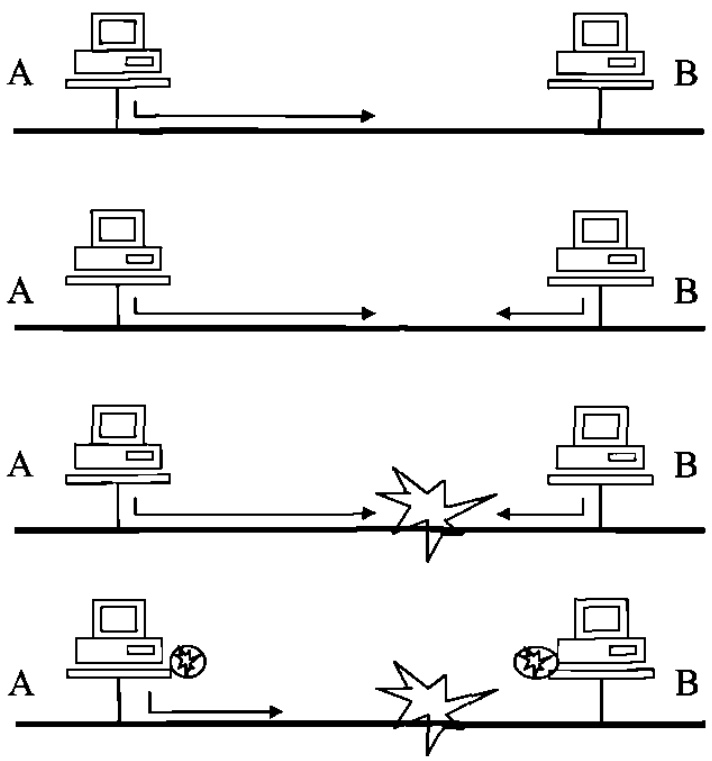


Figura 3-3 CSMA/CD en redes Ethernet.

Proceso de detección de colisiones.-

La primera estación que detecta una Colisión, mandará una señal especial de bloqueo para notificar a las demás estaciones que una Colisión ha ocurrido. Todas las estaciones esperarán un intervalo de tiempo aleatorio antes de volver a intentar transmitir.

Si ocurrieran muchas Colisiones sucesivamente, el intervalo de tiempo aleatorio se va duplicando sucesivamente después de cada Colisión. Después de diez Colisiones consecutivas, el intervalo ya no continúa duplicándose, porque esto disminuiría el desempeño de la red.

En una red extremadamente congestionada, es posible pensar que una estación nunca pueda transmitir, sin embargo en la realidad esto raramente ocurre, a menos que una red tenga muchas estaciones extremadamente ocupadas, o con aplicaciones corriendo durante todo el día.

Formato de frame Ethernet

Los datos transmitidos en una LAN Ethernet están empaquetados en frames. Los formatos de frame IEEE 802.3 y Ethernet son ligeramente diferentes. Estos se ilustran en la figura 3-4

IEEE 802.3

Pre-ámbulo	Delimitador de Inicio	Dirección Destino	Dirección Fuente	Longitud	Campo de Datos	Pad	FCS
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	N bytes	N bytes	4 bytes

1500 bytes

Ethernet

Preámbulo	Dirección Destino	Dirección Fuente	Tipo	Campo de Datos		FCS
8 bytes	6 bytes	6 bytes	2 bytes	N bytes		4 bytes

1500 bytes

Figura 3-4 Comparación entre formatos de frame IEEE 802.3 y Ethernet

Preámbulo	Son los primeros ocho bytes del frame Ethernet y los primeros siete bytes del frame IEEE 802.3. Estos son usados para Sincronización y, en el caso de Ethernet, para marcar el inicio de un frame.
Delimitador de inicio	(IEEE 802.3) Especifica un byte de inicio de frame.
Dirección Destino	Identifica la estación que va a recibir el frame. La dirección Destino puede referirse a una estación (Unicast), a un grupo de estaciones (Multicast), o a todas las estaciones (Broadcast). El IEEE 802.3 y el Ethernet especifican direcciones destino de 48 bits.
Dirección Fuente	Identifica a la estación que manda el frame. El IEEE 802.3 y el Ethernet especifican direcciones fuente de 48 bits.

Longitud	(IEEE 802.3) Determina la longitud del campo de información cuando un campo Pad se incluye en el frame.
Pad	(IEEE 802.3) Especifica un Número Mínimo de bytes por frame para que las colisiones se detecten apropiadamente. Si el frame no incluye muchos bytes, se suma el campo Pad.
Tipo	Ethernet no soporta los campos Pad y Longitud, en lugar de eso, un campo "Tipo" de dos bytes especifica el tipo de paquete para las capas superiores de la red.
Datos	Es la Información contenida en el paquete. El tamaño máximo de frame es de 1526 bytes incluyendo el preámbulo. Este tamaño refleja el tamaño del buffer de la tarjeta adaptadora y la necesidad de limitar el tiempo total en que se ocupa el medio mientras se está transmitiendo. Si los datos mandados requieren un frame más largo que 1526 bytes, las capas superiores deben dividir los datos en paquetes individuales (proceso de fragmentación).
Secuencia de Verificación de frame	(Frame Check Sequence -FCS) Verificación de errores de transmisión. La estación emisora realiza una Verificación de Frame Redundancia Cíclica (Cyclical Redundancy Check - CRC) en los bits del frame y almacena el resultado de este cálculo en el campo de Secuencia de Verificación de Frame FCS. La estación receptora realiza el mismo cálculo y compara el valor calculado con el valor del campo FCS. Si los valores son diferentes, la estación receptora asume que ha ocurrido un error y solicita una retransmisión del frame.

Estándares de cableado Ethernet

Hay tres estándares de cableado Ethernet de uso común:

- El estándar 10Base5 de Ethernet, está basado en Cable Coaxial grueso.
- El estándar 10Base2, Thin Ethernet, está basado en Cable Coaxial delgado.
- El estándar 10BaseT, está basado en cable UTP, par trenzado sin blindar (Unshielded Twisted Pair - UTP)

Los datos son transmitidos como una señal digital de banda base cuyo espectro no se altera excepto por repetidores y efectos del medio.

10Base5

En la designación 10Base5, el 10 es por los 10 Mbps de operación; Base representa la operación en Banda Base y el 5 es por segmentos de 500 mts. Un segmento sencillo de cable no puede ser más largo que 500 metros, después de esto, debe usarse un repetidor para amplificar y regenerar la señal.

El cable 10Base5 es conocido también como Thick Ethernet (grueso) porque el Cable Coaxial es más grueso que el utilizado para Thin Ethernet (10Base2). Cada estación Ethernet se comunica al cable coaxial a través de un transceiver externo también conocido como Unidad de Conexión al Medio (Medium Attachment Unit - MAU).

Una tarjeta adaptadora dentro de la estación, también conocida como tarjeta de Interfaz de Red (Network Interface Card -NIC), se conecta con el transceiver. Los terminadores eliminan la reflexión de la señal al Cable Coaxial en ambos extremos. La figura 2-5 ilustra los componentes de una red Thick Ethernet.

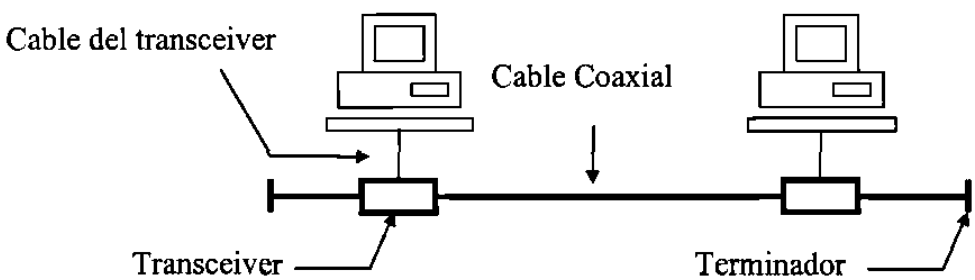


Figura 3-5 Componentes de una red Thick Ethernet

La tabla 3-1 describe las reglas de cableado para cable 10Base5

Tabla 3-1 Reglas de cableado 10Base5

Características 10Base5	**Valor**
Rango máximo de datos	10 Mbps
Repetidores máximos	4
Longitud máxima de cable del Transceiver	50 metros
Estaciones máximas por segmento	100
Estaciones máximas	1024
Distancia mínima entre estaciones	múltiplos de 2.5 m.
Segmento coaxial máximo sin Repetidor	500 metros
Longitud Ethernet máxima con Repetidores	2500 metros

Aunque el número máximo de estaciones totales conectadas a todos los segmentos es 1024, puede notarse que el repetidor cuenta como una estación.

10Base2

El Cable Coaxial 10Base2 es más delgado que el cable 10Base5, de ahí que muchas veces se le llame Thin Ethernet. Como es más delgado, es menos caro y más fácil de instalar que el Thick Ethernet. El número 2 representa aproximadamente 200 metros (realmente 185 metros) por segmento.

10Base2 no requiere un transceiver externo. La tarjeta NIC desempeña todas las *funciones del transceiver mientras que el conector "T" conecta la tarjeta con el Cable* Coaxial. La tabla 2-2 describe las reglas de cableado 10Base2.

Tabla 3-2 Reglas de cableado 10Base2

Características 10Base2	**Valor**
Rango de datos máximo	10 Mbps
Repetidores máximos	4
Máximas estaciones por segmento	30
Estaciones máximas	1024
Distancia mínima entre estaciones	0.5 m.
Segmento coaxial máximo sin Repetidor	185 metros
Longitud Ethernet máxima con Repetidores	925 metros

Independientemente de sí se implementa 10Base5 o 10Base2, el uso del Cable Coaxial tiene ciertas ventajas y desventajas. Mientras que este cable es resistente a

interferencias y ofrece un gran ancho de banda, es más caro que el cable Par Trenzado, y algunos estándares de red; como el Token Ring; no lo soportan, también es difícil de doblar y por lo tanto es más difícil de instalar.

10BaseT

Este estándar de cableado provee un desempeño de 10 Mbps sobre cable Par Trenzado sin Blindar (Unshielded Twisted Pair - UTP). El cable Par Trenzado viene en una variedad de formas y tamaños, incluyendo versiones blindadas y sin blindar. Los cables trenzados minimizan la interferencia creada entre dos cables adyacentes. El cable UTP tiene él más bajo costo de todos los tipos de cableado de cobre. Tanto Ethernet como Token Ring requieren dos pares de cables, uno para transmitir y otro para recibir. El UTP es uno el más popular estándar de cableado, debido a su bajo costo y a su relativa facilidad de instalación.

Sin embargo, el cable UTP está muy cerca de su ancho de banda límite, tiene poca resistencia al diafonía y es susceptible a interferencias magnéticas, ya que no está blindado. El cable STP tiene una mayor resistencia al diafonía y a otras interferencias, pero es más caro que el UTP y su tamaño más grueso llenan fácilmente los conductos de cableado. Las ventajas y desventajas deben considerarse para cada situación.

El estándar 10BaseT también especifica que las redes sean cableadas en una topología física de estrella. Las redes Ethernet tiene aún una topología lógica de bus, pero los cables UTP de cada estación deben llevarse hacia un panel de parcheo o en un concentrador (Hub) tal como se muestra en la figura 3-6.

Tabla 3-3 Reglas de cableado 10BaseT

Características 10BaseT	**Valor**
Rango de datos máximo	10 Mbps
Repetidores máximos	4
Máximas estaciones por repetidor	32
Estaciones máximas	128
Longitud Ethernet máxima con Repetidores	400 metros

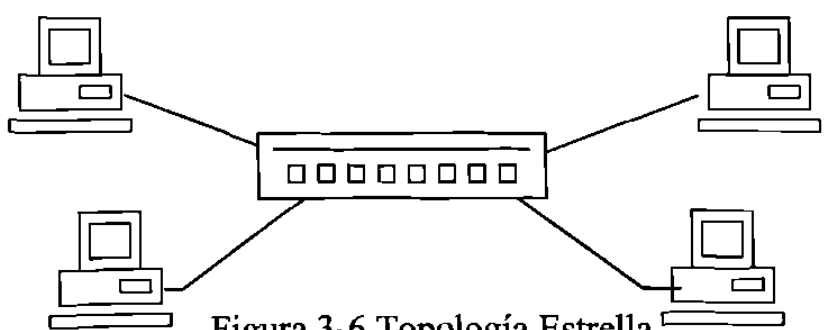


Figura 3-6 Topología Estrella.

3.4 Token Ring - IEEE 802.5

IBM fue la principal influencia detrás del estándar de LAN IEEE 802.5. La red Token Ring fue desarrollada por IBM para trabajar en sus ambientes de Mainframes. Como la base instalada de IBM es significante, tubo sentido definir un estándar de redes basado en la implementación de IBM.

Topología.-

Las LANs basadas en anillo están hechas de una cadena de enlaces punto a punto. Los anillos operan a 4 ó a 16 Mbps en un lazo cerrado. En el caso de cableado en anillo parece a una estrella. La figura 2-7 ilustra la topología de anillo.

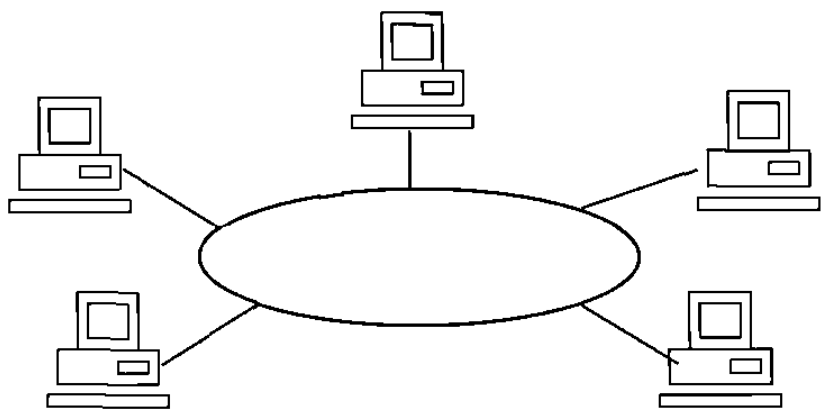


Figura 3-7 Topología de anillo.

