UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

“FUNDAMENTOS BÁSICOS DE REDES DE ÁREA LOCAL”

MONOGRAFÍA

PARA OBTENER EL TÍTULO DE

LICENCIADO EN COMPUTACIÓN

PRESENTA:

EVARISTO REYES LÓPEZ

ASESOR: M. en C. LUIS ISLAS HERNÁNDEZ

PACHUCA DE SOTO HGO. DICIEMBRE 2007.

DEDICATORIAS

A mi Mamá (qepd), a mi Papá. Hermanas y hermanos
A mi Esposa, a mi hija Wendy, a Daniel mi hijo
A DIOS gracias por la vida, por mi familia y por todo
y por tanto que hay que agradecer el ver un nuevo amanecer
al lado de nuestros seres queridos.

Justificación

En la actualidad, en los albores del siglo XXI el avance de la ciencia se torna un tanto acogedor, mientras que el desarrollo de la humanidad compite con el pensamiento del hombre. Por ello es necesario que el individuo hambriento de conocimientos se lance día tras día con un aferrado empeño a explorar los confines desconocidos.

Menester indispensable en toda labor de raciocinio ha sido y seguirá siendo un paso en el avance de nuestra cultura, sin duda alguna todos los materiales de que dispone el hombre serían insuficientes, si éstos, no fuesen ordenados de una manera lógica y sistemática.

Hoy en día el mundo nos parece demasiado complejo, sin embargo conocedores de la gran importancia que representa el uso de las computadoras, desde la más simple hasta la mas compleja, como un juego de niños lo que hace un siglo se consideraba imposible, hoy se han traspasado estas barreras y tratamos de introducirnos en lo que de hecho ya es y será una herramienta de trabajo común y corriente el uso de las redes.

Muchas compañías tienen una cantidad importante de computadoras en operación, con frecuencia alejadas entre sí. Por ejemplo una compañía con varias fábricas puede tener una computadora en cada localidad para llevar el control del inventario, vigilar la productividad y pagar la nómina local. Inicialmente cada una de estas computadoras puede haber trabajado aislada de las otras, pero en algún momento la gerencia decide conectarlas para poder extraer y correlacionar información acerca de la compañía.

En términos generales la cuestión es compartir los recursos y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos de los usuarios.

Una segunda meta es lograr una alta confiabilidad y no duplicidad de los datos, ya que aunque los archivos se encuentren en una o varias computadoras automáticamente

deberán actualizarse y si una computadora falla (algún problema de hardware) cualquier otra computadora será capaz de realizar el trabajo con las mismos archivos.

La principal causa de ésta es saber que la tecnología moderna tiene en la computación la más valiosa de las herramientas, ya no es noticioso, es tan común de que todo el orbe ha sido invadido de computadoras, y más de las llamadas compatibles. Estos recursos bien utilizados indudablemente optimizan la productividad en todos los campos de las ciencias y del quehacer cotidiano del hombre.

La misma computación en su constante y dinámica evolución, ha encontrado en las computadoras personales, una coyuntura más que ofrece mejores perspectivas al usuario, de éstas computadoras personales: LAS REDES.

Hoy en día la imperiosa necesidad de abatir costos en el manejo, transmisión e intercambio de información, ha encontrado en las REDES la respuesta positiva, ya que con ellas se comparten los recursos costosos, se actualiza y se organiza la información tanto en empresas y organismos particulares, como organismos oficiales, estatales y paraestatales, se logran enlaces remotos.

El propósito principal es proporcionar comunicación entre las computadoras, compartir recursos como impresoras de alta velocidad, capacidad de memoria masiva, acceder a bases de datos, programas de aplicación, compartir archivos, procesamiento de datos, funciones de automatización, distribución de documentos.

En universidades que requieren de la red para acceder la unidad central, conseguir un historial académico, en hospitales para la obtención de información de los pacientes, monitoreo y diagnóstico, etc.

Objetivo general

Proporcionar de manera sencilla y general de que se compone una red de área local, así como su funcionamiento para lograr un mejor y mayor entendimiento de la utilidad de las mismas, dentro de las organizaciones.

Objetivos específicos

- Dar a Conocer los elementos o componentes de una red de área local (topologías, protocolos de comunicación, tipos de cable y las diferentes arquitecturas de redes existentes, etc.)

- Ofrecer las alternativas posibles para la instalación de una red

- Identificar los componentes necesarios para tener una red que ofrezca la seguridad y confiabilidad de los datos.

Introducción

El desarrollo del hombre desde el nivel físico de su evolución, pasando por su crecimiento en las áreas sociales y científicas hasta llegar a la era moderna se ha visto apoyado por herramientas que extendieron su funcionalidad y poder como ser viviente.

Sintiéndose conciente de su habilidad creativa, metódicamente elaboró procedimientos para organizar su conocimiento, sus recursos y manipular su entorno para su comodidad, impulsando las ciencias y mejorando su nivel de vida a costa de sacrificar el desarrollo natural de su ambiente, produciendo así todos los adelantos que un gran sector de la población conoce: automóviles, aeroplanos, trasatlánticos, teléfonos, televisiones, etc.

En el transcurso de todo este desarrollo, también evolucionó dentro del sector tecnológico el cómputo electrónico. Este nació con los primeros ordenadores en la década de los años 40, porque la necesidad del momento era extender la rapidez del cerebro humano para realizar algunos cálculos aritméticos y procedimientos repetitivos.

Este esfuerzo para continuar avanzando, se reflejó en crear unidades de procesamiento cada vez más veloces, divididas en cuatro generaciones bien definidas: la primera con tubos al vacío, la segunda con transistores, la tercera con circuitos integrados y la cuarta con circuitos integrados que permitieron el uso de computadoras personales y el desarrollo de las redes de datos.

Este último elemento, las redes de ordenadores, consisten en "compartir recursos", y uno de sus objetivos principales es hacer que todos los programas, datos y hasta los propios equipos estén disponibles para cualquier usuario que así lo solicite, sin importar la localización física del recurso y del propio usuario.

Antes de la llegada de las redes, los usuarios de estaciones de trabajo necesitaban tener sus propias impresoras y otros periféricos, lo que constituía un factor caro para las grandes empresas. La revolución de las redes redujo drásticamente estos costes haciendo posible que varios usuarios compartieran hardware y software simultáneamente.

La interconexión de equipos en redes proporciona beneficios en las siguientes áreas: compartir información, compartir hardware y software, y soporte administrativo. Estos beneficios ayudan a incrementar la productividad. La capacidad de compartir información y datos rápida y económicamente es uno de los beneficios más habituales de las redes. El correo electrónico y la agenda basados en red son algunas de las actividades por las que las organizaciones utilizan actualmente las redes.

Los equipos en red también simplifican las tareas de administración y soporte. Desde una misma ubicación, el administrador de red puede realizar tareas administrativas en cualquier equipo de la red. Además, es más eficaz para el personal técnico ofrecer soporte sobre una versión de un sistema operativo o de una aplicación que tener que supervisar varios sistemas y configuraciones individuales y únicas.

Este trabajo, aborda temas acerca de las Redes de área local, con el fin de contribuir, como material de consulta, para aquellas personas que deseen adentrarse en el mundo de las redes de computadoras. Por tal motivo, primeramente de manera general abordamos algunos conceptos relacionados a las redes, posteriormente se define qué es una red desde un punto de vista informático y se muestra una breve reseña sobre la evolución de las mismas. De igual modo, se analiza la estructura de las redes, y las topologías que las caracterizan según la distribución geométrica de sus estaciones de trabajo. También se hace referencia a los protocolos que se utilizan para la configuración de estas estructuras así como los tipos de redes, sus alcances y los servicios que prestan las mismas. Finalmente aparece un glosario con algunos términos que pudieran esclarecer al consultante.

ÍNDICE

CAPÍTULO 3

MEDIOS DE TRANSMISIÓN

CAPÍTULO 4

PROTOCOLOS DE COMUNICACIÓN

CAPÍTULO 5

TECNOLOGÍAS DE REDES

CAPÍTULO 6

TARJETA DE INTERFACE DE RED

ÍNDICE DE FIGURAS

CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 Qué es una red de computadoras

Existen muchas definiciones aceptadas en la industria. Quizá la más simple sea la siguiente: “Una red de computadoras es un conjunto de computadoras conectadas entre sí mediante una vía de transmisión”. La vía de transmisión es a menudo un cable de línea telefónica o un cable coaxial debido a su comodidad y su presencia universal. O también, en su definición más simple una red es un conjunto de computadoras interconectadas entre sí a través de un medio físico para permitir la comunicación, intercambio de información y compartición de recursos.

Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos. Independientemente a esto, definir el concepto de red implica diferenciar entre el concepto de red física y red de comunicación.

Respecto a la estructura física, una red la constituyen dos o más ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento...) o sea software (aplicaciones, archivos, datos...). Desde una perspectiva más comunicativa, podemos decir que existe una red cuando se encuentran involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). En fin, una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Independientemente de la definición que se le de a una red de computadoras; éstas existen para cumplir un determinado objetivo: la transferencia e intercambio de datos entre computadoras. Este intercambio de datos es la base de muchos servicios basados en computadoras que utilizamos en nuestra vida diaria.

Una red tiene como objetivo principal compartir recursos materiales (equipos y sus periféricos) y recursos informáticos (programas, bases de datos, etc.), organizándolos, actualizándolos y explotándolos. [R9]

1.2 Breve reseña sobre la evolución de las redes

Los primeros enlaces entre ordenadores se caracterizaron por realizarse entre equipos que utilizaban idénticos sistemas operativos soportados por similar hardware y empleaban líneas de transmisión exclusivas para enlazar sólo dos elementos de la red.

En 1964 el Departamento de Defensa de los EE.UU. pide a la agencia DARPA (Defense Advanced Research Proyects Agency) la realización de investigaciones con el objetivo de lograr una red de ordenadores capaz de resistir un ataque nuclear. Para el desarrollo de esta investigación se partió de la idea de enlazar equipos ubicados en lugares geográficos distantes, utilizando como medio de transmisión la red telefónica existente en el país y una tecnología que había surgido recientemente en Europa con el nombre de Conmutación de Paquetes. Ya en 1969 surge la primera red experimental ARPANET, en 1971 esta red la integraban 15 universidades, el MIT; y la NASA; y al otro año existían 40 sitios diferentes conectados que intercambiaban mensajes entre usuarios individuales, permitían el control de un ordenador de forma remota y el envío de largos ficheros de textos o de datos. Durante 1973 ARPANET desborda las fronteras de los EE.UU. al establecer conexiones internacionales con la "University College of London" de Inglaterra y el "Royal Radar Establishment" de Noruega.