Operación.-

El Token Ring es un método de acceso determinístico, llamado Token Passing, a diferencia del Ethernet CSMA/CD (donde cada estación compite con las demás para accesar al Medio), cada estación Token Ring espera una suma de tiempo preconfigurado o predeterminado para accesar al medio. Un grupo especial de bits, llamados "Token" circulan alrededor del anillo. Cualquier estación puede tomar el Token y reemplazarlo con un frame de información. Un contador de tiempo controla qué tanto una estación puede apropiarse de la red, antes de pasar el Token al siguiente nodo. Cuando la estación está por transmitir, reinserta el Token al anillo.

1. Una estación Token Ring puede operar de los siguientes modos:

2. Modo de Transmisión
3. Modo de Escucha
4. Modo de Omisión (Bypass)
5. Modo de Recepción

Para entrar al modo de transmisión, una estación toma el Token. Cambia al Bit-Token dentro del Token de 1 a 0, lo cual indica que el Token está ocupado, transmite su frame de datos, que especifica las direcciones fuente y destino.

Todas las estaciones en modo de Escucha checan la dirección destino en el frame, para determinar si está dirrecionado a ellos. Si el frame está direccionado a otra estación, una estación en modo Escucha copia (retransmite) los bits que le llegan al enlace.

Si la estación está apagada, está en modo de Omisión (Bypass) y el flujo de bits pasa por esta estación sin ser atendido.

Si una estación descubre que la dirección destino de un frame es la propia, entra en modo de Recepción. Copia el frame en memoria, modifica la bandera de estado (Status) del frame para indicar que ha recibido los datos correctamente y copia al frame de regreso al anillo. Cuando el frame regresa a la estación transmisora original, se examinan estas banderas de estatus para determinar si la dirección fue reconocida, si el frame fue copiado, y si llegó bien o alterado. Finalmente, esta estación retira los Bits del anillo.

En el caso de que el Token se perdiese ó se alterará, una estación especial llamada Monitor Activo examina ciertos bits del Token para determinar si ha circulado en el anillo por mucho tiempo, o si debe ser generado un nuevo Token. Cualquier estación puede actuar como monitor Activo, la elección de la estación que será monitor Activo se determina durante la inicialización del anillo. En caso de que el monitor Activo falle, pueden seleccionarse también monitores en espera.

Como cada estación en el anillo regenera el frame de datos con la misma potencia original, los repetidores no son necesarios. Esto significa que las redes Token Ring no están limitadas en distancia o velocidad, como las redes de topología de bus.

Formato de trama Token Ring

La figura 3-8 ilustra el formato del frame de información Token Ring.

D. de Inicio	Control de Acceso	Control de Frame	Dirección Destino	Dirección Fuente	Datos	FCS	D. de Final	Campo de Estado
1 byte	1byte	1 byte	2 ó 6 bytes	2 ó 6 bytes		4 bytes	1 byte	1 byte

Figura 3-8. Formato de frame Token Ring

Delimitadores de Inicio y Final	Secuencia especial de bits que especifica el inicio y el final de cada frame transmitido, sin importar el contenido.
Control de Acceso	Contiene los bits, Bit-Prioridad, Bit-Token y Bit-Monitor y Bit-Reservación. Se usan para controlar el acceso al anillo.
Control de Frame	Define el tipo de paquete o frame (Control de Acceso al Medio) y otras funciones de control.
Direcciones Fuente y Destino	Puede ser de 16 bits ó de 48 bits de largo. Pero para una red especifica debe ser lo mismo para todas las estaciones.
Datos	Puede llevar datos o información de control adicional. No hay una longitud máxima específica, pero en la práctica está limitada al tiempo máximo permitido para que una estación transmita mientras retiene el Token.
Frecuencia de Verificación de frame	(Frame Check Sequence - FCS). Es una Verificación de Redundancia Cíclica (Cyclical Redundance Check - CRC) de 32 bits que funcionan similarmente a la descrita en el formato de Frame Ethernet.
Campo de estado del frame	Permite a la estación fuente, determinar si la estación direccionada no existe o está apagada, si está activa pero no el no copió el frame, o si está activa y copió el frame.

Componentes del Token Ring

El estándar 802.5 especifica ciertos tipos de dispositivos y cableados. Hay tres componentes básicos.

- Tarjetas de interfaz de Red (Network Interface Card - NIC)
- Unidades de Acceso Multiestación (Multi-station Access Unit - MAU)
- Cableado de Red.

Tarjetas de Interfaz de Red (Network Interface Card - NIC)

Las tarjetas Token Ring se conectan en cada estación y están disponibles en versiones de 4 Mbps y 16 Mbps. Sin embargo, dos tarjetas de diferente velocidad no pueden operar en el mismo anillo. La versión de 16 Mbps está diseñada para backbones departamentales que soportan múltiples grupos de usuarios y la versión de 4 Mbps es para conexiones de pequeños grupos de trabajo.

Unidades de Acceso Multiestación (Multi-station Access Unit - MAU)

La Unidad de Acceso Multiestación en un cableado centralizado en el que las estaciones Token Ring están conectadas mediante cables adaptadores, y pueden conectarse múltiples unidades juntas. La terminología Token Ring utiliza la abreviación MSAU en estas unidades, para que no sea confundida con la Unidad de Conexión al Medio (*Medium Attachment Unit* - MAU) del estándar IEEE 802.3.

Cableado de Red Token Ring

El sistema de cableado de Token Ring es implementado comúnmente con algunas variedades que son las siguientes:

Tipo 1.- Son dos pares STP para transmisión de datos. El cable adaptador del estándar Token Ring está hecho de 8 pies.

Tipo 2.- Incluye seis pares de cables, dos STP para datos y cuatro pares UTP para voz. Esto es considerado el backbone del sistema de cableado.

Tipo 3.- Es el cable telefónico convencional UTP.

Tipo 5.- Consiste de dos cables de fibra óptica de 100/140 micras para transmitir datos entre cuartos de cableado.

Tipo 6.- Utiliza dos pares trenzados para transmisión de datos y es similar al tipo 1 pero más flexible. Puede conectar estaciones de trabajo, pero es usado principalmente como cables de parcheo en centros de cableado.

La tabla 2-3 describe las reglas de cableado básicas de Token Ring para los tipos 1, 2 y 3.

Tabla 3-4 Reglas de cableado Token Ring para los tipos 1, 2 y 3.

Características Token Ring	**Tipo 1, 2**	**Tipo 3**
Dispositivos máximos por anillo	260	96
Rango de transmisión de datos	16 Mbps	4 Mbps
Estación a un simple MSAU	300 metros	100 metros
Estación a múltiples MSAUs	100 metros	45 metros
MSAUs máximos por LAN	12	2
Distancia entre MAUs	200 metros	120 metros

3.5 La Interfaz de Distribución de Datos por Fibra

Introducción

Las redes en crecimiento cuentan con cables de fibra óptica para conectar varias redes y para proveer mayores anchos de banda para nuevas aplicaciones. Las fibras ópticas ofrecen muchas ventajas sobre los cableados de cobre basados en par trenzado e incluyendo cable coaxial:

- Mayor ancho de banda.
- Menor atenuación de la señal.
- Mayor integridad de datos.
- Inmunidad a interferencias electromagnéticas y de radio frecuencia.
- Mayor distancia entre estaciones.
- Mayor durabilidad.
- Mayor seguridad.

La Interfaz de Distribución de Datos por Fibra (Fiber Data Distribuited Interface - FDDI) es el estándar definido por el comité X3T9.5 del Instituto Nacional de Estándares Americanos (American National Standards Institute - ANSI) para interconexiones de LANs sobre cables de fibra óptica. Desde 1990, muchos usuarios manejaban la aceptación de FDDI, centrados en la necesidad de mayor Ancho de banda para aplicaciones con imágenes. El almacenamiento y recuperación de imágenes gráficas y el interés en transmisiones multimedia fueron conduciendo a la migración hacia FDDI.

Topología

El FDDI es una Topología basada en anillo, orientada para tráfico de datos de alta velocidad en un Anillo Doble con rotación encontrada, para redundancia. La figura 3-9 ilustra esta Topología. FDDI opera en las dos capas inferiores del Modelo de Referencia OSI: La capa Física y la de Enlace de Datos.

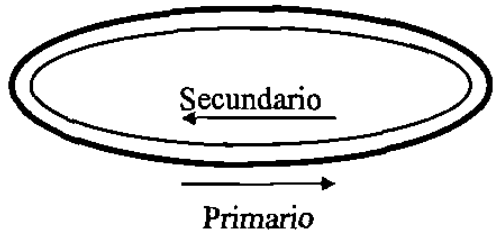


Figura 3-9 Anillos FDDI

Operación

El FDDI en un sistema de comunicación de datos que utiliza fibras ópticas en lugar de cables de cobre. La información es llevada sobre un medio óptico por haces modulados de luz. Los dispositivos en una red FDDI transforman las señales de luz en señales eléctricas para procesarse. La información es convertida nuevamente en haces de luz antes de ser colocada en el anillo.

Igual que el Token Ring, el FDDI es también un método de acceso a red Token Passing. La tecnología FDDI está basada en un par de anillos dobles, cada uno con dirección de rotación diferente. Operando a 100 Mbps, provee un Medio extremadamente rápido para el tráfico de datos, fue diseñada para operar con distancias entre estaciones de hasta 2 kilómetros.

La arquitectura de anillo doble también provee un alto grado de confiabilidad y tolerancia a fallas. Bajo operación normal, uno de los anillos (llamado Anillo Primario), lleva el tráfico de datos. El otro anillo (llamado Anillo Secundario) es generalmente usado para recuperación automática si hay una ruptura en el Anillo Primario.

Cuando ocurre una falla, como en la figura 3-10, las estaciones de cada lado de la falla, la detectan y omiten automáticamente. Está configuración de anillo es conocida como Anillo Protegido.

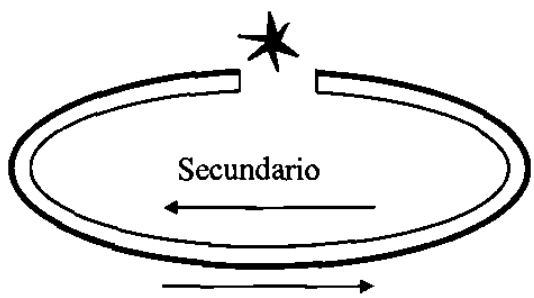


Figura 3-10 Anillo Protegido

En general, la operación FDDI es similar al método Token Passing descrito para Token Ring en la sección anterior de este capítulo.

Componentes FDDI

Existen tres componentes primarios de conexión en una red FDDI, los cuáles se ilustran en la figura 3-11.

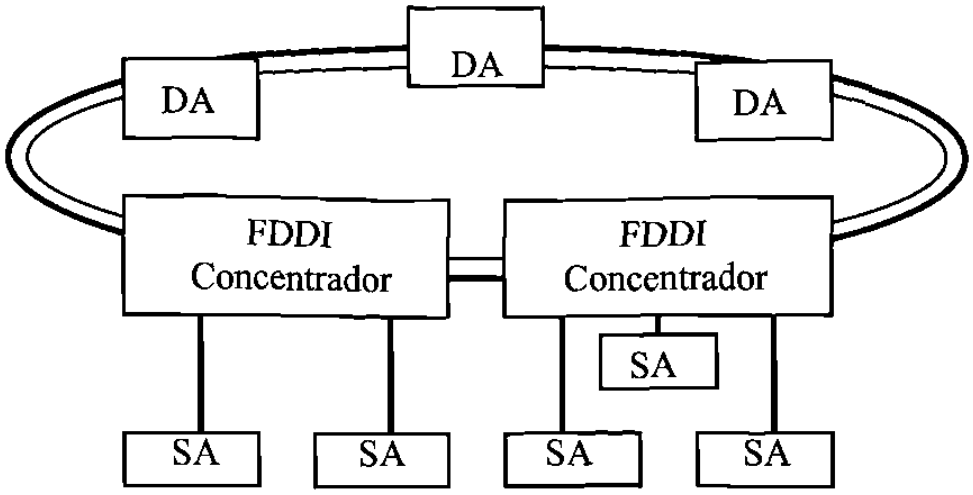


Figura 3-11 Componentes de una Arquitectura FDDI

El dispositivo de Conexión Doble (Dual Attachment - DA) conecta una estación a los anillos de fibra óptica Primario y Secundario (de respaldo) para permitir la Recuperación de Fallas (Fault Recovery). Si una falla ocurre en el Anillo Primario, los dispositivos cercanos a ambos extremos la detectan, y cada uno reconfigura automáticamente el camino de datos hacia el Anillo Secundario, protegiendo a la red de la falla.

El Concentrador FDDI se conecta a los dos anillos físicos de fibra óptica, para permitir la recuperación de fallas. Su función principal es administrar el acceso hacia el Backbone (Medio de transmisión principal) de fibra óptica, a todos los dispositivos no-FDDI conectados a él. Esto también contribuye a remover del anillo a los dispositivos con fallas y que no tienen la capacidad de recuperación de fallas

El dispositivo de Conexión Sencilla (Single Attachment - SA) conecta a una simple estación de trabajo al concentrador FDDI en una configuración estrella. Este dispositivo no ofrece

la recuperación de errores, debido a que no está conectado al Anillo Secundario, sin embargo el concentrador tiene una arquitectura altamente redundante.

Formato de frame FDDI

La figura 3-12 ilustra el formato de frame de información FDDI.

Todos los bits a ser transmitidos son codificados primero usando un código de grupo "4 de 5", lo que significa que por cada 4 bits, se genera una palabra codificada (símbolo) correspondiente de 5 bits, en el codificador. El número de símbolos de 5 bits, se muestra como una S en la figura 3-12

Pre - ámbulo	D. de Inicio	Control de Frame	Dirección Destino	Dirección Fuente	Datos	FCS	D. de Final	Campo de Estado
16 S	2 S	2 S	4 ó 12 S	4 ó 12 S		8 S	1 ó 2 S	3 S

Figura 3-12 Formato de frame FDDI

Preámbulo	Formado por 16 símbolos de 5 bits, establece la sincronización de reloj en el receptor.
Delimitadores Inicio y Final	Secuencia especial de bits que indica el inicio y el final de cada frame transmitido, sin importar su contenido.
Control de Frame	Define el tipo de paquete o frame (control de acceso al medio ó información) y otras funciones de control.
Direcciones Destino y Fuente	Similar al Token Ring, excepto que son de 4 o 12 símbolos de longitud.
Datos	Puede contener hasta 4500 bytes.
Frecuencia de Verificación del Frame	(Frame Check Sequence - FCS). Es una Verificación de Redundancia Cíclica (Cyclical Redundance Check - CRC)que funciona similarmente como se describe en el formato de frame Token Ring.
Campo de estado del frame	Permite a la estación fuente, determinar si la estación direccionada no existe o está apagada, si está activa pero no copió el frame, o si está activa y copió el frame.

Cableado de Fibra Optica

Las fibras ópticas transportan señales en una dirección, y para la comunicación en dos direcciones se requieren dos hilos de fibra. Las fibras ópticas difieren de los cables de cobre Cable Coaxial y Par Trenzado, en que transportan los datos como un haz de luz sobre una fibra de vidrio, en lugar de señales eléctricas.

Las ondas de luz tienen mayor ancho de banda y son inmunes a interferencias electromagnéticas y a efectos de diafonia, por lo que las fibras pueden transportar los bits a mayores velocidades. En la tabla 3-4, se muestra un resumen de las reglas de cableado de fibras ópticas para FDDI.

Tabla 3-5 Reglas para FDDI

Características FDDI	Valor
Rango de Datos máximo	100 Mbps
Estaciones máximas	500
Distancia entre estaciones	Hasta 2 Km
Máxima circunferencia del anillo	100 Km

Usos de FDDI

Las aplicaciones típicas para redes FDDI caen en tres categorías.

- Redes Backbone
- Redes Backend
- Conexiones directas de FDDI a escritorio.

Backbones basados en FDDI.-

Un Backbone es un mecanismo de conexión entre dos o más redes ó segmentos de redes. Un Backbone de Campus usualmente interconecta a altas velocidades, a redes que residen en varios edificios, en ocasiones distribuidos en grandes distancias.

Por esto un Backbone de Campus tiene requerimientos específicos, debido a su tamaño y función. La figura 3-13 muestra un Backbone FDDI.

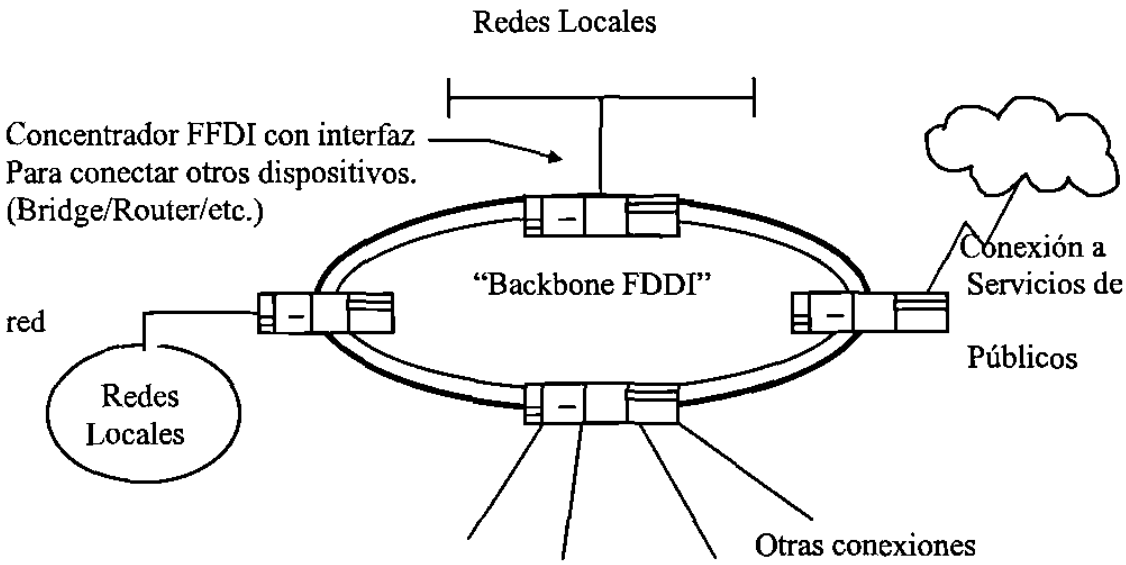


Figura 3-13 Red Backbone basada en FDDI

El Backbone de Campus es la principal carretera del tráfico de datos, necesita contar con un gran ancho de banda para transportar eficientemente grandes volúmenes de datos, también debe ser robusto y proveer características como tolerancia de fallas y redundancia. Las fallas deben ser detectadas, aisladas y reparadas rápidamente.

Al usar FDDI como un Backbone, se provee una solución completa a la demanda de una Red de Campus, en términos de distancia, el estándar FDDI especifica una longitud total del anillo de 200 km, que equivale a 100 km por anillo. El uso de la arquitectura de anillo doble, permite habilitar el mecanismo de Anillo Protegido, que aísla las fallas rápida y transparentemente.

Backends basados en FDDI.-

La motivación original para el desarrollo de FDDI fue el proveer una forma más rápida y eficiente de conectarse con Mainframes u otros Hosts. A la Arquitectura de Red que provee este tipo de conexión muy rápida para ambientes multiusuario, se le llama Backend. Muchos fabricantes están ofreciendo actualmente Mainframes de alta velocidad y otros Hosts con capacidad de conexión a FDDI, para que puedan utilizarse en Redes Backend FDDI. La figura 3-14 muestra una configuración Backend basada en FDDI.

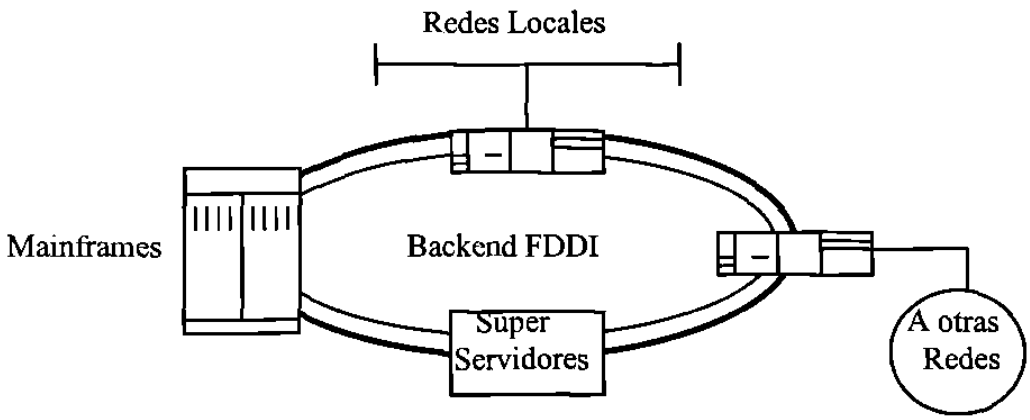


Figura 3-14. Red Backend basada en FDDI

La principal ventaja de un Backend FDDI es la Velocidad de Acceso, ya que con FDDI se aumenta enormemente el rendimiento en estos ambientes, donde los Hosts son frecuentemente mucho más accesados que los demás nodos de la red.

Conexión FDDI a estación de trabajo.-

En una configuración FDDI a estación de trabajo, todos los nodos de la Red están conectados al anillo FDDI. Para conexiones de estaciones de trabajo que requieran muy alta velocidad de acceso a la red, FDDI es la solución óptima. Sin embargo, el factor casi prohibitivo

de esta configuración es el elevado costo por conexión; desde el cableado de fibra óptica por todo el edificio hacia cada estación de trabajo y el costo de los adaptadores FDDI.

Debido a este factor, recientemente se desarrollo de una tecnología que trabaje con el estándar FDDI pero sobre cables de cobre, este estándar se le conoce como Interfaz de Distribución de Datos por Cobre (Copper Data Distributed Interface - CDDI).

En la figura 3-15, todos los nodos están conectados a ambos anillos FDDI, esto ilustra una de las formas posibles de implementar una conexión FDDI a estación de trabajo.

En la figura 3-16, se muestra la topología llamada "Anillo de Arboles" (ring of trees), que es la configuración de Estaciones de Trabajo más común en una Red FDDI.

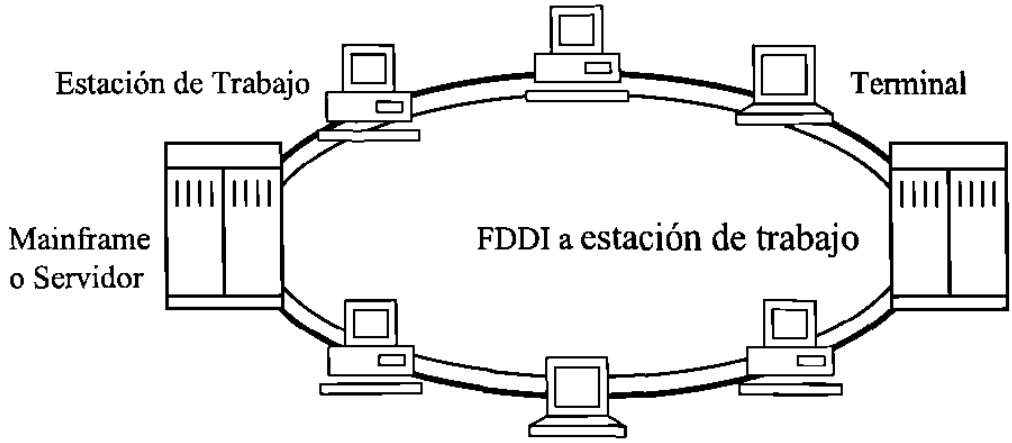


Figura 3-15 Conexión FDDI a estación de trabajo

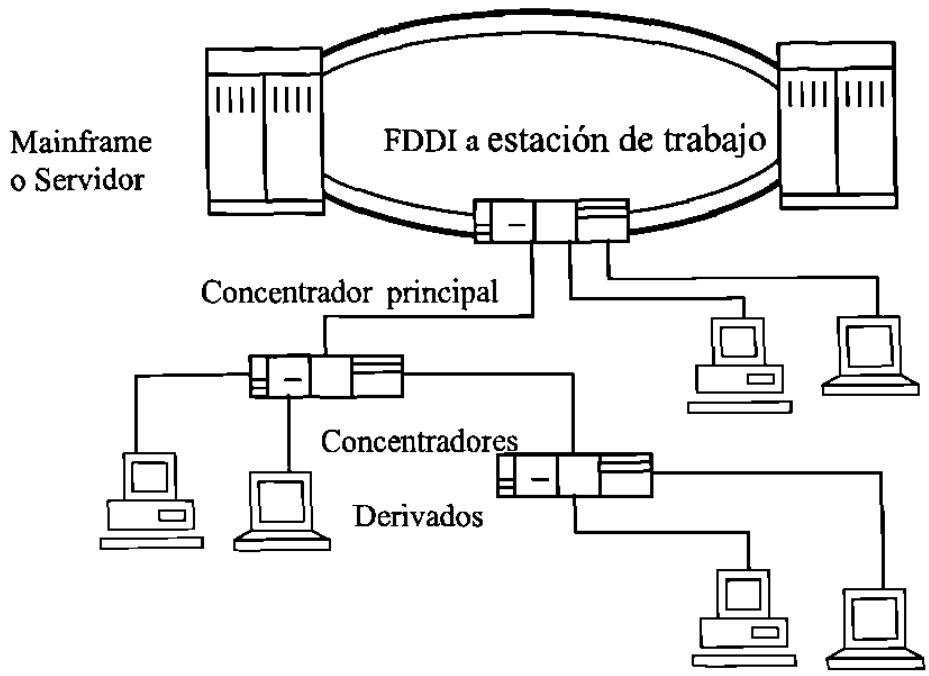


Figura 3-16. FDDI a estación de trabajo, topología Anillo de Arboles.

En esta topología los concentradores están conectados al Anillo troncal, las estaciones de trabajo y otros concetradores se derivan del concentrador principal. Las estaciones de trabajo sólo están conectadas al Anillo Primario, el anillo secundario se mantiene a nivel "troncal" para tolerancia de fallas, si hay alguna. La topología de Anillo de árboles es la configuración FDDI más fácil de administrar.

3.6. Redes inalámbricas

En esta sección, se habla de algunos de los estándares de comunicación inalámbrica de datos en la actualidad.

Además de las 3 tecnologías más comunes de red implementadas (Ethernet, Token Ring y FDDI), existen tecnologías y dispositivos de red que permiten la comunicación a través del aire en lugar de cables, en una amplia gama de frecuencias. Las redes inalámbricas ofrecen alternativas flexibles sobre los métodos tradicionales, porque el movimiento de estaciones ó el crecimiento de las redes no requiere modificaciones o recableados. Existen tres tipos básicos de redes inalámbricas, que se dividen de acuerdo a las frecuencias de transmisión.