En esta etapa inicial de las redes, la velocidad de transmisión de información entre los ordenadores era lenta y sufrían frecuentes interrupciones. Ya avanzada la década del 70, DARPA, le encarga a la Universidad de Stanford la elaboración de protocolos que permitieran la transferencia de datos a mayor velocidad y entre diferentes tipos de redes de ordenadores. En este contexto es que Vinton G. Cerf, Robert E. Kahn, y un grupo de sus estudiantes desarrollan los protocolos TCP/IP.

En 1982 estos protocolos fueron adoptados como estándar para todos los ordenadores conectados a ARPANET, lo que hizo posible el surgimiento de la red universal que existe en la actualidad bajo el nombre de Internet.

En la década de 1980 esta red de redes conocida como la Internet fue creciendo y desarrollándose debido a que con el paso del tiempo cientos y miles de usuarios, fueron conectando sus ordenadores. [R1]

1.3 Estructura de las redes

Las redes tienen tres niveles de componentes: software de aplicaciones, software de red y hardware de red.

- El Software de Aplicaciones, programas que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).
- El software de Red, programas que establecen protocolos para que los ordenadores se comuniquen entre sí. Dichos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes.
- El Hardware de Red, formado por los componentes materiales que unen los ordenadores. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otros ordenadores.

En resumen, las redes están formadas por conexiones entre grupos de ordenadores y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. En estas estructuras, los diferentes ordenadores se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores.

Dichos servidores son ordenadores como las estaciones de trabajo pero con funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso a la red y a los recursos compartidos. Además de los ordenadores, los cables o la línea telefónica, existe en la red el módem para permitir la transferencia de información convirtiendo las señales digitales a analógicas y viceversa, también existen en esta estructura los llamados Hubs y Switches con la función de llevar acabo la conectividad.

1.4 Componentes básicos de una red de área local

Los componentes principales de una red son:

1.4.1 Servidor (server)

El servidor es la computadora principal de la red, es la que se encarga de administrar los recursos de la red y el flujo de la información. Existen servidores dedicados, es decir están realizando tareas específicas, por ejemplo, un servidor de impresión sólo realiza tareas de impresión, un servidor de base de datos sólo administra o sirve la base de datos. Para que una computadora sea un servidor, es necesario que ésta sea se alto rendimiento en cuanto a velocidad y procesamiento y gran capacidad de almacenamiento. Y servidores no dedicados, éstos además de administrar los recursos de la red, también funciona como estación de trabajo.

1.4.2 Estación de trabajo (Workstation)

Éstas son representadas por cada una de las computadoras que se encuentran físicamente conectadas a la red por medio de algún tipo de cable. La estación de trabajo puede ejecutar su propio sistema operativo y ya después se puede añadir al ambiente de red.

1.4.3 Tarjeta interfase

Tarjeta que va instalada dentro de cada computadora. Cada tarjeta determina la forma de conexión (topología) de cada red.

1.4.4 Sistema operativo de red

Es el sistema o programa (software) que administra y controla en forma general la red, entre ellos está, los recursos a compartir, los periféricos, la entrada/salida, los dispositivos de almacenamiento, etc.

1.4.5 Recursos a compartir

Son todos aquellos dispositivos de hardware y software que tienen un alto costo, y los más comunes son las impresoras, los plotters, unidades de almacenamiento, etc.

1.5 Elementos que definen a una red de área local

- Topología. Es la forma física mediante el cual la computadora es conectada a la red.
- Medio de transmisión. Es el medio físico (cable) utilizado para interconectar la computadora a la red.
- Protocolo de acceso. Son las normas que determinan como es la comunicación entre las computadoras y el acceso al medio para enviar y recibir información.

1.6 Alcance de las redes

El alcance de una red hace referencia a su tamaño geográfico. El tamaño de una red puede variar desde unos pocos equipos en una oficina hasta miles de equipos conectados a través de grandes distancias. Importante

El alcance de una red no hace referencia sólo al número de equipos en la red; también hace referencia a la distancia existente entre los equipos. El alcance de una red está determinado por el tamaño de la organización o la distancia entre los usuarios en la red.

El alcance determina el diseño de la red y los componentes físicos utilizados en su construcción.

Existen dos tipos generales de alcance de una red:

• Redes de área local

• Redes de área extensa

Redes de área local

Una red de área local (LAN) conecta equipos ubicados cerca unos de otros. Por ejemplo, dos equipos conectados en una oficina o dos edificios conectados mediante un cable de alta velocidad pueden considerarse una LAN. Una red corporativa que incluya varios edificios adyacentes también puede considerarse una LAN.

Redes de área extensa

Una red de área extensa (WAN) conecta varios equipos que se encuentran a gran distancia entre sí. Por ejemplo, dos o más equipos conectados en lugares opuestos del mundo pueden formar una WAN. Una WAN puede estar formada por varias LANs interconectadas. Por ejemplo, Internet es, de hecho, una WAN. [R8]

1.7 Ampliación de una red:

Para satisfacer las necesidades de red crecientes de una organización, se necesita ampliar el tamaño o mejorar el rendimiento de una red. No se puede hacer crecer la red simplemente añadiendo nuevos equipos y más cable.

Cada topología o arquitectura de red tiene sus límites. Se puede, sin embargo, instalar componentes para incrementar el tamaño de la red dentro de su entorno existente. Entre los componentes que le permiten ampliar la red se incluyen:

- **Repetidores y concentradores (hub**) Los repetidores y concentradores retransmiten una señal eléctrica recibida en un punto de conexión (puerto) a todos los puertos para mantener la integridad de la señal.

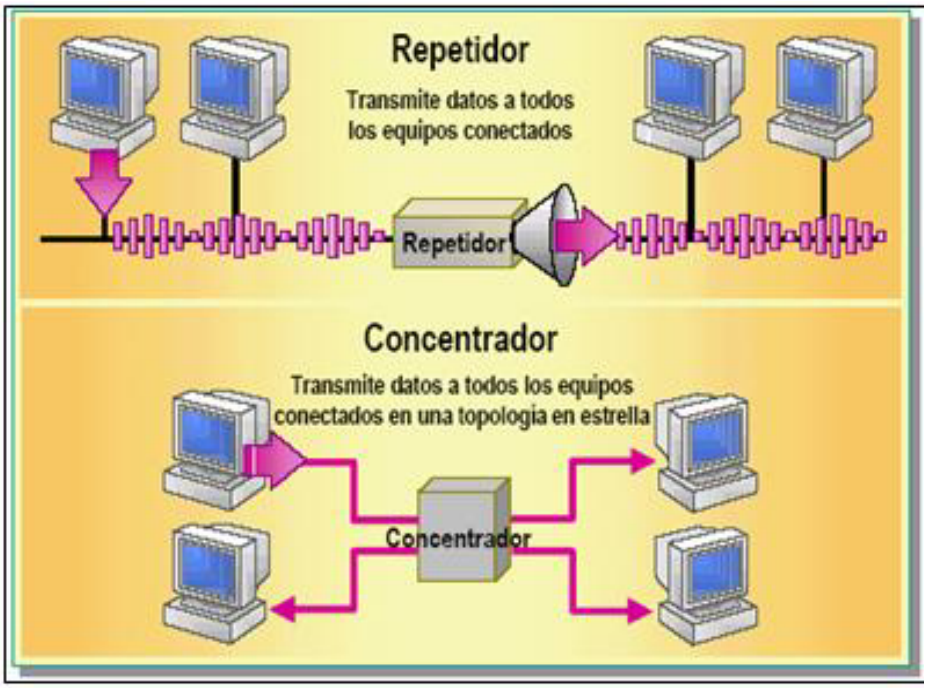

Figura 1.1 Repetidor – Concentrador

Podemos utilizar repetidores y concentradores para ampliar una red añadiendo dos o más segmentos de cableado. Estos dispositivos utilizados habitualmente son económicos y fáciles de instalar. (Vea figura 1.1)

Los repetidores reciben señales y las retransmiten a su potencia y definición originales. Esto incrementa la longitud práctica de un cable (si un cable es muy largo, la señal se debilita y puede ser irreconocible).

Instalar un repetidor entre segmentos de cable permite a las señales llegar más lejos. Los repetidores no traducen o filtran las señales. Para que funcione un repetidor, ambos segmentos conectados al repetidor deben utilizar el mismo método de acceso.

Por ejemplo, un repetidor no puede traducir un paquete Ethernet a un paquete *Token Ring*. Los repetidores no actúan como filtros para restringir el flujo del tráfico problemático. Los repetidores envían cada bit de datos desde un segmento de cable a otro, incluso si los datos están formados por paquetes malformados o no destinados a un equipo en otro segmento.

Importante Los repetidores son una forma económica de extender la longitud de cableado sin sacrificar la pérdida de datos. Los concentradores permiten conectar varios equipos a un punto central sin pérdida de datos. Un concentrador transmite el paquete de datos a todos los equipos y segmentos que están conectados al mismo.

Utilice un repetidor para:

- Conectar dos o más segmentos con cable similar.
- Regenerar la señal para incrementar la distancia transmitida.
- Transmitir todo el tráfico en ambas direcciones.
- Conectar dos segmentos del modo más rentable posible.

Concentradores (Hub) Los concentradores son dispositivos de conectividad que conectan equipos en una topología en estrella. Los concentradores contienen múltiples puertos para conectar los componentes de red.

Si utiliza un concentrador, una rotura de la red no afecta a la red completa; sólo el segmento y el equipo adjunto al segmento falla. Un único paquete de datos enviado a través de un concentrador fluye a todos los equipos conectados. Hay dos tipos de concentradores:

• *Concentradores pasivos*. Envían la señal entrante directamente a través de sus puertos sin ningún procesamiento de la señal. Estos concentradores son generalmente paneles de cableado.

• *Concentradores activos.* A veces denominados *repetidores multipuerto,* reciben las señales entrantes, procesan las señales y las retransmiten a sus potencias y definiciones originales a los equipos conectados o componentes.

Use un concentrador para:

- Cambiar y expandir fácilmente los sistemas de cableado.
- Utilizar diferentes puertos con una variedad de tipos de cable.
- Permitir la monitorización central de la actividad y el tráfico de red.