Microondas	Esta forma de transmisión es actualmente la más común, se extiende hasta 200 pies, pero requiere un camino libre de obstáculos. Además, es necesario ajustarse a una serie de reglas de las Secretarías de Comunicaciones en cada país, para obtener el permiso de utilización de determinadas frecuencias.
UHF	La transmisión por UHF no requiere de línea de vista, pero está sujeta a interferencias con señales de Televisión.
Infrarrojo	La transmisión en este rango de frecuencias está disponible en varios modos: • Línea de Vista • Reflectiva Aunque la interferencia no es un problema, la transmisión infrarroja está limitada a menos de 100 pies.

Los sistemas inalámbricos son más caros que los de cobre y los de fibra óptica, sin embargo, no son instalables en todos los lugares.

Capitulo 4

Dispositivos de Conectividad

4.1 Introducción

Para mejorar el funcionamiento de las redes locales, uniendo o segmentando, se requiren dispositivos de conectividad como el hub, puente,.

4.2 Hubs

Como todavía no hay un estándar para arquitectura de Hubs, cada fabricante implementa diferentes características para distinguirse de los competidores, por los que se ven muchas variaciones en los diseños y características. Los tipos de básicos de Hubs pueden clasificarse como sigue:

- Hubs estibables
- Hubs de medio alcance, basados en chasis
- Hubs de Alto Desempeño

Hubs stackable (estibables).-

Los Hubs estibables están destinados primariamente para pequeños grupos de trabajo. Son pequeñas unidades autocontenidas y no son expandibles. Cada Hub usualmente soporta un tipo de red particular (Ethernet, Token Ring) y tiene un número fijo de puertos. Los fabricantes han desarrollado sistemas que interconectan los Hubs estibables usando cables que funcionan como un chasis.

Hasta cuatro Hubs estiblables pueden ser enlazados para formar un repetidor lógico, cuando normalmente cuatro Hubs individuales pueden representar cuatro repetidores. El estándar Ethernet permite no más que cuatro repetidores entre dos dispositivos cualesquiera en un mismo cable. Por funcionar como un simple repetidor,

los Hubs estibables pueden conectarse a muchos segmentos sin llegar al límite de la regla de cuatro repetidores de Ethernet. Algunos fabricantes también ofrecen diferentes medios.

Las principales ventajas de los Hubs estibables son su flexibilidad, simplicidad y efectividad de costos. Es más barato aumentar puertos poniendo otro dispositivo estibable que agregar un módulo de puertos a un Hub basado en chasis.

La figura 4-1 ilustra tres Hubs estibados y enlazados con cables como chasis. Los cables conectan los Chasis de cada Hub.

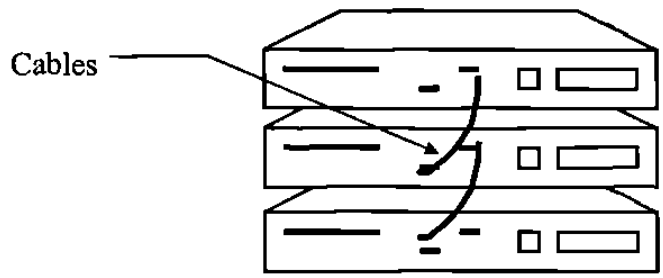


Figura 4-1 Hubs estibables con cables como chasis.

Los Hubs estibables pueden ser administrables, y son una buena elección para redes departamentales u oficinas remotas. Sin embargo, las redes más grandes que requieren conectividad sobre múltiples tipos de medio son mejores atendidas con Hubs de medio alcance basados en chasis.

Hubs de medio alcance, basados en chasis.-

Estos Hubs tienen un Chasis de bus compartido, y son llamados en ocasiones "Hubs de chasis". Aunque algunos Hubs de medio alcance soportan sólo una tecnología de red, usualmente contienen hasta 3 buses de chasis para diferentes tipos de red, su rendimiento depende del número de buses.

Los Hubs de chasis soportan módulos plug-in para administración de redes y módulos opcionales para puenteo y ruteo (puentes y routers), pero ofrecen menos slots que los Hubs de alto desempeño. Estos controlan típicamente hasta 100 puertos, son colocados en lugares donde conectan muchos grupos de trabajo o en un piso o nivel con múltiples tipos de medio. La figura 4-2 ilustra un Hub de chasis típico.

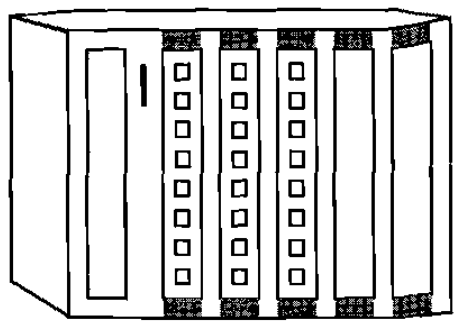


Figura 4-2 Hub de chasis

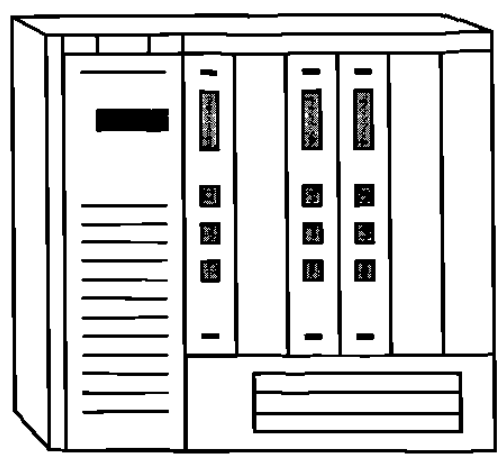
Hubs de Alto Desempeño.-

Alto Desempeño, High End, Tercera Generación; la terminología varía por el fabricante pero el concepto es el mismo. Estos Hubs agregan altos rangos de velocidades de 300 Mbps a 3 Gbps, y ofrecen un amplio rango de módulos:

- Administración de red.
- Ethernet, FDDI, Token Ring, y LocalTalk.
- Puentes y Servidores de terminales.
- Transporte de Area Local (Local Area Transport - LAT), 3270.
- Interfaces con redes de Area Amplia.

Este estado del diseño de los Hubs permite la segmentación del chasis en múltiples Redes, pueden soportar muchos cientos de puertos. Los chasis de más altas velocidades soportan conectividad a redes de área amplia, lo que permite transmisiones más rápidas y soporte de tecnologías como Frame Relay y ATM. La figura 4-3 ilustra un Hub típico de Tercera Generación.

Figura 4-3 Hub de Tercera Generación



Muchos de estos Hubs High End están moviéndose del chasis tradicional de bus compartido a un diseño de Switcheo (conmutación). Por esto en la terminología de Conectividad actual, estos Hubs muy inteligentes llevan el nombre más descriptivo de "Switches".

Los "Switches" han incorporado grandes avances en el ambiente de la conectividad, y es por ello que se ha destinado un capítulo especial para ellos más adelante, en donde se describen con detalle.

Ventajas de los Hubs

- Como los Hubs crean una topología estrella, se resuelven los problemas de cableado y se ahorra tiempo al buscar después problemas de red.

- Las tecnologías que pueden incluirse en un Hub de alto desempeño son ilimitadas, aunque esto puede parecer un problema complicado, muchos administradores de red prefieren administrar múltiples tecnologías en una sola caja, en lugar que en una red no integrada.

- Una red puede ser diseñada para que todo el tráfico fluya a través de uno ó más Hubs. Esto hace más fácil administrar el flujo del tráfico, evitando cuellos de botella y proveyendo seguridad.

- Los Hubs de switcheo de alto desempeño pueden proveer completo ancho de banda de red a cada escritorio.

Desventajas de los Hubs

- La desventaja número 1 de un Hub centralizado con topología de estrella es que es un punto de falla, como están localizados centralmente y todos los equipos se conectan a ellos, una falla en el Hub, ocasiona la caída de la red.

- Ethernet y IEEE 802.3 especifica que no pueden estar más de cuatro *repetidores regenerando una señal*. Un Hub crea automáticamente la primera regeneración, y esto puede limitar a las grandes redes. Una forma para evitar esta limitación es usar Puentes, que colocan en cero el conteo del repetidor.

4.3. Puentes.

Cuando las Redes crecen, todas las estaciones deben compartir el ancho de banda disponible. Cuando hay más estaciones en la red, el tiempo que debe esperar cada estación para poder transmitir, aumenta considerablemente. En las redes Token Ring, cuando hay muchas estaciones conectadas al anillo, el retardo que se forma a lo largo del mismo también aumenta.

El factor distancia, en cualquiera de estas redes, limita la longitud de los segmentos de red, es por eso que en las redes de grandes organizaciones, una simple red no cubre todas las necesidades, y los repetidores comunes no son suficientes para la comunicación eficaz entre varios Segmentos.

Definición de Puente

El tipo más básico de Puente, conecta dos o más redes. La interfaz entre un Puente y cada segmento de red, es conocida como Puerto, y las redes conectadas a cada Puerto, son Segmentos de red.

El Puente escucha todos los paquetes transmitidos en cada uno de los Segmentos de red conectados a él. Cuando el destino de un paquete es un dispositivo de un segmento de red diferente al que fue transmitido, el puente reenvía al paquete por el Puerto correspondiente. Al reenviar sólo los paquetes direccionados a dispositivos de otros segmentos, los Puentes incrementan el rendimiento efectivo en toda la red.

Los puentes operan en la subcapa de Control de Acceso al Medio de la Capa de Enlace de Datos OSI, esta capa organiza el flujo de bits en paquetes. A diferencia de los Repetidores, que operan en la capa Física y reenvían los bits de datos, los Puentes almacenan y envían los datos en un paquete frame. El propósito primario de la Capa de Enlace de Datos es proveer una transmisión libre de errores de información sobre el Medio físico.

Los Puentes ven la red en términos de las direcciones fuente y destino de la capa MAC, como operan en la capa de Enlace de Datos, no tienen conocimiento de los caminos entre las direcciones. Esta información de los caminos sólo está disponible en los niveles superiores, como la capa de red.

Por lo tanto, los puentes son relativamente dispositivos sencillos, esta simplicidad tiene ciertas ventajas, como que es completamente transparentes a los protocolos de alto nivel. Ellos pueden conectar protocolos de alto nivel incompatible como DECnet, TCP/IP o XNS. Esto no significa que una red DECnet pueda recibir un paquete codificado TCP/IP, en tal caso, el paquete TCP/IP podría atravesar una porción de red DECnet en su camino hacia otro segmento TCP/IP que incluye el dispositivo a donde fue direccionado.

Hay dos tipos Básicos de algoritmos de Puenteo.

- Puenteo Transparente
- Puenteo de Ruteo Fuente

Puenteo Transparente

Los Puentes transparentes están diseñados para permitir que los paquetes vayan y regresen entre dos segmentos de red corriendo el mismo protocolo de capa MAC. El Puenteo transparente típicamente conecta redes Ethernet, sin embargo también puede ser usado con redes Token Ring. Este tipo de Puenteo se llama "transparente" porque las terminales no perciben la existencia de estos Puentes.

Los puentes transparentes actuales, tienen tres funciones.

1. Aprendizaje
2. Filtrado
3. Reenvío

Aprendiendo, Filtrando y Reenviando.-

Uno de los propósitos primarios de los puentes, es evitar que el tráfico local de un segmento de red, se desborde o inunde a otros segmentos.

La figura 4-4 muestra como un puente reenvía los paquetes a las estaciones en otros segmentos e ignora a los paquetes del mismo segmento. Para realizar esta operación, los Puentes utilizan la dirección destino para construir una base de datos de las direcciones de la red, ésta contiene una tabla de ruteo que asocia a los dispositivos con los segmentos de red; todas las funciones básicas de los puentes, implican transacciones con esta base dc datos.

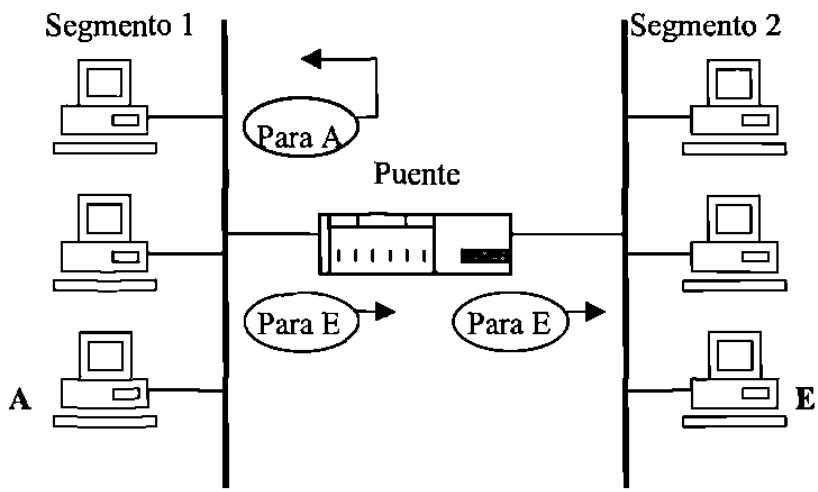


Figura 4-4 Filtrado y reenvío de paquetes.

Cuando un puente recibe un paquete, determina la dirección fuente del paquete y la compara con las direcciones de la base de datos. Si la dirección fuente no está en la base de datos, el Puente la da de alta, de esta forma "aprende" las direcciones de los dispositivos de la red. Por esta capacidad de aprendizaje, pueden agregarse nuevos dispositivos a la red, sin tener que reconfigurarse.

El puente compara entonces la dirección destino con su base de datos, que consiste de una lista de direcciones Ethernet que pueden ser alcanzadas a través de cada puerto. Si la dirección destino está en el mismo segmento que la dirección fuente, el puente filtra el paquete, descartándolo del reenvío. Este proceso ayuda a prevenir a toda la red, de ocuparse con tráfico innecesario. Una base de datos de direcciones es construida para cada puerto, como se muestra en la figura 4-5.

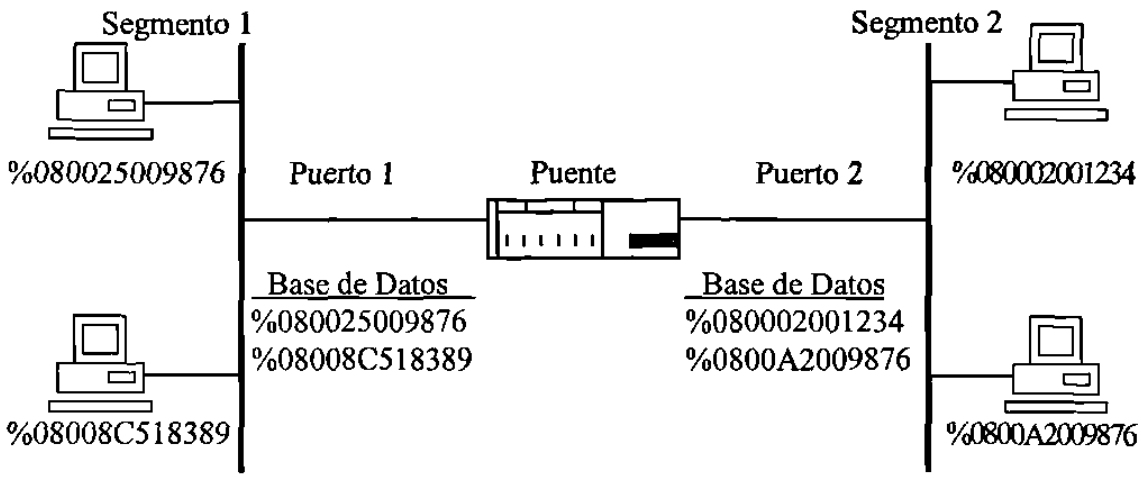


Figura 4-5. Construcción de una base de datos para un puente

Si la dirección destino está en la base de datos, el puente determina cuál de sus puertos está asociado con la dirección y reenvía el paquete al puerto apropiado. Si la dirección destino no está en la base de datos, se reenvía el paquete a todos los puertos, excepto dónde se recibió el paquete. El reenvío asegura que el paquete toma el siguiente paso correcto para llegar a su destino.

Las figuras 4-6 y 4-7 ilustran los procesos de aprendizaje, filtrado y reenvío. Asumamos que las estaciones A y B son dispositivos nuevos en el segmento.

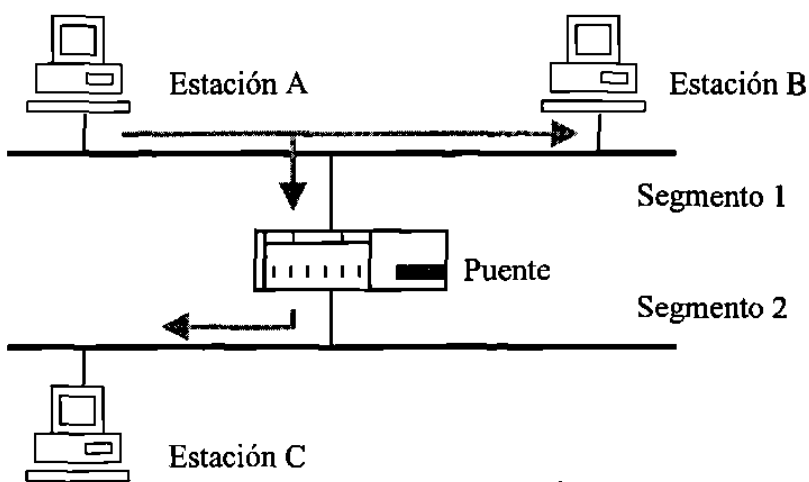


Figura 4-6. Aprendizaje y reenvío

La primera vez que la estación A transmite un paquete a la estación B, el puente determina que la dirección de red de la estación A no está en la base de datos, así que el Puente agrega esta dirección en el segmento1.

Como el Puente no conoce todavía que la estación B está también en el segmento 1, reenvía el paquete al segmento de red 2. Cuando la estación B responde en la figura 4-7, el Puente determina que la dirección de red de la estación A no está en la Base de Datos, así que la agrega para segmento1.

Luego el puente realiza una comparación con su base de datos y determina que la estación destino (A), está en el mismo segmento, entonces ya no se reenvía la respuesta de la estación B hacia el segmento 2. Cuando cualquier estación A o B transmiten un paquete a la estación C, el puente determina que la estación C está en el segmento 2 y reenvía el paquete hacia allá.

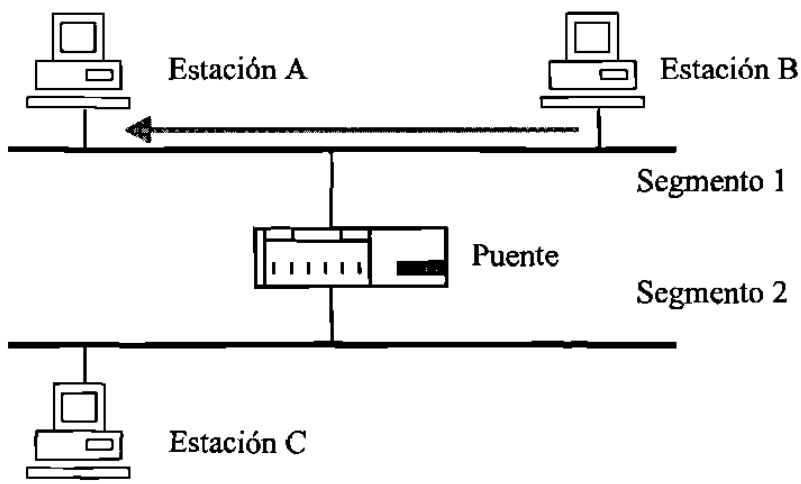


Figura 4-7. Filtrado

Los puentes transparentes no permiten reenviar paquetes conteniendo errores. Ellos verifican con rutinas "Checksum", pero no efectúan correcciones; si se detecta un error, se descarta el paquete.

Estas funciones del puente, confían en que sólo existe un camino entre dos dispositivos cualesquiera de la red. En las topologías simples, es muy fácil garantizar

que sólo existe un camino entre dos dispositivos. Pero cuando el número de conexiones se incrementa, es más probable tener múltiples caminos o lazos cerrados dentro de la red, estos lazos cerrados se llaman "loops activos", los cuáles son un gran problema porque ocasionan la duplicación innecesaria de paquetes. El tráfico redundante degrada el desempeño de la red.

La figura 4-8 muestra una topología conteniendo un loop activos. Cada vez que la estación A manda un paquete a la estación B, cada puente reenvía un paquete separado, resultando que dos paquetes idénticos atraviesen a la red.

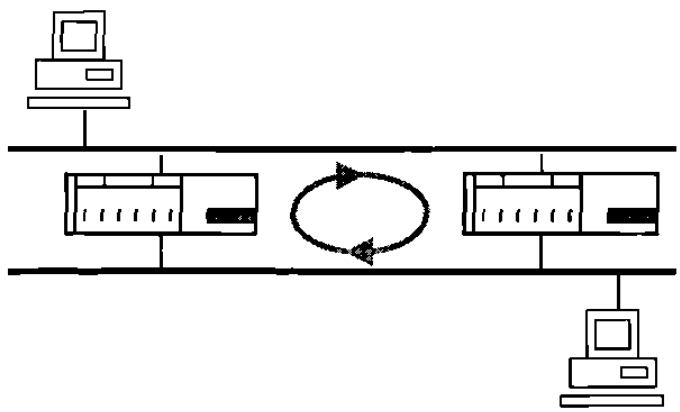


Figura 4-8. Loops activos en una red puenteada.

El problema de los loops activos en una red puenteada ha sido reconocido por IEEE. Que ha elaborado una solución para los loops activos, conocida como Algoritmo de Arbol Expandido (Spanning Tree Algorithm - STA), el cuál ha llegado a ser una parte básica de la funcionalidad de los puentes.

Algoritmo de Arbol Expandido (STA).-

Un árbol expandido crea un conjunto de caminos a través de la red, dejando uno y sólo un camino entre dos dispositivos. El algoritmo STA construye un árbol expandido a través de una serie de negociaciones puente a puente, los cuáles determinan qué caminos están habilitados para transmitir y cuáles están temporalmente deshabilitados. Como resultado de estas negociaciones, un puerto de cada puente en el

árbol es colocado en estado reenvío. Todos los demás son colocados en estado bloqueado.

En otras palabras, el algoritmo de árbol expandido crea una topología de red lógica, libre de loops, al no usar ciertos caminos (bloqueando todos los caminos redundantes). En este algoritmo, si por alguna razón el único camino falla, los puentes pueden reactivar los puertos bloqueados, para crear un nuevo Arbol.

Puenteo de Ruteo Fuente

Mientras que el ruteo transparente puede implementarse en redes Ethernet/802.3, Token Ring y FDDI, el Puenteo de Ruteo Fuente, solamente se puede implementar en redes Token Ring y FDDI. Este tipo de ruteo fue desarrollado por IBM como parte de la tecnología de red Token Ring, y rápidamente llegó a ser un estándar de fábrica para él puenteo en la capa MAC.

El puenteo de Ruteo Fuente es un método que permite a una estación ó nodo en un anillo, comunicarse con otras estaciones en otro anillo diferente, (dentro del mismo anillo, no es necesario) interconectados por puentes. La estación fuente de un anillo es responsable de determinar dinámicamente y de mantener la información sobre la ruta hacia la estación destino en otro anillo. Una ruta es el camino que un paquete debe tomar a través de múltiples anillos en redes Token Ring, desde la estación fuente hasta la estación destino. En un ambiente de múltiples anillos, las estaciones en diferentes anillos necesitan información de ruteo adicional, antes de poder comunicarse con las demás.

Una estación fuente en un anillo debe determinar primero si existe una ó más rutas hacia otra estación en un anillo remoto, para esto desempeña un proceso de determinación de la ruta insertando instrucciones dentro de un paquete y enviándolo a través de la red multianillo. Los puentes de Ruteo Fuente reenvían este paquete "descubridor" de acuerdo a las instrucciones contenidas en el paquete; y de la misma manera, le reenvían cualquier respuesta desde la estación destino en otro anillo.

Una vez que recibe la respuesta, la estación fuente actualiza su propia tabla de ruteo con la información de ruteo obtenida por su paquete, y una vez determinada la ruta

adecuada, incluirá esta información en todos los paquetes transmitidos. La figura 4-9 ilustra la tabla de ruteo para la estación A.

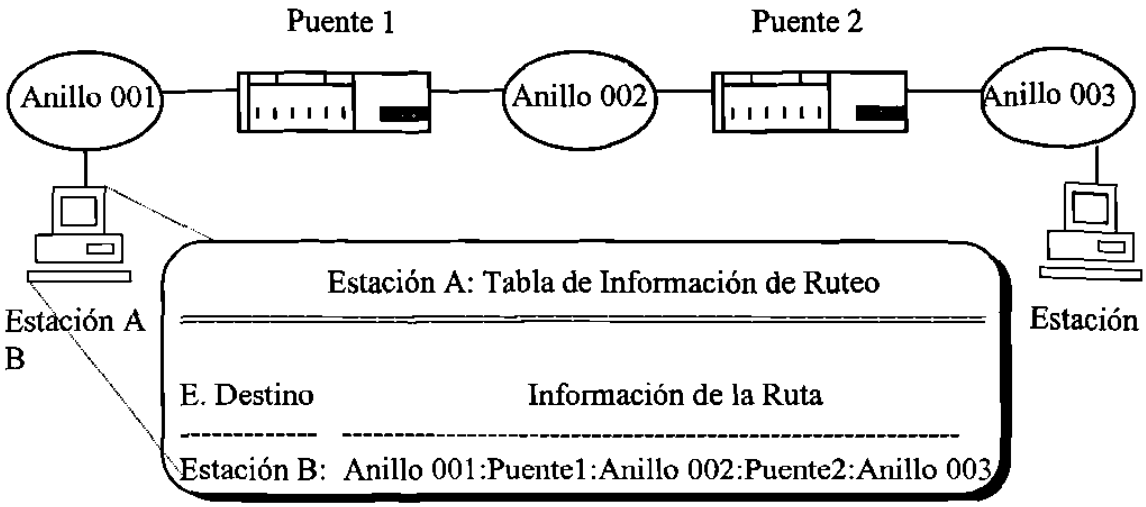


Figura 4-9 Tabla de Ruteo usando Puente de Ruteo Fuente.

Los puentes de Ruteo Fuente pueden conectar anillos operando a diferentes velocidades, y en anillos adyacentes se pueden conectar puentes de Ruteo Fuente paralelos, para tolerar posibles fallas.

Comparación entre el Puenteo Transparente y Puente de Ruteo Fuente

Él puenteo transparente lee las direcciones MAC del paquete para determinar si será reenviado a otros segmentos, cuando desempeña esta función, inspecciona la base de datos de su tabla de ruteo, para determinar en cuál segmento está la estación; Se llama transparente porque la estación fuente transmite un paquete a la estación destino como sí fuera del mismo segmento físico de red.

En contraste a la base de datos centralizada del puenteo Transparente, el puenteo de Ruteo Fuente distribuye el método de mantener la información de ruteo, proporcionando un gran control individual sobre las decisiones de ruteo de cada estación. Todas las estaciones del anillo construyen y mantienen sus propias tablas de ruteo. Cuando se escoge entre los dos tipos de puento, deben considerarse algunos aspectos, como los siguientes:

El algoritmo de ruteo fuente manda paquetes descubridores para determinar la mejor ruta hacia el destino, este tipo de paquetes genera una copia en cada camino de la red, y pueden incrementarse exponencialmente.