Puentes (bridges) Un puente es un dispositivo que distribuye paquetes de datos en múltiples segmentos de red que utilizan el mismo protocolo de comunicaciones. Un puente distribuye una señal a la vez. Si un paquete va destinado a un equipo dentro del mismo segmento que el emisor, el puente retiene el paquete dentro de ese segmento. Si el paquete va destinado a otro segmento, lo distribuye a ese segmento. (Vea figura 1.2)

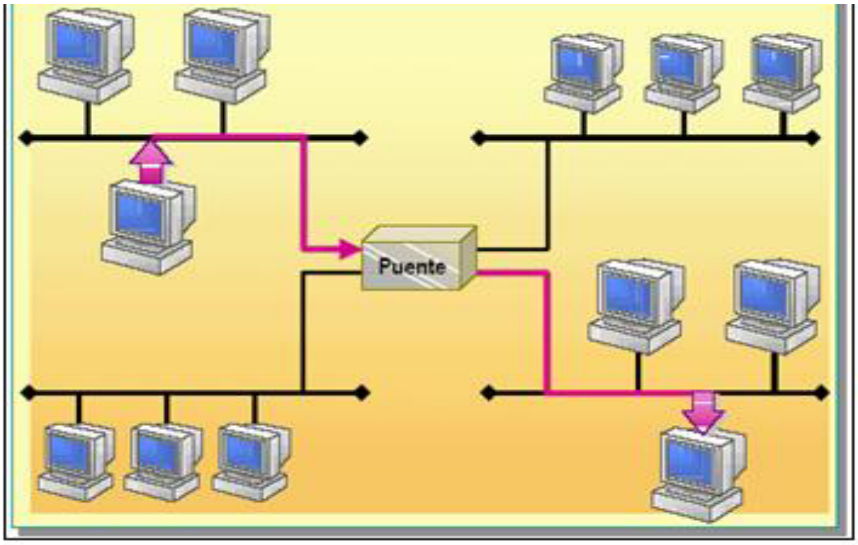

Figura 1.2 Puente (bridge)

A medida que el tráfico cruza a través del puente, la información sobre las direcciones MAC de los equipos emisores se almacena en la memoria del puente. El puente usa esta información para construir una tabla basada en estas direcciones.

A medida que se envían más datos, el puente construye una tabla puente que identifica a cada equipo y su ubicación en los segmentos de red. Cuando el puente recibe un paquete, la dirección de origen se compara a la dirección de origen listada en la tabla. Si la dirección fuente no está presente en la tabla, se añade a la misma. A continuación, el puente compara la dirección de destino con la dirección de destino listada en la tabla. Si reconoce la ubicación de la dirección de destino, reenvía el paquete a esta dirección. Si no reconoce la dirección de destino, reenvía el paquete a todos los segmentos.

Use un puente para:

- Expandir la longitud de un segmento.
- Proporcionar un mayor número de equipos en la red.
- Reducir cuellos de botella de tráfico resultante de un excesivo número de equipos conectados.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo cada red más eficiente.
- Enlazar cables físicos de distinto tipo, como cable de par trenzado con cable coaxial en Ethernet.

Conmutadores o Switches Los conmutadores son similares a los puentes, pero ofrecen una conexión de red más directa entre los equipos de origen y destino. Cuando un conmutador recibe un paquete de datos, crea una conexión interna separada, o segmento, entre dos de sus puertos cualquiera y reenvía el paquete de datos al puerto apropiado del equipo de destino únicamente, basado en la información de la cabecera de cada paquete. Esto aísla la conexión de los demás puertos y da acceso a los equipos origen y destino a todo el ancho de banda de una red.

A diferencia de un concentrador, los conmutadores son comparables a un sistema telefónico con líneas privadas. En tal sistema, si una persona llama a cualquier otra, el operador o conmutador telefónico les conecta a una línea dedicada. Esto permite que tengan lugar más conversaciones a más en un momento dado. (Vea figura 1.3)

Use un conmutador para:

- Enviar un paquete directamente del equipo origen al destino.
- Proporcionar una mayor velocidad de transmisión de datos.

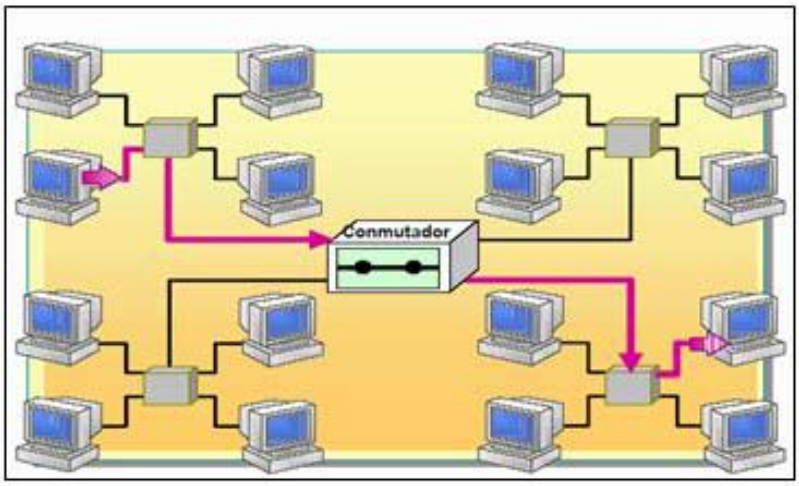

Figura 1.3 Conmutador (Switches)

Enrutadores (Routers) Un enrutador es un dispositivo que actúa como un puente o conmutador, pero proporciona funcionalidad adicional. Al mover datos entre diferentes segmentos de red, los enrutadores examinan la cabecera del paquete para determinar la mejor ruta posible del paquete.

- Un enrutador conoce el camino a todos los segmentos de la red accediendo a información almacenada en la tabla de rutas. Los enrutadores permiten a todos los usuarios de una red compartir una misma conexión a Internet o a una WAN. Los enrutadores permiten el flujo de datos a través de LANs o WANs, dependiendo de la red de destino de los datos. (Vea figura 1.4)

Use un enrutador para:

- Enviar paquetes directamente a un equipo de destino en otras redes o segmento. Los enrutadores usan una dirección de paquete más completa que los puentes. Los enrutadores garantizan que los paquetes viajen por las rutas más eficientes a sus destinos. Si un enlace entre dos enrutadores falla, el enrutador de origen puede determinar una ruta alternativa y mantener el tráfico en movimiento.

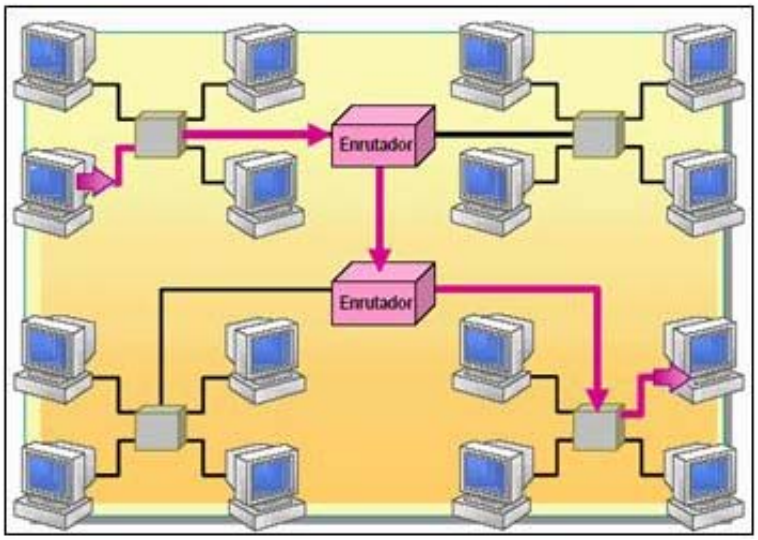

Figura 1.4 Enrutador (Router)

- Reducir la carga en la red. Los enrutadores leen sólo los paquetes de red direccionados y pasan la información sólo si la dirección de red es conocida. De este modo, no pasan información corrupta. Esta capacidad de controlar los datos que pasan a través del enrutador reduce la cantidad de tráfico entre redes y permite a los enrutadores utilizar estos enlaces más eficientemente que los puentes.

Puertas de enlace (Gateway) Las puertas de enlace permiten la comunicación entre diferentes arquitecturas de red. Una puerta de enlace toma los datos de una red y los empaqueta de nuevo, de modo que cada red pueda entender los datos de red de la otra.

Una puerta de enlace es cómo un intérprete. Por ejemplo, si dos grupos de personas pueden físicamente hablar entre sí pero hablan idiomas diferentes, necesitan un intérprete para comunicarse. De modo similar, dos redes pueden tener una conexión física, pero necesitan una puerta de enlace para traducir la comunicación de red. Permiten el flujo de datos a través de LANs o WANs y funcionan de modo que equipos que utilizan diversos protocolos puedan comunicarse entre sí. (Vea figura 1.5)

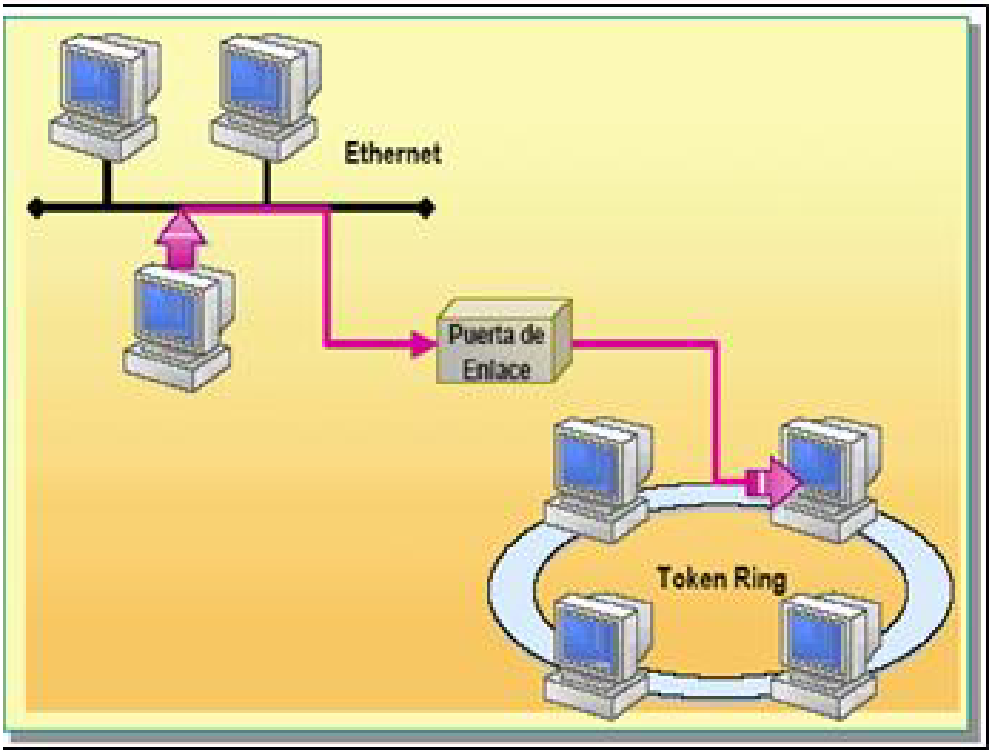

Figura 1.5 Puerta de enlace (Gateway)

Use una puerta de enlace para enlazar dos sistemas que no utilizan:

- La misma arquitectura.
- Los mismos conjuntos de reglas de comunicación y regulaciones.
- Las mismas estructuras de formateo de datos. [R8]

1.8 Servicios de una red

Para que el trabajo de una red sea efectivo, debe prestar una serie de servicios a sus usuarios, como son:

1. Acceso, este servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario para determinar cuales son los recursos de la misma que puede utilizar, como servicios para permitir la conexión de usuarios de la red desde lugares remotos.
2. Ficheros, el servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los

requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

3. Impresión, este servicio permite compartir impresoras entre múltiples usuarios, reduciendo así el gasto. En estos casos, existen equipos servidores con capacidad para almacenar los trabajos en espera de impresión. Una variedad de servicio de impresión es la disponibilidad de servidores de fax.
4. Correo, el correo electrónico, aplicación de red más utilizada que ha permitido claras mejoras en la comunicación frente a otros sistemas. Este servicio además de la comodidad, ha reducido los costos en la transmisión de información y la rapidez de entrega de la misma.
5. Información, los servidores de información pueden bien servir ficheros en función de sus contenidos como pueden ser los documentos hipertexto, como es el caso de esta presentación. O bien, pueden servir información dispuesta para su proceso por las aplicaciones, como es el caso de los servidores de bases de datos.
6. Otros, generalmente existen en las redes más modernas que poseen gran capacidad de transmisión, en ellas se permite transferir contenidos diferentes de los datos, como pueden ser imágenes o sonidos, lo cual permite aplicaciones como: estaciones integradas (voz y datos), telefonía integrada, servidores de imágenes, videoconferencia de sobremesa, etc.