- El ruteo fuente requiere que todas las redes tengan asignado un número, todos los puentes deben configurarse con el número de red en cada puerto y con el número de Puente en cada par de Red que conecten. Algún error en la configuración puede causar serios problemas en la red. El ruteo transparente no requiere ninguna configuración previa, excepto para ajustar parámetros de desempeño.

- Sin embargo, el ruteo fuente provee múltiples caminos hacia un destino. Debido al algoritmo de Arbol Expandido STA, el puenteo transparente no puede usar enlaces redundantes, a menos que se activen en caso de una falla.

Existe otro algoritmo que ofrece conectividad tanto al puenteo transparente como al puente de ruteo fuente, llamado puenteo transparente de ruteo fuente, ideal para el caso de empresas que tiene los dos tipos de puenteo.

Características de los puentes

Los puentes juegan un papel importante en la administración de los recursos de redes muy complejas. Como ellos reciben todo el tráfico de cada segmento conectado, puede decirse que son "observadores privilegiados". Las características avanzadas que algunos puentes ofrecen incluyen:

Seguridad.-

Los puentes pueden aislar a dispositivos individuales ó segmentos de red de paquetes con ciertas direcciones fuente y destino, ó de algunos tipos de paquetes en particular.

Los puentes pueden implementar cualquiera de cuatro tipos de seguridad:

1. Reenvío explícito de fuente. Este tipo de seguridad, reenvía sólo los paquetes recibidos de una dirección fuente en especial, mientras que todos los demás paquetes son descartados.

2. Bloqueo explícito de fuente. Bloquea todos los paquetes recibidos de una dirección fuente específica, mientras reenvía todos los demás

3. Reenvío explícito de destino. Reenvía los paquetes hacia una dirección destino específica, mientras que bloquea a todas las demás.

4. Bloqueo explícito de destino bloquea todos los paquetes enviados hacia una dirección destino específica, mientras reenvía hacia todas las demás.

Filtrado personalizado.-

Esta característica filtra el tráfico, basándose en los protocolos, en las direcciones fuente y destino, y en el tipo, longitud ó contenido del paquete. Los filtros permiten particionar la red para incrementar la eficiencia ó restringir las requisiciones de servicios específicos. Por ejemplo, se puede especificar quién o qué recursos pueden accesar a un segmento de red ó el Backbone, o permitir el paso sólo a paquetes tipo IPX hacia un segmento dado.

Compresión de datos.-

La compresión de datos reduce el tamaño de los mensajes, convirtiendo los datos a un formato diferente y con menos bits que el mensaje original, como hay menos bit que transmitir, el tiempo de transmisión del mensaje se reduce. Las técnicas de compresión de datos ofrecen altos rendimiento en enlaces de red de área amplia, tiempos de respuesta rápidos para los usuarios y un mejor uso de las líneas de baja velocidad.

Técnicas de marcación en demanda.-

En los enlaces red de área amplia no privados, se utilizan estás técnicas cuando los datos están esperando a ser transmitidos; lo que ahorra el costo en enlaces de larga distancia, al utilizarlo sólo cuando se necesita. Aunque la conexión física esté activa o no, las estaciones creen que está permanentemente activa.

Ventajas

Dentro de las ventajas más importantes que ofrecen los puentes, pueden mencionarse las siguientes:

- Los puentes son fáciles de instalar y utilizan características avanzadas de puenteo como filtros personalizados; necesitan una configuración mínima, y se hace mediante una interfaz muy fácil de usar.

- La presencia de un Puente es transparente a los usuarios desde el instante de su instalación, y se adaptan automáticamente a los cambios de la red.

- Los puentes pueden conectar redes que corran diferentes protocolos de alto nivel sin requerir software adicional. Operan debajo de la Capa de Red OSI, por lo que no es necesario conocer sobre los protocolos que están corriendo, para configurar el puente. Algunos protocolos no ruteables, como el protocolo DECLAT utilizado en comunicaciones de terminales, pueden puentearse.

Desventajas

Los puentes no pueden tomar ventajas simultáneas de los caminos redundantes de una red, no pueden dividir la carga de tráfico sobre varios segmentos de red.

En algunas ocasiones, los puentes pueden propiciar incrementos significativos en el tráfico, inundando la red; como cuando se manda un paquete con una dirección desconocida.

Los Puentes no pueden prevenir "tormentas Broadcast", una tormenta Broadcast puede ocurrir cuando ciertos protocolos Broadcast causan que los paquetes sean reenviados a todos los puertos.

Los Puentes no proveen un buen soporte para el aislamiento de fallas, ni tienen capacidades de administración distribuida, la redes pueden hacerse más difíciles de administrar cuando su tamaño y complejidad se incrementan. Además de que no son muy rápidos comparados con otros dispositivos de conectividad.

4.4. Switches.

Como se menciona en la sección "Repetidores y Hubs" en este capítulo, los Hubs inteligentes modernos, cuentan con características y funciones que los hacen una herramienta muy poderosa para la conectividad.

Un Switch (ó Hub de switcheo) puede ser usado para extender una red más allá de los límites de un Hub repetidor. Los switches ofrecen un mayor ancho de banda, mayor rendimiento y en muchos casos, posibilidades de conexión a altas velocidades. Cuando se compara con un encaminador, un Switch tiene menor costo, es más simple y más rápido; generalmente son dispositivos "plug and play", y son altamente configurables utilizando administración local ó remota.

En un backplane de Bus-Compartido, el transporte de los paquetes está basado en un algoritmo Token Passing ó en algún algoritmo de contención. En estos algoritmos, todos los paquetes deben compartir el medio (cable), y no tienen acceso inmediato al backplane.

Los datos que son sensibles a retardos, como voz, imágenes, vídeo y aplicaciones multimedia no pueden tolerar los cuellos de botella, requieren de una arquitectura que pueda recibir inmediatamente todos los paquetes que son enviados, establecer enlaces directos entre los transmisores y los receptores, tal y como lo hace el sistema telefónico. Los Switches fueron desarrollados para cubrir estas necesidades.

Actualmente, todos los Switches están basados en conexiones Ethernet, con algunos fabricantes proveyendo módulos adicionales para FDDI. El switcheo Token Ring no está siendo desarrollado actualmente, quizás por el énfasis está en el desarrollo de tecnologías de alta velocidad como ATM.

Arquitectura de switcheo

Cada fabricante implementa su propia arquitectura de switcheo (conmutación), pero pueden dividirse en dos tipos:

- Conmutación de puente Multi-puerto.
- Conmutación por Matriz.
- Conmutación de Puente Multi-puerto.-

Muchos Switches usan un bus de datos interno de alta velocidad para almacenar y reenviar paquetes de manera similar a un puente. La diferencia es que los Puentes tienen de dos a doce conexiones de segmentos de red (puertos). Un Switch está equipado con múltiples backplanes de alta velocidad que aceptan múltiples tarjetas de puertos, cada una de las cuales conectan de ocho a doce nodos. El chasis también acepta otros módulos tales como fuentes de poder, Puentes internos, unidades de administración de red, etc.

Almacenar y reenviar significa que el Switch lee el "header" (encabezado) completo del paquete para determinar su destino antes de conmutar. Aunque esto incrementa el retraso del paquete, ofrece una mayor confiabilidad que la Conmutación de Matriz, porque durante el retraso, las rutinas Checksum (detección de errores) pueden verificar los paquetes y pueden filtrarse los que tengan errores. También, son posibles las conexiones hacia medios de alta velocidad como FDDI, y la segmentación para propósitos de seguridad

La figura 4-10 muestra la arquitectura de un Switch convencional. En esta arquitectura, la segmentación se cumple al permitir a los sub-segmentos residir en las tarjetas de puertos individuales. Cada una de las cinco tarjetas de puertos contienen ocho puertos de usuarios. Todas las estaciones conectadas a una tarjeta de puertos específica pertenece al mismo sub-segmento. Los sub-segmentos (tarjetas de puertos) están combinados para crear un segmento completo, conectando cada tarjeta de puertos a uno de los backplanes del switch. Todas las tarjetas de puertos conectadas al mismo Backplane son miembros del mismo segmento físico.

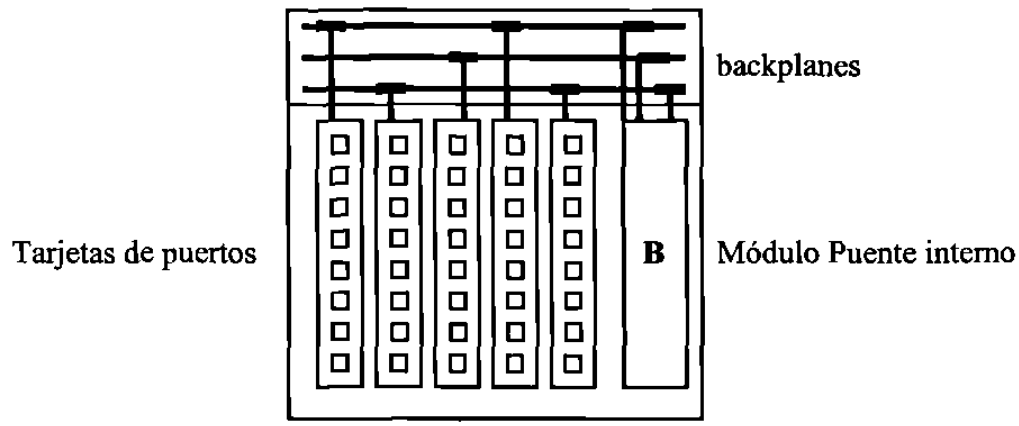


Figura 4-10 Arquitectura convencional de los switches

En la figura 4-10, las estaciones conectadas a la tarjeta de puertos 1 y a la 4, son miembros del mismo segmento físico. Las estaciones conectadas a la tarjeta de puertos 2 y a la 5 son miembros del mismo segmento. La comunicación entre estaciones conectadas a diferentes segmentos se logra utilizando un módulo interno de encaminador. Un encaminador / encaminador externo dedicado puede también proveer la conectividad entre los segmentos del backplane. Con los switches, las estaciones pueden dividirse en muchos segmentos diferentes, conectándolas a una tarjeta de puertos en particular.

Conmutación por Matriz.-

Este tipo de Switch está habilitado para conmutar paquetes a gran velocidad con muy poco retraso, en múltiples puertos simultáneamente. Este desempeño se logra al conmutar paquetes instantáneamente, después de leer sólo la dirección destino (Destination Address) Ethernet de 6 bytes. De hecho, la conmutación de matriz puede empezar a sacar los paquetes antes de que hayan entrado completamente. Esto es mucho más rápido que los puentes y encaminadores, que deben leer en encabezado completo del paquete antes de reenviarlo.

La figura 4-11 Ilustra la Conmutación por Matriz, entre Ethernet y un backbone FDDI.

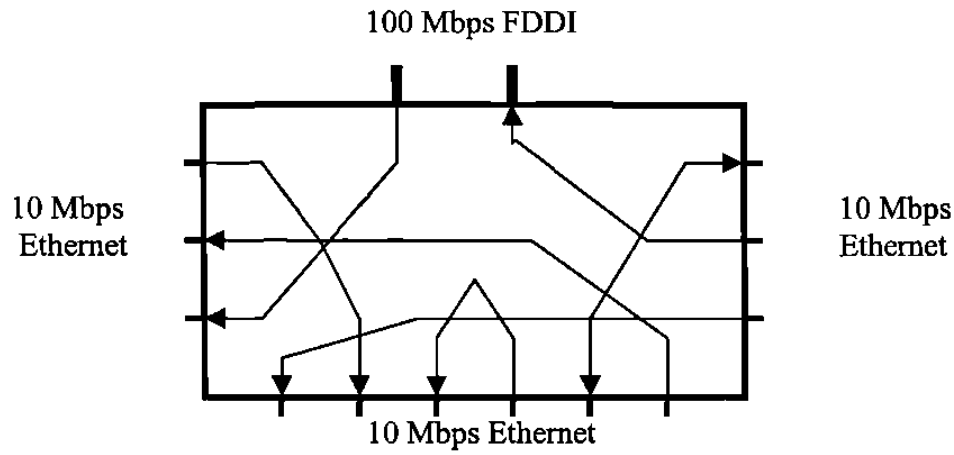


Figura 4-11 Conmutación por Matriz Ethernet

Algunos fabricantes están ofreciendo un switch de matriz full dúplex. Ethernet normalmente trabaja a Half dúplex para evitar colisiones, dos switches full dúplex pueden mandar y recibir simultáneamente, incrementando así la velocidad máxima de Ethernet a 20 Mbps, siempre y cuando exista el Switch en ambos extremos.

La principal desventaja de la conmutación de matriz es que todos sus puertos deben ser de la misma velocidad. El switch no puede conmutar de múltiples puertos Ethernet hacia puertos FDDI a alta velocidad ó ATM, para hacerlo se necesitaría recibir el header (encabezado) del paquete entero antes de transmitirlo a una velocidad mas alta, pero se perdería la ventaja de rapidez.