1.9 Beneficios de la redes

Una de las razones de que tantas compañías estén conectando en red sus computadoras es que se acrecientan muchos beneficios del uso de una red. Algunos de éstos beneficios son evidentes de inmediato, mientras que otros se hacen evidentes después de que se ha instalado la red y se ha usado por algún tiempo. Los beneficios son:

a) Hardware compartido. Los usuarios de redes pueden compartir muchos dispositivos de hardware como impresoras, CD-ROM, espacio en disco, en

cinta. Así adquiere menos periféricos costosos para cada computadora. Lo cual significa un ahorro inmediato en los costos.

b) Aumento de la productividad. Las redes hacen que la información esté disponible de inmediato para muchas personas, lo cual significa que el personal no necesita caminar de una estación de trabajo a otra o de un edificio a otro para copiar un archivo. Esto significa más tiempo para trabajar en las tareas sin interrupción.

c) Aumento en la precisión. Toda la información compartida se almacena en una sola ubicación, se requiere una sola vez la captura de datos. No existe la duplicidad.

d) Soporte técnico más fácil. Existe personal dedicado a mantener el software y hardware en óptimas condiciones dentro de la empresa. En un entorno de red es más fácil dar soporte a programas de aplicación y sistemas operativos comunes. Esto es más productividad para el personal de soporte y menor costo para la empresa.

e) Comunicaciones extendidas. La conectividad permite a los usuarios de redes comunicarse con otros, tanto dentro como fuera de la empresa. Esto se traduce en realizar negocios con mayor rapidez. La compañía responde de manera oportuna a las necesidades internas como externas.

f) Recursos de investigación. Cuando se conecta a redes fuera de la empresa (Internet) los usuarios pueden tener acceso a más información que nunca. Esto proporciona la oportunidad para tomar mejores decisiones con información concreta y actualizada.

CAPÍTULO 2

TOPOLOGÍAS DE RED

TOPOLOGÍAS DE RED

Una topología de red es un mapa de distribución de la red física. Es la forma en la que el cableado se realiza en una red. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a considerar que topología usar cuando se decide instalar una red y son:

- La distribución de los equipos a interconectar
- El tipo de aplicaciones que se van a ejecutar
- La inversión que se va hacer
- El costo que se va a dedicar al mantenimiento y actualización de la red local
- El tráfico que va a soportar la red
- La capacidad de expansión, teniendo en cuenta la escalabilidad

2.1 Tipos de Topologías

Existen cinco topologías básicas, las cuáles son:

1.• *Bus.* Los equipos están conectados a un cable común compartido.
2.• *Estrella.* Los equipos están conectados a segmentos de cable que se extienden desde una ubicación central, o concentrador.
3.• *Anillo*. Los equipos están conectados a un cable que forma un bucle alrededor de una ubicación central.
4.• *Malla.* Los equipos de la red están conectados entre sí mediante un cable.
5.• *Híbrida.* Dos o más topologías utilizadas juntas.

2.2.1 Topología en bus

En una topología de bus, todos los equipos de una red están unidos a un cable continuo, o segmento, que los conecta en línea recta. (Vea figura 2.1)

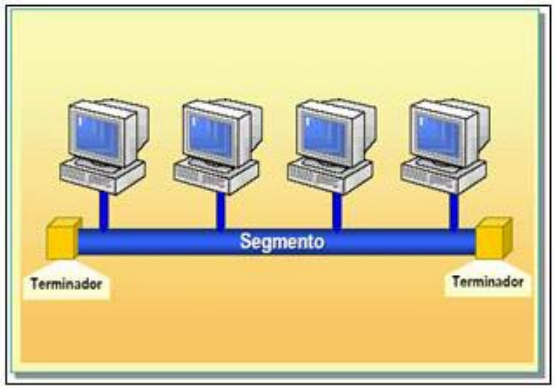

Figura 2.1 Topología en bus

Debido a la forma de transmisión de las señales eléctricas a través de este cable, sus extremos deben estar terminados por dispositivos de hardware denominados terminadores, que actúan como límites de la señal y definen el segmento.

Si se produce una rotura en cualquier parte del cable o si un extremo no está terminado, la señal balanceará hacia adelante y hacia atrás a través de la red y la comunicación se detendrá.

El número de equipos presentes en un bus también afecta al rendimiento de la red. Cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus, y en consecuencia, la red irá más lenta.

Además, debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho *ruido*. Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente. Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.

2.2.2 Topología en estrella

En una topología en estrella, los segmentos de cable de cada equipo en la red están conectados a un componente centralizado, o *concentrador*. Un concentrador es un

dispositivo que conecta varios equipos juntos. En una topología en estrella, las señales se transmiten desde el equipo, a través del concentrador, a todos los equipos de la red. A mayor escala, múltiples LANs pueden estar conectadas entre sí en una topología en estrella. (Vea figura 2.2)

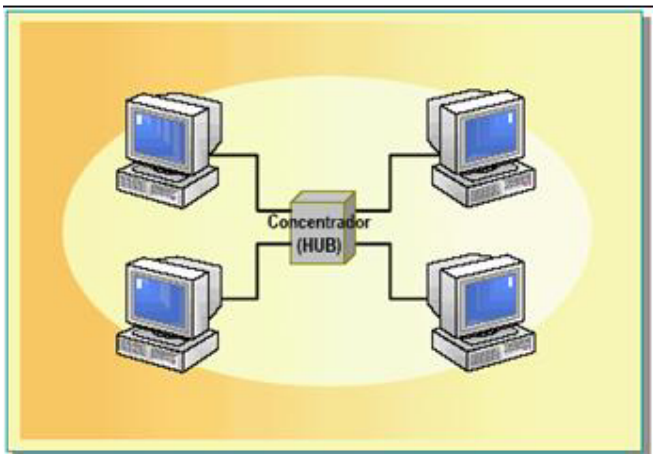

Figura 2.2 Topología en estrella

Una ventaja de la topología en estrella es que si uno de sus equipos falla, únicamente este equipo es incapaz de enviar o recibir datos. El resto de la red funciona normalmente.

El inconveniente de utilizar esta topología es que debido a que cada equipo está conectado a un concentrador, si éste falla, fallará toda la red. Además, en una topología en estrella, el ruido se crea en la red.

2.2.3 Topología en anillo

En una topología en anillo, los equipos están conectados con un cable de forma circular. A diferencia de la topología de bus, no hay extremos con terminaciones. Las señales viajan alrededor del bucle en una dirección y pasan a través de cada equipo, que actúa como repetidor para amplificar la señal y enviarla al siguiente equipo.

A mayor escala, en una topología en anillo múltiples LANs pueden conectarse entre sí utilizando el cable coaxial ThickNet o el cable de fibra óptica. (Vea figura 2.3)

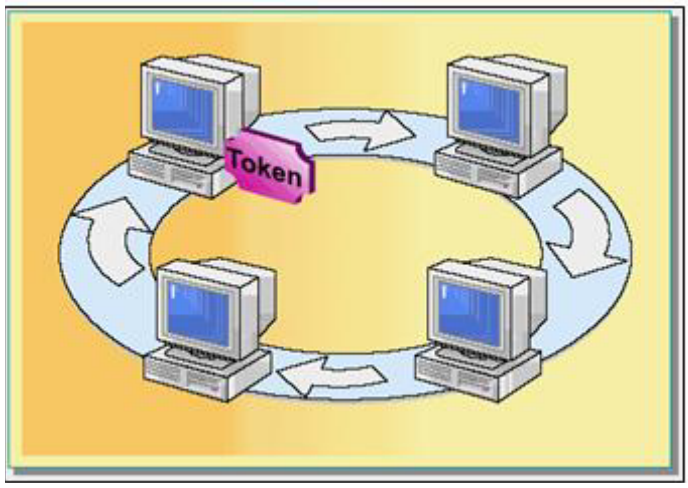

Figura 2.3 Topología en anillo

La ventaja de una topología en anillo es que cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo, conservando la potencia de la señal.

La ventaja de una topología en anillo es que puede gestionar mejor entornos con mucho tráfico que las redes con bus. Además, hay mucho menos impacto del ruido en las topologías en anillo.

El inconveniente de una topología en anillo es que los equipos sólo pueden enviar los datos de uno en uno en un único *Token Ring*. Además, las topologías en anillo son normalmente más caras que las tecnologías de bus.

2.2.4 Topología en malla

En una topología de malla, cada equipo está conectado a cada uno del resto de equipos por un cable distinto. Esta configuración proporciona rutas redundantes a través de la red de forma que si un cable falla, otro transporta el tráfico y la red sigue funcionando. (Vea figura 2.4)

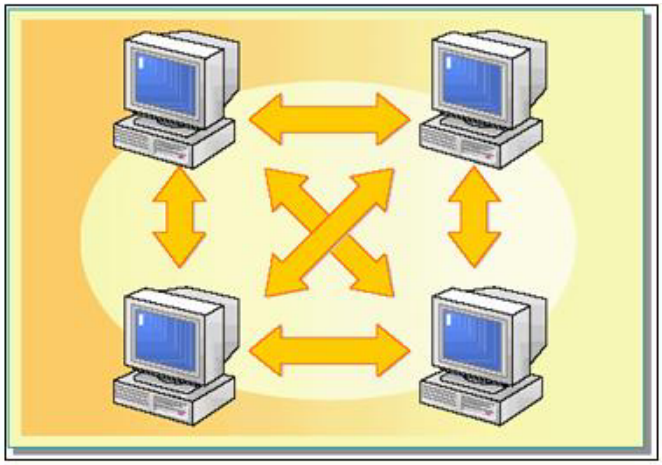

Figura 2.4 Topología en malla

A mayor escala, múltiples LANs pueden estar en estrella conectadas entre sí en una topología de malla utilizando red telefónica conmutada, un cable coaxial ThickNet o el cable de fibra óptica.