Características de los switches

Segmentación	En un switch se pueden conectar un gran número de segmentos de red, lo que significa que se puede dedicar un segmento para cada terminal, de manera que tenga su propio segmento de red Ethernet de 10 Mbps. Esto puede ser crítico en estaciones científicas y de ingeniería.
Interfazs con diferentes velocidades	Un switch puede comparar los requerimientos de ancho de banda de los dispositivos conectados, y así "enviarlos" los datos tan rápida ó lentamente como la terminal lo requiera.
Tolerancia a fallas	Los switches soportan el Algoritmo de Arbol Expandido para conexiones redundantes en Redes de misión crítica.
Traducción De paquetes	Los switches pueden desempeñar procesos de traducción de paquetes entre Ethernet y FDDI, permitiendo operar con el máximo tamaño de paquetes IP en FDDI para mayor eficiencia. Debido a la diferencia en la longitud de los paquetes entre Ethernet y FDDI, la reenviar paquetes IP desde FDDI a Ethernet, automáticamente se fragmentan si la longitud es mayor de 1518 bytes. Además de la traducción estándar, es posible ejecutar procesos como puenteo Apple Talk Fase II.
Filtrado	Además de las propiedades del estándar filtrado/reenvío, se pueden ejecutar en cada puerto del switch, procesos como filtrado definido por el usuario y filtrado por Grupos de Direcciones. Por ejemplo, el filtrado puede ser usado para permitir sólo algunos protocolos o aplicaciones, o para permitir/restringir la comunicación entre grupos de trabajo y/o dispositivos. El Filtrado para Grupos de Direcciones permite formar grupos de trabajo Virtuales.
Tormentas Broadcast	Los puentes tradicionales Ethernet sufren de tormentas broadcast que pueden reducir el rendimiento de una red. Sin embargo, cada puerto de un switch puede configurarse con protección contra estas tormentas, limitando el número de

	reenvíos de paquetes broadcast, permitidos en cada puerto, lo que permite la misma seguridad que un encaminador, más la funcionalidad de independencia de protocolos.
Buffer de Paquetes	Un Buffer de paquetes adecuado para paquetes evita la pérdida de datos, lo que incrementa la eficiencia de los servidores para con sus clientes; mientras mayor es la memoria del buffer, el switch es más flexible para recibir grandes flujos de bits. El buffer puede funcionar de manera estática o dinámica, un buffer Estático garantiza una cantidad de espacio fijo por puerto, sin importar qué tan llenos estén los otros puertos. En el buffer Dinámico, el espacio se asigna de acuerdo a las necesidades, lo que ayuda a descongestionar a los puertos muy ocupados. Los switches modernos soportan una combinación de buffers de paquetes dinámico y estático, con 1 Mb. De memoria.
Desempeño	Los mejores switches actuales, construidos mediante un chip ISE (Intelligent Switching Engine), tienen la capacidad de switchar en rangos de arriba de los 562,000 paquetes por segundo, ya que la comunicación puede ocurrir entre múltiples segmentos simultáneamente. Además, cuentan con tiempos de Retraso alrededor de 15 μseg. (El retraso es una característica conocida como "Latency" en inglés, definida como el tiempo que un paquete se retrasa dentro de un dispositivo, antes de ser reenviado; 'tardanza")

Todas estas características, aunadas a las facilidades de Administración local y remota, dentro y fuera de banda (desde la red ó mediante un puerto RS-232), y desde una Conexión de Consola ó Conexión Telnet, hacen que los Switches sean quizás, la mejor y más veloz herramienta actual de conectividad, debido a que entre switches, pueden usarse protocolos de interconexión de alta velocidad (como FDDI ó ATM), porque no sufren de cuellos de botella.

Capitulo 5

Conectividad en Redes de Cobertura Amplia

5.1 Introducción

Al igual que los puentes, los encaminadores interconectan dos o más segmentos de red, solo que éstos mantienen la identidad lógica de cada segmento. Por lo tanto, una inter red basada en encaminadores consiste de muchas sub redes lógicas, cada una de las cuáles es potencialmente un "dominio" independiente. A diferencia de los puentes que leen la dirección física del dispositivo, los encaminadores reenvían el tráfico basados en el número de red destino indicado en el paquete.

5.2 Encaminadores

Los encaminadores no solo se basan en las direcciones fuente y destino, sino también en los caminos que cada paquete toma a través de la red. Como operan en la Capa de Red del Modelo de Referencia OSI, y cada protocolo de alto nivel utiliza un esquema diferente para identificar los números de red, los encaminadores son dispositivos dependientes de los protocolos. También, ellos pueden conectar diferentes tipos de redes, como Token Ring con Ethernet, porque pueden tener interfazs de cada tipo de red.

Funcionalidad de los Encaminadores

Los encaminadores son dispositivos visibles a las estaciones, esto les permite controlar el flujo de tráfico de una estación transmisora a una estación receptora, si una estación transmite paquetes más rápido de lo que otra puede recibir, el encaminador puede guardar los datos en su buffer, y señalarle a la estación que pare o disminuya su transmisión.

La función básica de un encaminador en el reenviar paquetes entre las redes en donde hay usualmente más de un camino entre ellas, así que el trabajo del encaminador es encontrar el mejor camino por el cuál enviar los paquetes. Mientras que un puente examina todos los paquetes que pasan por los segmentos en donde está conectado, un encaminador recibe solo los paquetes direccionados a él, ya sea por una estación ó por otro encaminador; esto significa que tiene que hacer más decisiones que los puentes y necesita más información. Esta información adicional, que puede incluir datos relacionados al costo de transmisión del paquete, que está contenida en la Base de Datos del encaminador.

Esta base de datos es diferente de la que tienen los puentes, y se le conoce como tabla de ruteo. La principal diferencia es que la tabla de ruteo incluye información sobre los caminos que puede tomar un paquete desde su origen hasta su destino.

5.3 Tablas de ruteo

Las tablas de ruteo pueden ser creadas estática ó dinámicamente. Un encaminador primero establece un conjunto inicial de rutas, información que puede ser obtenida leyendo una tabla de ruteo inicial desde un disquete en el arranque, la información para esta tabla es suministrada por el administrador de la red y puede incluir información sobre las redes conectadas y algunas posibles rutas hacia redes remotas. Una vez que la tabla de ruteo está en memoria residente, el encaminador debe responder a los cambios en las rutas.

Si el protocolo sólo soporta ruteo estático, entonces el administrador de la red debe construir manualmente la tabla de ruteo, elaborando entradas a la base de datos para cada segmento y para cada posible camino de la red; y cuando la topología cambia, todos los encaminadores deben actualizarse manualmente. Las tablas de ruteo incluyen información tales como el tamaño del paquete, velocidad disponible de la línea, hora del día y protocolo.

Muchos de los protocolos de alto nivel soportan ruteo dinámico, así las tablas de ruteo son construidas automáticamente por los encaminadores, el algoritmo de ruteo

dinámico responde automáticamente a la congestión de la red ó a los cambios en la topología de red. Para realizar esto, el encaminador utiliza tipos de paquetes especiales conteniendo información orientada a los caminos, los nuevos cambios son incorporados a la red automáticamente, borrando ó aumentando entradas a las tablas de ruteo.

Para crear y mantener las tablas de ruteo, un encaminador realiza broadcasts de información cuando detecta cambios en la red, ejemplos de tal información puede ser la existencia de un nuevo camino; la información de ruteo puede variar mucho, desde una simple entrada incremental, hasta la tabla completa.

Determinando el mejor camino...

Cuando un paquete alcanza un encaminador, éste examina la dirección destino de la capa de red del paquete y determina cuál es el mejor camino para enviarlo, esta determinación depende de muchos factores incluyendo:

- La Medida de distancia en uso (Medida de Ruteo)
- El algoritmo implementado por el protocolo de alto nivel que se está usando
- La arquitectura de la red ruteada

En términos sólo de distancia, el mejor camino de una red es el más corto, y para calcular la distancia los encaminadores utilizan una Medida de Ruteo "número de hops". Un hop es una transmisión encaminador a encaminador que un paquete requiere. La figura 5-1 ilustra una configuración con encaminadores y sus tablas de ruteo.

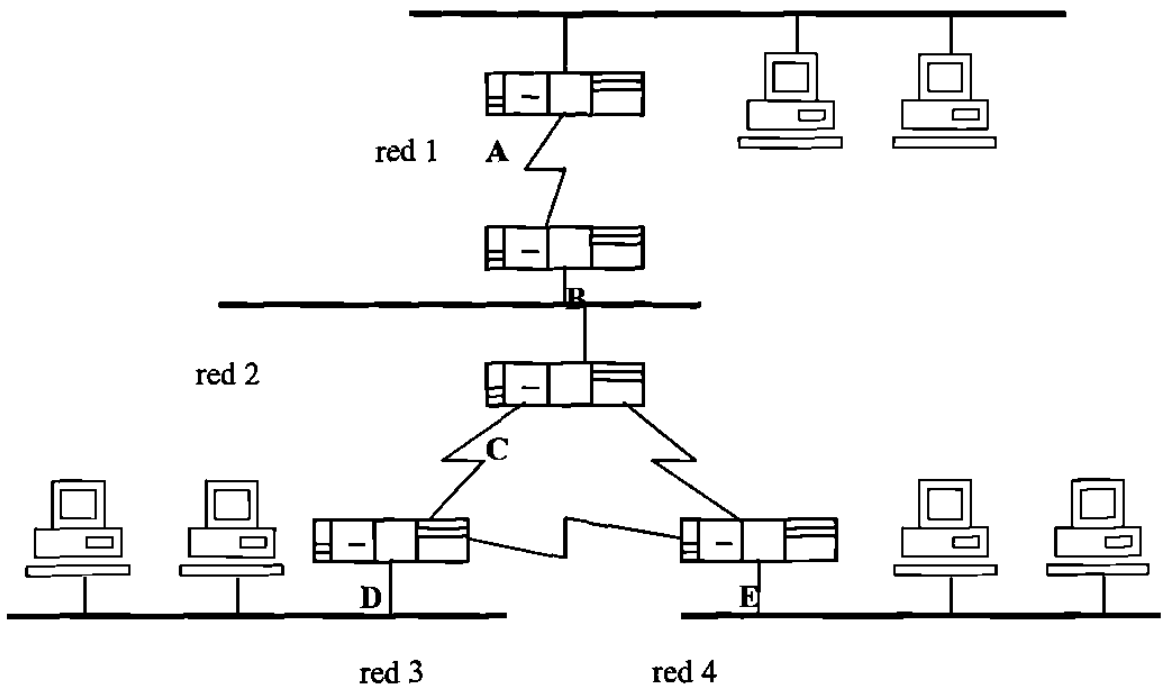


Tabla de Ruteo del encaminador A

Destino	encaminador cercano	Medida Hops
red 1	conectado	0
red 2	B	1
red 3	B	3
red 4	B	3

Tabla de Ruteo del encaminador B

Destino	encaminador cercano	Medida Hops
red 1	A	1
red 2	conectado	0
red 3	C	2
red 4	C	2

Figura 5-1 Tablas de ruteo.

Basado en las transmisiones recibidas de otros, cada **encaminador** expande su tabla de ruteo dinámicamente para incluir todas las redes que pueden ser alcanzadas a través de otros **encaminador**es. La tabla de ruteo para el **encaminador** A puede explicarse como sigue.

- Para alcanzar a la red 1 desde el encaminador A, el puerto está conectado directamente.
- Para alcanzar a la red 2 desde el encaminador A, los paquetes deben ser reenviados al encaminador B; la red 2 está a un hop de distancia.
- Para alcanzar a la red 3 desde el encaminador A, los paquetes deben ser reenviados al encaminador B; la red 3 está a tres hops de distancia.
- Para alcanzar a la red 4 desde el encaminador A, los paquetes deben ser reenviados al encaminador B; la red 4 está a tres hops de distancia.

La tabla de ruteo para el encaminador B puede explicarse como sigue.

- Para alcanzar a la red 1 desde el encaminador B, los paquetes deben ser reenviados al encaminador A; la red 1 está a un hop de distancia.
- Para alcanzar a la red 2 desde el encaminador B, el puerto está conectado.
- Para alcanzar a la red 3 desde el encaminador B, los paquetes deben ser reenviados al encaminador C; la red 3 está a dos hops de distancia.
- Para alcanzar a la red 4 desde el encaminador B, los paquetes deben ser reenviados al encaminador C; la red 4 está a dos hops de distancia.

La forma de reenviar los paquetes de un encaminador, requiere un proceso extra para calcular el origen y destino del paquete, así como el mejor camino disponible, por esto muchos protocolos implementan un algoritmo "Tiempo de vida", que consiste en destruir todos los paquetes que hayan viajado mucho tiempo ó a través de muchas rutas, para prevenir que los paquetes con errores o redundantes congestionen la red.

5.4 Algoritmos de ruteo

Existen dos tipos de algoritmos que forman las bases para el ruteo dinámico, estos son conocidos como:

- Algoritmo de Vector Distancia (Distance Vector Algorithm - DVA)
- Algoritmo de Estado de Enlace (Link State Algorithm - LSA)

La diferencia más importante entre estos dos algoritmos se refleja en la base de datos de sus tablas de ruteo. El camino más corto entre la red se determina examinando todas las rutas hacia el destino y seleccionando la que tenga la medida menor; está medida puede ser el conteo de hops, el retardo de las transmisiones, la capacidad de la línea ó alguna distancia definida administrativamente.

Algoritmo de Vector Distancia (DVA).-

Este algoritmo se basa en compartir las tablas de ruteo, todos los encaminadores realizan un Broadcast de sus tablas de ruteo y cuando reciben las de otros encaminadores, calculan las distancias de sus vecinos y actualizan sus tablas de ruteo. Los encaminador no saben nada de cómo están conectados los segmentos en la red.

Cuando ocurre un cambio, todas las reconfiguraciones se transmiten a través de la red, lo que provoca una "lenta convergencia". La convergencia se refiere al tiempo de retraso entre cuando ocurre un cambio y el tiempo que toma sincronizar la red. Una vez que todas las tablas de ruteo han sido actualizadas y todos los encaminadores están en línea, la reconfiguración está completa; un cambio en la tabla de ruteo ocasiona un intercambio de actualizaciones y puede llevar mucho tiempo para que esta información alcance a todos los encaminadores dentro del dominio de ruteo. Las grandes redes convergen más lentamente que las pequeñas.

Algoritmo de Estado de Enlace (LSA).-

Las tablas de ruteo construidas por este algoritmo incluyen información de la distancia y de cómo están enlazados ó conectados los segmentos de red. Un encaminador de estado de enlace debe conocer la topología completa de la red para computar el mejor camino hacia cada destino de la red. Cada encaminador realiza un broadcast con mensajes de actualización a todos los otros encaminadores de la red, estos mensajes contienen el estado de cada enlace conectado al encaminador, cualquier cambio en la topología es detectado por el encaminador local, y reportado en broadcast a todos los demás encaminadores en el dominio de ruteo.