Una de las ventajas de las topologías de malla es su capacidad de respaldo al proporcionar múltiples rutas a través de la red. Debido a que las rutas redundantes requieren más cable del que se necesita en otras topologías, una topología de malla puede resultar cara.

2.2.5 Topologías híbridas

En una topología híbrida, se combinan dos o más topologías para formar un diseño de red completo. Raras veces, se diseñan las redes utilizando un solo tipo de topología. Por ejemplo, es posible que desee combinar una topología en estrella con una topología de bus para beneficiarse de las ventajas de ambas. (Vea figura 2.5)

En una topología híbrida, si un solo equipo falla, no afecta al resto de la red. Normalmente, se utilizan dos tipos de topologías híbridas: topología en estrella-bus y topología en estrella-anillo.

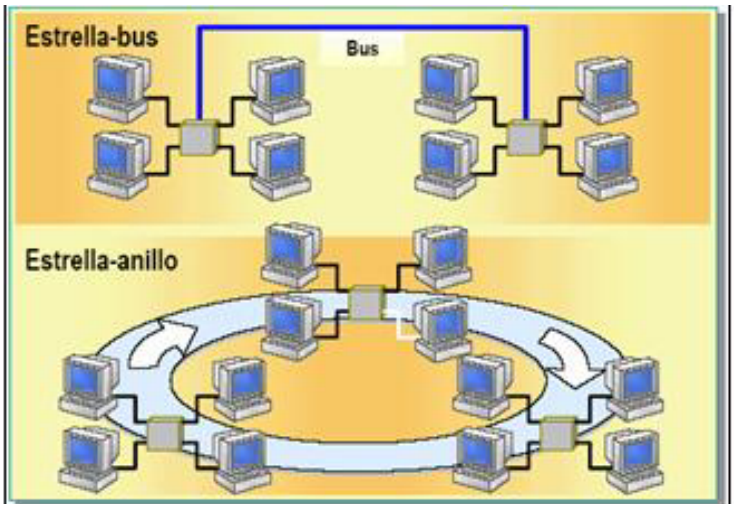

Figura 2.5 Topología híbrida

En una topología en estrella-bus, varias redes de topología en estrella están conectadas a una conexión en bus. Cuando una configuración en estrella está llena, podemos añadir una segunda en estrella y utilizar una conexión en bus para conectar las dos topologías en estrella.

En una topología en estrella-bus, si un equipo falla, no afectará al resto de la red. Sin embargo, si falla el componente central, o concentrador, que une todos los equipos en estrella, todos los equipos adjuntos al componente fallarán y serán incapaces de comunicarse.

En la topología en estrella-anillo, los equipos están conectados a un componente central al igual que en una red en estrella. Sin embargo, estos componentes están enlazados para formar una red en anillo.

Al igual que la topología en estrella-bus, si un equipo falla, no afecta al resto de la red. Utilizando el paso de testigo, cada equipo de la topología en estrella-anillo tiene las mismas oportunidades de comunicación. Esto permite un mayor tráfico de red entre segmentos que en una topología en estrella-bus. [R8]

CAPÍTULO 3

MEDIOS DE TRANSMISIÓN

3 MEDIOS DE TRANSMISIÓN

El cable que se utiliza para conectar una red se denomina medio de transmisión. Los tres factores que se deben tener en cuenta a la hora de elegir que cable se va utilizar para conectar las computadoras a la red son:

1. Velocidad de transmisión que se quiere conseguir
2. Distancia máxima entre computadoras que se van a conectar
3. Nivel de ruido e interferencias habituales en la zona que se va a instalar la red

Al conectar equipos para formar una red utilizamos cables que actúan como medio de transmisión de la red para transportar las señales entre los equipos. Un cable que conecta dos equipos o componentes de red se denomina *segmento*. Los cables se diferencian por sus capacidades y están clasificados en función de su capacidad para transmitir datos a diferentes velocidades, con diferentes índices de error.

Existe una gran cantidad de tipos de cables. Algunos fabricantes de cables publican un catálogo con cientos de tipos diferentes, los cuáles se pueden clasificar en tres grupos principales:

- Coaxial
- Par trenzado
- Fibra óptica.

El cable coaxial se utiliza cuando los datos viajan por largas distancias.

El cable de par trenzado es el tipo más habitual utilizado en redes.

El cable de fibra óptica se utiliza cuando necesitamos que los datos viajen a la velocidad de la luz.

3.1 Cable Coaxial

Hubo un tiempo donde el cable coaxial fue el más utilizado. Existían dos importantes razones para la utilización de este cable: era relativamente barato, y era ligero, flexible y sencillo de manejar.

Un cable coaxial consta de un núcleo de hilo de cobre rodeado por un aislante, un blindaje de metal trenzado y una cubierta externa. (Vea figura 3.1)

Figura 3.1 Cable coaxial

El término blindaje hace referencia al trenzado o malla de metal (u otro material) que rodea algunos tipos de cable. El blindaje protege los datos transmitidos absorbiendo las señales electrónicas espúreas, llamadas ruido, de forma que no pasan por el cable y no distorsionan los datos. Al cable que contiene una lámina aislante y una capa de blindaje de metal trenzado se le denomina cable apantallado doble. Para entornos que están sometidos a grandes interferencias, se encuentra disponible un blindaje cuádruple. Este blindaje consta de dos láminas aislantes, y dos capas de blindaje de metal trenzado,

El núcleo de un cable coaxial transporta señales electrónicas que forman los datos. Este núcleo puede ser sólido o de hilos. Si el núcleo es sólido, normalmente es de cobre.

Rodeando al núcleo hay una capa aislante dieléctrica que la separa de la malla de hilo. La malla de hilo trenzada actúa como masa, y protege al núcleo del ruido eléctrico y de la intermodulación (la intermodulación es la señal que sale de un hilo adyacente).

El núcleo de conducción y la malla de hilos deben estar separados uno del otro. Si llegaran a tocarse, el cable experimentaría un cortocircuito, y el ruido o las señales que se encuentren perdidas en la malla circularían por el hilo de cobre. Un cortocircuito eléctrico ocurre cuando dos hilos de conducción o un hilo y una tierra se ponen en contacto. Este contacto causa un flujo directo de corriente (o datos) en un camino no deseado. En el caso de una instalación eléctrica común, un cortocircuito causará el chispazo y el fundido de un fusible o del interruptor automático. Con dispositivos electrónicos que utilizan bajos voltajes, el resultado no es tan dramático, y a menudo casi no se detecta. Estos cortocircuitos de bajo voltaje generalmente causan un fallo en el dispositivo y lo habitual es que se pierdan los datos.

Una cubierta exterior no conductora (normalmente hecha de goma, Teflón o plástico) rodea todo el cable. El cable coaxial es más resistente a interferencias y atenuación que el cable de par trenzado.

La malla de hilos protectora absorbe las señales electrónicas perdidas, de forma que no afecten a los datos que se envían a través del cable de cobre interno. Por esta razón, el cable coaxial es una buena opción para grandes distancias y para soportar de forma fiable grandes cantidades de datos con un equipamiento poco sofisticado.

Tipos de cable coaxial:

- Cable fino (Thinnet).
- Cable grueso (Thicknet).

El tipo de cable coaxial más apropiado depende de 1as necesidades de la red en particular.

Cable Thinnet (Ethernet fino). El cable Thinnet es un cable coaxial flexible de unos 0,64 centímetros de grueso (0,25 pulgadas). Este tipo de cable se puede utilizar para la mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.

El cable coaxial Thinnet puede transportar una señal hasta una distancia aproximada de 185 metros (unos 607 pies) antes de que la señal comience a sufrir atenuación.

Los fabricantes de cables han acordado denominaciones específicas para los diferentes tipos de cables. El cable Thinnet está incluido en un grupo que se denomina la familia RG-58 y tiene una impedancia de 50 ohm. (La impedancia es la resistencia, medida en ohmios, a la corriente alterna que circula en un hilo.)

La característica principal de la familia RG-58 es el núcleo central de cobre y los diferentes tipos de cable de esta familia son:

- RG-58/U: Núcleo de cobre sólido.
- RG-58 A/U: Núcleo de hilos trenzados.
- RG-58 C/U: Especificación militar de RG-58 A/U.
- RG-59: Transmisión en banda ancha, como el cable de televisión.
- RG-60: Mayor diámetro y considerado para frecuencias más altas que RG-59, pero también utilizado para transmisiones de banda ancha.
- RG-62: Redes ARCnet.

Cable Thicknet (Ethernet grueso). El cable Thicknet es un cable coaxial relativamente rígido de aproximadamente 1,27 centímetros de diámetro. Al cable Thicknet a veces se le denomina Ethernet estándar debido a que fue el primer tipo de cable utilizado con la conocida arquitectura de red Ethernet. El núcleo de cobre del cable Thicknet es más grueso que el del cable Thinnet.

Cuanto mayor sea el grosor del núcleo de cobre, más lejos puede transportar las señales. El cable Thicknet puede llevar una señal a 500 metros. Por tanto, debido a la capacidad de Thicknet para poder soportar transferencia de datos a distancias mayores, a veces se utiliza como enlace central para conectar varias redes más pequeñas basadas en Thinnet.

Cable Thinnet frente a Thicknet. Como regla general, los cables más gruesos son más difíciles de manejar. El cable fino es flexible, fácil de instalar y relativamente barato. El cable grueso no se dobla fácilmente y, por tanto, es más complicado de instalar. Éste es un factor importante cuando una instalación necesita llevar el cable a través de espacios estrechos, como conductos y canales. El cable grueso es más caro que el cable fino, pero transporta la señal más lejos.

Hardware de conexión del cable coaxial

Tanto el cable Thinnet como el Thicknet utilizan un componente de conexión llamado conector BNC, para realizar las conexiones entre el cable y los equipos. Existen varios componentes importantes en la familia BNC, incluyendo los siguientes:

- El conector de cable BNC. El conector de cable BNC está soldado, o incrustado, en el extremo de un cable.
- El conector BNC T. Este conector conecta la tarjeta de red (NIC) del equipo con el cable de la red.
- Conector acoplador (barrel) BNC. Este conector se utiliza para unir dos cables Thinnet para obtener uno de mayor longitud.
- Terminador BNC. El terminador BNC cierra el extremo del cable del bus para absorber las señales perdidas.

El origen de las siglas BNC no está claro, y se le han atribuido muchos nombres, desde «British Naval Connector» a «Bayonet Neill-Councelman». Haremos referencia a esta familia hardware simplemente como BNC, debido a que no hay consenso en el nombre apropiado y a que en la industria de la tecnología las referencias se hacen simplemente como conectores del tipo BNC.

Utilice el cable coaxial si necesita un medio que pueda:

- Transmitir voz, vídeo y datos.

- Transmitir datos a distancias mayores de lo que es posible con un cableado menos caro
- Ofrecer una tecnología familiar con una seguridad de los datos aceptable.

3.2 Cable de par trenzado

En su forma más simple, un cable de par trenzado consta de dos hilos de cobre aislados y entrelazados. Hay dos tipos de cables de par trenzado: cable de par trenzado sin blindar (UTP) y par trenzado blindado (STP).

A menudo se agrupan una serie de hilos de par trenzado y se encierran en un revestimiento protector para formar un cable. El número total de pares que hay en un cable puede variar. El trenzado elimina el ruido eléctrico de los pares adyacentes y de otras fuentes como motores y transformadores.

Cable de par trenzado sin blindar (UTP)

El UTP, con la especificación 10BaseT, es el tipo más conocido de cable de par trenzado y ha sido el cableado LAN más utilizado en los últimos años. El segmento máximo de longitud de cable es de 100 metros.

La mayoría de los sistemas telefónicos utilizan uno de los tipos de UTP. De hecho, una razón por la que UTP es tan conocido es debido a que muchas construcciones están preparadas para sistemas telefónicos de par trenzado. Como parte del proceso previo al cableado, se instala UTP extra para cumplir las necesidades de cableado futuro. Si el cable de par trenzado preinstalado es de un nivel suficiente para soportar la transmisión de datos, se puede utilizar para una red de equipos. Sin embargo, hay que tener mucho cuidado, porque el hilo telefónico común podría no tener entrelazados y otras características eléctricas necesarias para garantizar la seguridad y nítida transmisión de los datos del equipo.

La intermodulación es un problema posible que puede darse con todos los tipos de cableado (la intermodulación se define como aquellas señales de una línea que interfieren con las señales de otra línea.)

UTP es particularmente susceptible a la intermodulación, pero cuanto mayor sea el número de entrelazados por pie de cable, mayor será la protección contra las interferencias.

Cable de par trenzado blindado (STP)

El cable STP utiliza una envoltura con cobre trenzado, más protectora y de mayor calidad que la usada en el cable UTP. STP también utiliza una lámina rodeando cada uno de los pares de hilos. Esto ofrece un excelente blindaje en los STP para proteger los datos transmitidos de intermodulaciones exteriores, lo que permite soportar mayores tasas de transmisión que los UTP a distancias mayores.

Aunque hayamos definido el cable de par trenzado por el número de hilos y su posibilidad de transmitir datos, son necesarios una serie de componentes adicionales para completar su instalación. Al igual que sucede con el cable telefónico, el cable de red de par trenzado necesita unos conectores y otro hardware para asegurar una correcta instalación.

El cable de par trenzado utiliza conectores telefónicos RJ-45 para conectar a un equipo. Éstos son similares a los conectores telefónicos RJ11. Aunque los conectores RJ-11 y RJ-45 parezcan iguales a primera vista, hay diferencias importantes entre ellos.

El conector RJ-45 contiene ocho conexiones de cable, mientras que el RJ-11 sólo contiene cuatro.

La necesidad de incrementar el ancho de banda nunca cesa, cuanto más se tenga, más se necesita. Las aplicaciones cada vez se vuelven más complejas, y los ficheros cada vez son más grandes. A medida que su red se vaya congestionando con más datos, la velocidad va disminuyendo y no volverá a ser rápida nunca más. Las buenas noticias son que la próxima generación de cableado está en marcha. Sin embargo, tendrá que tener cuidado con el cableado que esté instalado hoy, y asegurarse que cumplirá con sus necesidades futuras.

3.3 Cable de fibra óptica

En el cable de fibra óptica las señales que se transportan son señales digitales de datos en forma de pulsos modulados de luz. Esta es una forma relativamente segura de enviar datos debido a que, a diferencia de los cables de cobre que llevan los datos en forma de señales electrónicas, los cables de fibra óptica transportan impulsos no eléctricos.

El cable de fibra óptica es apropiado para transmitir datos a velocidades muy altas y con grandes capacidades debido a la carencia de atenuación de la señal y a su pureza.

Composición del cable de fibra óptica

Una fibra óptica consta de un cilindro de vidrio extremadamente delgado, denominado núcleo, recubierto por una capa de vidrio concéntrica, conocida como revestimiento. Las fibras a veces son de plástico. (Vea figura 3.2)

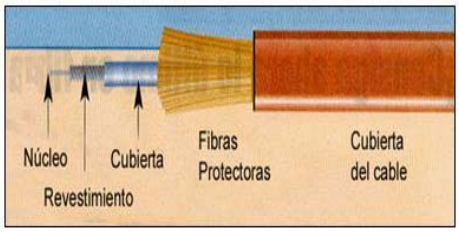

Figura 3.2 Cable de fibra óptica

El plástico es más fácil de instalar, pero no puede llevar los pulsos de luz a distancias tan grandes como el vidrio, debido a que los hilos de vidrio pasan las señales en una sola dirección, un cable consta de dos hilos en envolturas separadas. Un hilo transmite y el otro recibe. Una capa de plástico de refuerzo alrededor de cada hilo de vidrio y las fibras Kevlar ofrecen solidez. En el conector de fibra óptica, las fibras de Kevlar se colocan entre los dos cables. Al igual que sus homólogos (par trenzado y coaxial), los cables de fibra óptica se encierran en un revestimiento de plástico para su protección. (Vea Figura 3.3)

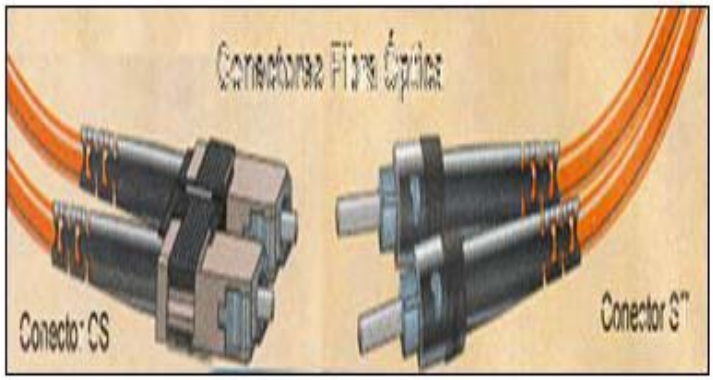

Figura 3.3 Conectores de fibra óptica

Las transmisiones del cable de fibra óptica no están sujetas a intermodulaciones eléctricas y son extremadamente rápidas, comúnmente transmiten a unos 100 Mbps, con velocidades demostradas de hasta 1 gigabit por segundo (Gbps). Pueden transportar una señal (el pulso de luz) varios kilómetros.

Consideraciones sobre el cable de fibra óptica

El cable de fibra óptica se utiliza si:

- Necesita transmitir datos a velocidades muy altas y a grandes distancias en un medio muy seguro.
- El cable de fibra óptica no se utiliza si:
- Tiene un presupuesto limitado.
- No tiene el suficiente conocimiento para instalar y conectar los dispositivos de forma apropiada.

Incremento del rendimiento del ancho de banda

El incremento de la velocidad de transmisión de datos es tan importante como el aumento del tamaño de la red y del tráfico de los datos. Maximizando el uso del canal de datos, podemos intercambiar más datos en menos tiempo. Al formato más básico de transmisión de datos o de información se le denomina unidireccional o simplex. Esto

significa que los datos se envían en una única dirección, desde el emisor al receptor. Ejemplos de transmisiones unidireccionales son la radio y la televisión. Con la transmisión unidireccional, los problemas que se encuentran durante la transmisión no se detectan ni corrigen. Incluso el emisor no tiene seguridad de que los datos son recibidos.

En el siguiente nivel de transmisión de datos, llamado transmisión alterna o half-duplex, los datos se envían en ambas direcciones, pero en un momento dado sólo se envían en una dirección. Ejemplos de tecnología que utilizan la comunicación alterna son las radios de onda corta y los walkie-talkies. Con la transmisión alterna se puede incorporar detección de errores y peticiones para reenvío de datos erróneos.

La World Wide Web es una forma de transmisión de datos alterna. Se envía una petición a una página Web y se espera mientras la está devolviendo. La mayoría de las comunicaciones por módem utilizan transmisión de datos alterna.

El método más eficiente para la transmisión de datos consiste en la utilización de la transmisión bidireccional o full-duplex, donde los datos pueden ser transmitidos y recibidos al mismo tiempo. Un buen ejemplo es una conexión de cable que no sólo permite que se reciban canales de televisión, sino que además soporta el teléfono y la conexión a Internet. Un teléfono es una conexión bidireccional porque permite hablar al mismo tiempo a las dos partes. Los módems, por diseño, son dispositivos alternos. Éstos envían o reciben datos, conmutando entre el modo de transmisión y el modo de recepción. Se puede crear un canal de módem bidireccional usando dos módems y dos líneas telefónicas. Lo único que se necesita es que los dos equipos estén conectados y configurados para soportar este tipo de comunicación.

3.4 Selección del cable

Para determinar cuál es el mejor cable para un lugar determinado habrá que tener en cuenta distintos factores:

- Carga de tráfico en la red
- Nivel de seguridad requerida en la red

- Distancia que debe cubrir el cable
- Presupuesto para el cable

Cuanto mayor sea la protección del cable frente al ruido eléctrico interno y externo, llevará una señal clara más lejos y más rápido. Sin embargo, la mayor velocidad, claridad y seguridad del cable implica un mayor costo.

Al igual que sucede con la mayoría de los componentes de las redes, es importante el tipo de cable que se adquiera. Si se trabaja para una gran organización y se escoge el cable más barato, inicialmente los administradores del dinero estarían muy complacidos, pero pronto podrían observar que la LAN es inadecuada en la velocidad de transmisión y en la seguridad de los datos.

El tipo de cable que se adquiera va a estar en función de las necesidades del sitio en particular. El cableado que se adquiere para instalar una LAN para un negocio pequeño tiene unos requerimientos diferentes del cableado necesario para una gran organización, como por ejemplo, una institución bancaria.

En una pequeña instalación donde las distancias son pequeñas y la seguridad no es un tema importante, no tiene sentido elegir un cable grueso, caro y pesado.