El Algoritmo de Estado de Enlace LSA fue diseñado reduciendo el tiempo de proceso del Vector Distancia DVA; reduciendo el consumo de ancho de banda al reenviar sólo paquetes de actualización de estado de enlace, en lugar de las tablas de

ruteo completas. Este algoritmo puede aislar áreas del resto de la red, lo que puede reducir el tráfico que cruza el backbone. La Suite de protocolos TCP/IP originalmente usaba el protocolo de información de ruteo (RIP), que es DVA. Este tenía serias limitaciones que incluía un límite de conteo de 16 hops. Actualmente, la comunidad de Internet está interesada en un protocolo de ruteo llamado Primer Camino más Corto Abierto (Open Shortest Path First - OSPF), que es LSA.

5.5 Arquitectura de red basadas en encaminadores

Hay dos tipos de arquitectura de **encaminador**es que se usan actualmente, que son:

- Horizontal
- Jerárquica

En una red horizontal, todos los **encaminador**es están en el mismo nivel lógico, la Inter-red no se divide en áreas específicas, no hay distinción entre diferentes partes de la red, todos los segmentos de red están en la misma área.

Una red jerárquica está comprendida típicamente de dos niveles:

Los Encaminadores en el primer nivel son usados generalmente para comunicación con ciertas áreas definidas de la red (nivel 1)que pueden ser varios segmentos.

Los encaminadores de alto desempeño forman un área especial llamada Nivel 2, está área es conocida generalmente como área de backbone. Esta área se encarga de la distribución de la información sobre los cambios a la red que sólo afectan a las áreas inferiores. Por ejemplo en la Figura 5-2, los cambios en el área A (Nivel 1) sólo necesitan ser comunicados a los Encaminadores del área de backbone (Nivel 2), en lugar que a la red entera.

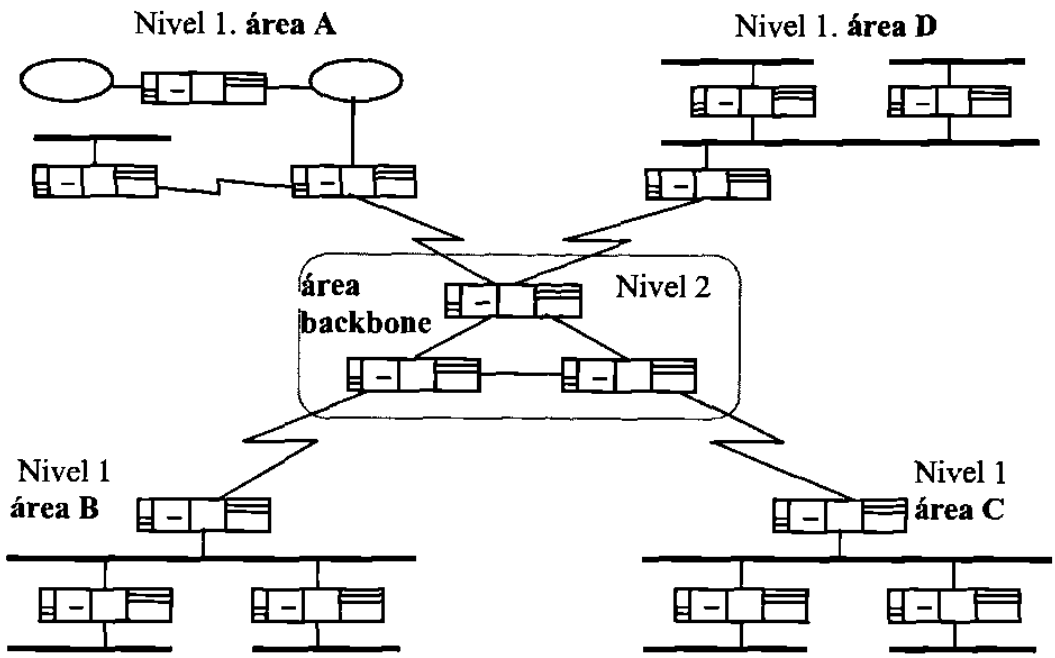


Figura 5-2. Red ruteada Jerárquica. Nivel 1 y Nivel 2.

La presencia de loops en una red horizontal, puede significar que la red tomará mucho tiempo de convergencia, ya que provoca que se creen mensajes de actualización de más y congestionar la red. Este problema se resuelve con las redes jerárquicas, porque la propagación de un mensaje sobre un cambio que sólo afecta un bloque en particular, sólo se limita a esa área.

Tanto el algoritmo Vector Distancia DVA y el de Estado de Enlace LSA, pueden implementar Arquitecturas jerárquicas; sin embargo, como las tablas de ruteo asociadas con el LSA ya incluyen datos topológicos, como la interconexión de los segmentos de red, es necesario crear tales arquitecturas. Por otro lado, la información contenida en las tablas de ruteo DVA, deben aumentarse manualmente por el administrador de la red, para formar arquitecturas jerárquicas en ambientes de protocolos basados en DVA.

5.6 Ruteo avanzado

Con respecto a los encaminadores, la funcionalidad avanzada depende primariamente de qué protocolos son soportados, y como son implementados por un fabricante en particular. Puede ser necesario un proceso extra para calcular el mejor camino disponible para el paquete hacia su destino. Si los encaminadores son configurados correctamente, pueden tener la habilidad de dividir los paquetes para el uso eficiente de la línea, y rutear diferentes protocolos sobre varios enlaces de comunicación. De una manera más detallada, el encaminador determina el mejor camino, basado en algunas funciones como:

Ruteo de Menor costo	Los administradores determinan la configuración apropiada para que el encaminador escoja siempre el camino de menor costo que un paquete deba tomar, los factores para determinar este costo pueden incluir el ancho de banda y el retardo de la línea, así como costos puramente económicos.
División de la carga	Los encaminadores utilizan en forma efectiva los caminos redundantes a través de la red; la división de carga les permite mandar todos los paquetes de una determinada transacción, sobre varios caminos simultáneamente. Si hay más de una mejor ruta, un administrador de red puede decidir dividir la carga entre rutas de igual costo, para mejorar el rendimiento de la red. La división de la carga depende del protocolo.
Ruteo de Clase de Servicio	Este tipo de ruteo es similar al puenteo Clase de Servicio, que permite especificar varias categorías de servicios de ruteo, y asociar varias características de desempeño con cada categoría. Se pueden asignar paquetes a diferentes filas de prioridades y asignar un rango, de X paquetes de alta prioridad, por un paquete de baja prioridad. Típicamente los paquetes asociados con procesos interactivos, deben asignarse a una fila de alta prioridad, mientras que los procesos en background pueden asignarse a las filas de baja prioridad.

Ruteo Tipo de Servicio	Este tipo de ruteo permite especificar hasta 16 clases de servicio y establecer caminos separados para cada clase. Estas clases pueden incluir velocidad y retraso de la línea. Las conexiones de larga distancia tienen prioridad para utilizar las líneas más veloces, para asegurar la transmisión más rápida posible.
Ruteo basado en Políticas	Este tipo de ruteo permite a los administradores especificar fuentes adicionales de información para la Tabla de Ruteo y el Modelo de Red, esta información puede controlar la comunicación encaminador a encaminador, las políticas pueden definir quién le habla a quién, quién escucha a quién, y qué tipos de información pueden transmitirse ó recibirse. Estos tipos de ruteo ofrecen seguridad, y son dependientes de los protocolos soportados.

Como los encaminadores aíslan lógicamente los segmentos de red, permiten la implementación de firewalls. "Firewall" es una barrera lógica que aísla y protege a los segmentos, de congestiones, tormentas broadcast, ó cualesquier otro incidente de ruteo. Los encaminadores crean estas barreras (firewalls) para las redes locales, porque sólo les reenvían los paquetes que están direccionados específicamente a ellas.

Es importante señalar, que en el capítulo 2 se analizaron los protocolos más comunes de la Capa de Enlace de Datos, Ethernet, Token Ring y FDDI. Y aunque los encaminadores utilizan estos protocolos para Accesar al Medio y transmitir datos; para comunicarse con los demás Encaminadores, utilizan otros protocolos que operan en la Capa de Red, estos protocolos son llamados protocolos de ruteo, y contienen información relacionada a la comunicación entre encaminadores.

5.7 Puente/ Encaminador ó Brouter

Algunos fabricantes han creado dispositivos que mezclan las tecnologías de puenteo y ruteo en un sólo sistema, algunos les llaman brouters y otro puente/ encaminador. En realidad, son sistemas que proveen una acción simultánea de operación, rutean paquetes de diferentes protocolos, y los protocolos no ruteables (como DEC LAT y NetBIOS), son reenviados como un puente.

Ventajas de los encaminadores

- Eliminan tráfico en una red porque no reenvían paquetes broadcast de un segmento a otro.
- Generalmente son más flexibles que los puentes, pueden diferenciar entre varios caminos, basados en diferentes factores, como costos, características de las líneas, etc.
- Proveen una efectiva protección entre sub-redes, aislando los segmentos con barreras firewalls, para controlar la congestión de tráfico individual de cada segmento.
- Soportan cualquier topología y se acomodan fácilmente a redes de gran tamaño y complejidad.
- Los encaminador toman ventaja de los caminos redundantes de la red, ya que pueden dividir la carga de tráfico a través de esos caminos redundantes.
- Pueden traducir paquetes de un protocolo a otro, de la capa de Enlace de Datos (de Ethernet a Token Ring), más fácilmente que los Puentes.

Desventajas de los encaminadores

- Como los encaminadores son dispositivos dependientes de protocolos, requieren un software para cada protocolo que corran.
- Cuando un encaminador soporta más protocolos, deben haber Administradores mucho más experimentados, para configurarlos ó darles soporte.
- Si se corre un Protocolo de Ruteo Estático, la configuración puede ser un proceso muy laborioso y tardado.
- Algunos de los protocolos que operan debajo de la Capa de Red, no son ruteables, así que sólo pueden ser reenviados por un Puente.
- Cuando las redes son muy grandes, la resincronización de los Encaminadores consume mucho tiempo después de un cambio, además de que se aumenta el tráfico de la red cuando intercambian mensajes de actualización.

Capitulo 6

Conclusiones y Recomendaciones

6.1 Conclusiones

El desarrollo de este trabajo tuvo su origen en la necesidad de mejorar la formación de recursos humanos con conocimientos de conectividad, de redes de computadora y la administración de las mismas.

Nuestra facultad cuenta con una infraestructura de conectividad basada en un backbone de fibra óptica, dispositivos de conectividad tales como ruteadores, puentes, repetidores, switches, etc. Además con un laboratorio de conectividad en donde es factible la experimentación con redes de computadora con protocolos de comunicación y con sistemas operativos de red.

Este trabajo contribuye en buena parte a facilitar la tarea de los administradores de redes y a los maestros y estudiantes de comunicaciones ya que trata los estándares de las redes locales, las diferentes topología existentes, los protocolos y los dispositivos de conectividad tanto para redes locales como para redes de cobertura amplia.

6.2 Recomendaciones

El campo de las redes de computadoras es demasiado amplio. Este trabajo se limita al estudio de las redes locales y sus dispositivos de conectividad, también se incluyo el tema de ruteadores como dispositivo que puede emplearse tanto en redes locales como en redes de cobertura amplia.

Considero que este trabajo puede extenderse hacia los siguientes tópicos:

- Protocolo TCP/IP
- Redes de alta Velocidad
- Simulación de redes de computadora

Bibliografia

- Stallings, William
  Data and Computers Communications
  Prentice Hall, 1997

- Stallings, William
  Handbook of Computer-Communications Vol.1,2,Y 3
  Macmillan Books, 1990

- Stallings, William
  Local and Metropolitan Area Networks
  Macmillan Books, 1993

- Tanden Baun, Andrew S.
  Redes de Ordenadores
  Prentice Hall, 1997

Listado de Tablas

Listado de Figuras

Glosario

CSMA/CD	Acceso Múltiple percibiendo portadoras, con detección de colisiones
FDDI	Interfaz de Distribución de Datos por Fibra
Gateway	Dispositivo para conectar redes con diferentes protocolos
Hub	Dispositivo de conexión con administración
IEEE	Instituto de Ingenieros en electricidad y Electrónica
LAN	Red de área local
LLC	Capa de Control de Enlace Lógico
MAC	Capa de control de Acceso al Medio
MAU	Unidades de Acceso Multiestación o (unidad de conexión al Medio)
NIC	Tarjeta de Interfaz de red
NOS	Sistema operativo de red
OSI	Suite de protocolos de Interconexión de sistemas abiertos
Puente	Dispositivo que une redes del mismo protocolo
Repetidor	Dispositivo de conexión (Reenvía señales)
Ruteador	Dispositivo (Encaminador) para encontrar el mejor camino
TCP/IP	Protocolo de Control de Transporte / Protocolo Internet
UTP	Cable de par Trenzado sin blindar
WAN	Red de cobertura amplia

Resumen Autobiográfico

Ciro Calderón Cárdenas nació el 3 de febrero de 1948 en Monclova Coahuila, México tiene nacionalidad Mexicana y es egresado de la Universidad Autónoma de Nuevo León de la Facultad de Ingeniería Mecánica y Eléctrica en el año de 1972, con título de Ingeniero Mecánico Electricista. Labora como catedrático de tiempo completo en la U.A.N.L. F.I.M.E., Impartiendo materias del área de comunicaciones. Su tesis es en opción al grado de Maestro en Ciencias de la Ingeniería Eléctrica con Especialidad en Electrónica. Sus Padres son Adolfo Calderón González y Catalina Cárdenas Meza. Su Esposa es Rosario Santos Santoy y sus hijos son Ciro Calderón Santos y Kelly Calderón Santos.