El nivel de blindaje requerido afectará al costo del cable. La mayoría de las redes utilizan algún tipo de cable apantallado. Será necesario un mayor blindaje cuanto mayor sea el ruido del área por donde va el cable. También el mismo blindaje en un cable de tipo plenum será más caro.

La intermodulación y el ruido pueden causar graves problemas en redes grandes, donde la integridad de los datos es fundamental. El cableado barato tiene poca resistencia a campos eléctricos exteriores generados por líneas de corriente eléctrica, motores, y transmisores de radio. Esto lo hace susceptible al ruido y a la intermodulación.

La velocidad de transmisión se mide en megabits por segundo. Un punto de referencia estándar para la transmisión de la LAN actual en un cable de cobre es de 100 Mbps. El cable de fibra óptica trasmite a más de 1 Gbps.

Los cables de grado más alto pueden transportar datos con seguridad a grandes distancias, pero son relativamente caros; los cables de menor grado, los cuales proporcionan menos seguridad en los datos a distancias más cortas, son relativamente más baratos.

Los diferentes tipos de cables tienen diferentes índices de atenuación; por tanto, las especificaciones del cable recomendadas especifican límites de longitud para los diferentes tipos. Si una señal sufre demasiada atenuación, el equipo receptor no podrá interpretarla. La mayoría de los equipos tienen sistemas de comprobación de errores que generarán una retransmisión si la señal es demasiado tenue para que se entienda. Sin embargo, la retransmisión lleva su tiempo y reduce la velocidad de la red. [R5]

CAPÍTULO 4

PROTOCOLOS DE COMUNICACIÓN

4 PROTOCOLOS DE COMUNICACIÓN

Los protocolos de comunicación de red son el conjunto de reglas o normas que especifican el método para enviar y recibir datos entre varias computadoras. Su instalación está en correspondencia con el tipo de red y el sistema operativo que la computadora tenga instalado.

No existe un único protocolo de red, y es posible que en un mismo ordenador coexistan instalados varios de ellos, pues cabe la posibilidad que un mismo ordenador pertenezca a redes distintas. La variedad de protocolos puede suponer un riesgo de seguridad: cada protocolo de red que se instala en un sistema queda disponible para todos los adaptadores de red existentes en dicho sistema. Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no deseado a los recursos de la red. Son varios los métodos de acceso que pueden emplearse en redes de área local. Sin embargo sólo se describen específicamente dos grandes grupos de métodos de acceso a redes de área local. Concretamente el primero de ellos lo forma el método llamado de contención o colisión.

En el presente se detalla el método CSMA/CD perteneciente a éste primer grupo utilizado de manera profusa en redes de arquitectura en bus. Los métodos de acceso conocidos como token passing o testigo circulante y protocolo por poleo, que son empleados mayoritariamente en redes de área local con arquitectura en anillo, constituyen el segundo grupo de métodos de acceso al medio.

4.1 Protocolo CSMA/CD

CSMA/CD, siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple con Escucha de Portadora y Detección de Colisiones"), es una técnica usada en redes **Ethernet**. Apareció primeramente la técnica **CSMA**, que fue posteriormente mejorada con la aparición de CSMA/CD.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no.

CSMA/CD (Carrier Sense Multiple Access, acceso múltiple con escucha de portadora) significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir

previamente escucha el canal antes de emitir. Lo cual es el protocolo de señal eléctrica que se usa. En función de como actúe la estación, el método **CSMA/CD** se puede clasificar en:

- CSMA no-persistente: si el canal está ocupado espera un tiempo **aleatorio** y vuelve a escuchar. Si detecta libre el canal, emite inmediatamente
- CSMA 1-persistente: con el canal ocupado, la estación pasa a escuchar constantemente el canal, sin esperar tiempo alguno. En cuanto lo detecta libre, emite. Puede ocurrir que, si durante un retardo de propagación o **latencia** de la red posterior a la emisión de la trama emitiera otra estación, se produciría una colisión (probabilidad 1).
- CSMA p-persistente: después de encontrar el canal ocupado, y quedarse escuchando hasta encontrarlo libre, la estación decide si emite. Para ello ejecuta un algoritmo o programa que dará orden de transmitir con una probabilidad p, o de permanecer a la espera (probabilidad (1-p)). Si no transmitiera, en la siguiente ranura o división de tiempo volvería a ejecutar el mismo algoritmo. Así hasta transmitir. De esta forma se reduce el número de colisiones (compárese con CSMA 1-persistente, donde p=1).

Una vez comenzado a emitir, no para hasta terminar de emitir la trama completa. Si se produjera una colisión, esto es, que dos tramas de distinta estación fueran emitidas a la vez en el canal, ambas tramas serán incompresibles para las otras estaciones y la transmisión habrá sido un desastre.

Finalmente **CSMA/CD** supone una mejora sobre **CSMA**, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión, para inmediatamente la transmisión.

La ganancia producida es el tiempo que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

El primer paso a la hora de transmitir será saber si el medio está libre. Para eso escuchamos lo que dicen los demás. Si hay portadora en el medio, es que está ocupado y, por tanto, seguimos escuchando; en caso contrario, el medio está libre y podemos transmitir. A continuación, esperamos un tiempo mínimo necesario para poder diferenciar bien una trama de otra y comenzamos a transmitir. Si durante la transmisión

de una trama se detecta una colisión, entonces las estaciones que colisionan abortan el envío de la trama y envían una señal de reinicio. Después de una colisión, las estaciones esperan un tiempo aleatorio para volver a transmitir una trama.

En redes inalámbricas, resulta a veces complicado llevar a cabo el primer paso (escuchar al medio para determinar si está libre o no). Por este motivo, surgen dos problemas que pueden ser detectados:

1. Problema del nodo oculto: la estación cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo al que la estación no "oye".
2. Problema del nodo expuesto: la estación cree que el medio está ocupado, cuando en realidad lo está ocupando otro nodo que no interferiría en su transmisión a otro destino.

Para resolver estos problemas, la **IEEE 802.11** propone **MACA** (MultiAccess Collision Avoidance – Evitación de Colisión por Acceso Múltiple).

CSMA / CD (Carrier Sense Multiple Access / Collision Detection) es el protocolo utilizado en redes **Ethernet** para asegurar que sólo un nodo de red se transmite en la red de cable en cualquier momento.

Carrier Sense significa que cada dispositivo Ethernet escucha el cable Ethernet antes de que los intentos de transmitir. Si el dispositivo Ethernet sentidos otro dispositivo que está transmitiendo, se espera transmitir.

Multiple Access significa que más de un dispositivo Ethernet puede teledetección (escucha y espera transmitir) a la vez.

Detección de colisión significa que cuando múltiples dispositivos Ethernet accidentalmente transmitir al mismo tiempo, son capaces de detectar este error.

¿Cómo se producen las colisiones en virtud del CSMA / CD

Imagine una red Ethernet muy simple con sólo dos nodos.

Cada nodo, de manera independiente, decide enviar una estructura Ethernet al otro nodo.

Ambos nodos escuchar el cable Ethernet y el sentir que ninguno está presente.

Ambos nodos transmiten simultáneamente, causando una colisión.

Ambos nodos detectan la colisión y cada nodo espera una cantidad aleatoria de tiempo antes de remitirla de nuevo.

Colisiones son normales en una red Ethernet. Una pequeña cantidad de colisiones que se espera en el diseño de protocolos.

Si son demasiados los nodos se transmite en una red Ethernet, el número de colisiones puede elevarse a un nivel inaceptable. Esto puede reducir la cantidad de ancho de banda disponible en una red Ethernet, ya que se pierde mucho ancho de banda en la retransmisión.

CSMA/CD opera de la siguiente manera:

Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.

Si el medio esta libre (ninguna otra estación esta transmitiendo), se envía la transmisión.

Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.

Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.

Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.

Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.

Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Detección de portadora

La detección de portadora es utilizada para escuchar al medio (la portadora) para ver si se encuentra libre. Si la portadora se encuentra libre, los datos son pasados a la capa física para su transmisión. Si la portadora está ocupada, se monitorea hasta que se libere.

Detección de colisiones

Luego de comenzar la transmisión, continúa el monitoreo del medio de transmisión. Cuando dos señales colisionan, sus mensajes se mezclan y se vuelven ilegibles. Si esto ocurre, las estaciones afectadas detienen su transmisión y envían una señal de expansión. La señal de expansión de colisión asegura que todas las demás estaciones de la red se enteren de que ha ocurrido una colisión.

Encapsulado

El encapsulado es realizado por la estación emisora. El encapsulado es el acto de agregar información, direcciones y bytes para el control de errores, al comienzo y al final de la unidad de datos transmitidos. Esto es realizado luego que los datos son

recibidos por la subcapa de control de enlace lógico (LLC). La información añadida es necesaria para realizar las siguientes tareas:

Sincronizar la estación receptora con la señal.

Indicar el comienzo y el fin de la trama.

Identificar las direcciones tanto de la estación emisora como la receptora.

Detectar errores en la transmisión.

Desencapsulado

El desencapsulado es realizado por la estación receptora. Cuando es recibida una trama, la estación receptora es responsable de realizar las siguientes tareas:

Reconocer la dirección de destino y determinar si coincide con su propia dirección.

Realizar la verificación de errores.

Remover la información de control que fue añadida por la función de encapsulado de datos en la estación emisora.

Administración de acceso al medio

En la estación emisora, la función de administración de acceso al medio es responsable de determinar si el canal de comunicación se encuentra disponible. Si el canal se encuentra disponible puede iniciarse la transmisión de datos.

Adicionalote, la función de administración es responsable de determinar que acción deberá tomarse en caso de detectarse una colisión y cuando intentará retransmitir.

En la estación receptora la función de administración de acceso al medio es responsable de realizar las comprobaciones de validación en la trama antes de pasarla a la función de desencapsulado.

Codificación/decodificación de datos

Esta función es responsable de obtener la forma eléctrica u óptica de los datos que se van a transmitir en el medio.

La codificación de datos es realizada por la estación emisora. Esta es responsable de traducir los bits a sus correspondientes señales eléctricas u ópticas para ser trasladadas a través del medio. Adicionalmente, esta función es responsable de escuchar el medio y notificar al la función de administración de acceso al medio si el medio se encuentra libre, ocupado o se ha detectado una colisión.

La decodificación de datos es realizada en la estación receptora. Esta es responsable de la traducción de las señales eléctricas u ópticas nuevamente en un flujo de bits.

Trama de transmisión CSMA/CD

Se defina a una trama de transmisión como el grupo de bits en un formato particular con un indicador de señal de comienzo de la trama.

El formato de la trama permite a los equipos de red reconocer el significado y propósito de algunos bits especificos en la trama. Una trama es generalmente una unidad lógica de transmisión conteniendo información de control para el chequeo de errores y para el direccionamiento.

4.2 Protocolo Token Passing

Estos protocolos se pueden considerar como un conjunto de líneas punto a punto simplex que interconectan nodos en un anillo, que puede ser lógico y/o físico. Los frames se transmiten en un determinado sentido dentro del anillo y dan la vuelta completa. Cada frame que se recibe del nodo anterior se transmite al siguiente. El nodo emite un frame hacia el siguiente nodo, y paralelamente, recibe y procesa los bits que le llegan del nodo anterior en el anillo.

En un determinado momento, sólo un nodo de la red puede estar en modo transmisión, y los demás deben estar a la escucha. Si no hay tráfico en la red todos los nodos están escuchando.

Cuando ningún host desea transmitir, todos están en modo escucha y se envía por el anillo un frame especial denominado *token*. El token va pasando de un host a otro indefinidamente

Cuando algún nodo desea transmitir debe esperar a que pase por él el token. En ese momento, se apodera de éste, típicamente convirtiendo el token en el delimitador de inicio del frame. A partir de ese momento, el nodo pasa a modo transmisión y envía el frame al siguiente nodo

Todos los demás hosts del anillo, incluido el destino, siguen en modo escucha, retransmitiendo el frame recibido hacia el siguiente nodo. El host destino, además de retransmitirlo, retiene una copia del frame que pasará al nivel de red para su proceso

Al finalizar la vuelta, el emisor empieza a recibir su propio frame. Éste puede optar por descartarlo o compararlo con el frame enviado para verificar si la transmisión ha sido correcta

Cuando el nodo ha terminado de transmitir el último bit del frame pueden ocurrir dos cosas: que restaure el token en el anillo inmediatamente, o que espere hasta recibir, de la estación anterior, su frame, y sólo entonces restaure el token

El primer modo de funcionamiento recibe un nombre especial, y se le conoce como *Early Token Release*.

Si el emisor tiene varios frames listos para emitir puede enviarlos sin liberar el token, hasta consumir el tiempo máximo permitido, denominado *token-holding time*. Una vez agotados los frames que hubiera en el buffer, o el tiempo permitido el nodo restaura el token en el anillo. Bajo ninguna circunstancia un host debe estar en modo transmisión durante un tiempo superior al token-holding time. Este protocolo genera problemas nuevos: qué pasa si se pierde un frame? qué pasa si el nodo encargado de regenerar el token falla?. En toda red token passing existe una estación monitora que se ocupa de resolver estas situaciones y garantizar el normal funcionamiento del protocolo. En caso de problemas restaurará un token en el anillo para que el tráfico pueda seguir circulando normalmente. Cualquier estación de una red token passing está capacitada para actuar como monitor en caso necesario. Cuando un nodo se añade a la red queda a la escucha en busca de tokens o datos. Si no detecta actividad, emite un frame de control especial denominado *claim token*. Si existe ya un monitor éste responderá con un token a la petición. Si no, el recién incorporado recibirá su propio claim token, momento en el cual pasará a constituirse en monitor. Existe también un mecanismo de prioridades, el que funciona de la siguiente manera: existen bits en el frame que permiten establecer la prioridad de un nodo, por lo que nodos de mayor prioridad podrán tomar el control del token aunque algún host, pero de menor prioridad, esté transmitiendo. Una vez finalizada la transferencia, se debe devolver la prioridad que tenía al token. [R7]

4.3 Protocolo Por Poleo

Éste método cuenta con un dispositivo controlador central, que es una computadora como servidor. Pasa lista a cada nodo en una secuencia predefinida solicitando acceder a la red. Si tal solicitud se realiza, el mensaje se transmite; de lo contrario, el dispositivo central pasa lista al siguiente nodo.

Éste protocolo evita la posibilidad de que una estación interfiera con la comunicación de otra. Realiza una encuesta de dispositivo a dispositivo.

CAPÍTULO 5

TECNOLOGÍAS DE REDES

5 TECNOLOGÍAS DE REDES

Utilizamos diferentes tecnologías de redes para la comunicación entre equipos de LANs y WANs. Podemos utilizar una combinación de tecnologías para obtener la mejor relación costo-beneficio y la máxima eficacia del diseño de una red.

Las redes de área local nos permiten aplicar tecnología informática para compartir sus recursos de manera más eficiente y posibilitar la comunicación entre los usuarios.

Hay diferentes tecnologías de redes disponibles, entre las que se encuentran:

- Ethernet.
- Token ring.
- Arcnet
- Modo de transferencia asíncrona (*asynchronous transfer mode*, ATM).
- Interfaz de datos distribuidos por fibra (*Fiber Distributed Data Interface*, FDDI).

Entre otras, de las cuáles solo se explicarán las tres primeras.

Una de las principales diferencias entre estas tecnologías es el conjunto de reglas utilizada por cada una para insertar datos en el cable de red y para extraer datos del mismo. Este conjunto de reglas se denomina *método de acceso*.

5.1 Redes Ethernet

Ethernet surge como el primer esfuerzo real hacia les redes locales de computadoras. Surge en la decada de los 70´s como un desarrollo de los laboratorios de investigación Xerox Corp en Palo Alto California.

El diseño de Ethernet se sustenta en un bus general, que une a todos los elementos, por analogía con el “eter” de los antiguos griegos, que era la sustancia que unía todas las cosas (el sol con la tierra y los demás planetas así como los cuerpos entre sí), por lo que se le denominó Ethernet.

Ethernet es una popular tecnología LAN que utiliza el Acceso múltiple con portadora y detección de colisiones (*Carrier Sense Múltiple Access with Collision Detection*, CSMA/CD) entre estaciones con diversos tipos de cables. Ethernet es pasivo, lo que significa que no requiere una fuente de alimentación propia, y por tanto no falla a menos que el cable se corte físicamente o su terminación sea incorrecta. Ethernet se conecta utilizando una topología de bus en la que el cable está terminado en ambos extremos.

Método de acceso: El método de acceso a la red utilizado por Ethernet es el Acceso múltiple con portadora y detección de colisiones (*Carrier Sense Múltiple Access with Collision Detection*, CSMA/CD). CSMA/CD es un conjunto de reglas que determina el modo de respuesta de los dispositivos de red cuando dos de ellos intentan enviar datos en la red simultáneamente. La transmisión de datos por múltiples equipos simultáneamente a través de la red produce una colisión.

Cada equipo de la red, incluyendo clientes y servidores, rastrea el cable en busca de tráfico de red. Únicamente cuando un equipo detecta que el cable está libre y que no hay tráfico envía los datos. Después de que el equipo haya transmitido los datos en el cable, ningún otro equipo puede transmitir datos hasta que los datos originales hayan llegado a su destino y el cable vuelva a estar libre. Tras detectar una colisión, un dispositivo espera un tiempo aleatorio y a continuación intenta retransmitir el mensaje. Si el dispositivo detecta de nuevo una colisión, espera el doble antes de intentar retransmitir el mensaje.

Ethernet estándar, denominada 10BaseT, soporta velocidades de transferencia de datos de 10 Mbps sobre una amplia variedad de cableado. También están disponibles versiones de Ethernet de alta velocidad. Fast Ethernet (100BaseT) soporta velocidades de transferencia de datos de 100 Mbps y Gigabit Ethernet soporta velocidades de 1 Gbps (gigabit por segundo) o 1,000 Mbps.

Principales características

Velocidad de transmisión: 10 mbps.

Protocolo de acceso: CSMA/CD

Topología: bus

Su velocidad de transmisión excelente, sin embargo, en cuanto crece la red, dicha velocidad disminuye, debido al protocolo de comunicación que usa.

Ethernet opta por un control distribuido en vez de un control centralizado, aumentando con ello la confiabilidad del conjunto en el caso de fallas en alguna estación.

5.2 Redes Token ring

Las redes Token Ring originalmente fueron desarrolladas por IBM en los años 1970s, con topología lógica en anillo y técnica de acceso de paso de testigo.

El primer diseño de una red de Token-Ring es atribuido a E. E. Newhall en 1969. IBM publicó por primera vez su topología de Token-Ring en marzo de 1982. IBM anunció un producto Token-Ring en 1984, y en 1985 éste llegó a ser un standard debido al apoyo de la primera empresa informática mundial.

Hasta finales de 1988, la máxima velocidad permitida en este tipo de redes era de 4 Mbps, con soporte físico de par trenzado. En esa fecha se presentó la segunda generación Token Ring-II, con soporte físico de cable coaxial y de fibra óptica, y velocidades de hasta 16 Mbps. Sin embargo, las redes antiguas, con cable de par trenzado, debían recablearse si se querían utilizar las prestaciones de las de segunda generación, lo cual representa un buen ejemplo de la importancia que las decisiones sobre cableado tienen en la implantación de una red de área local.

En la topología de red en anillo las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo. No hay una computadora host central que guarde todos los datos. Las comunicaciones fluyen en una sola dirección alrededor del anillo. En esta topología los datos se distribuyen con un orden preestablecido

Esquemas de la Red Token Ring

Los datos en Token-Ring se transmiten a 4 ó 16mbps. Todas las estaciones se deben de configurar con la misma velocidad para que funcione la red. Cada computadora se conecta a través de cable Par Trenzado ya sea blindado o no a un concentrador llamado MAU(Media Access Unit), y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por el cual da vueltas el Token. En realidad el MAU es el que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información.

Principales características

Topología: anillo

Toda la información viaja en una sola dirección a lo largo del círculo formado por el anillo.

El anillo no representa un medio de difusión sino que una colección de enlaces punto a punto individual.

Cada estación se conecta a otras.

Cada nodo siempre pasa el mensaje, si este mensaje es para él, entonces lo copia y lo vuelve a enviar.

Número máximo de nodos por red 260.

En la implementación es posible diseñar anillos que permitan saltar a un nodo que este fallando.

Resultan más caras que las redes Ethernet pero son más estables.

Ventajas

- No requiere de enrutamiento.

- Requiere poca cantidad de cable.
- Fácil de extender su longitud, ya que el nodo esta diseñado como repetidor, por lo que permite amplificar la señal y mandarla mas lejos.

Desventajas

- Altamente susceptible a fallas.
- Una falla en un nodo deshabilita toda la red (esto hablando estrictamente en el concepto puro de lo que es una topología de anillo).
- El software de cada nodo es mucho más complejo.

Token ring utiliza el método de acceso conocido como Token passing o Paso de testigo y consiste en que una sola estación puede transmitir en determinado instante y es precisamente la que posea en ese momento el Token, este es el encargado de asignar los permisos para transmitir los datos.

La información que viaja en él recorre una sola dirección a lo largo de la red. No requiere de enrutamiento, ya que cada paquete es pasado a su vecino y así consecutivamente, por ejemplo, tenemos tres estaciones de trabajo A, B, C, etc., si una estación A transmite un mensaje, éste pasa a la estación B, independientemente de si va dirigido a ella o no, o si va dirigido a otra estación y luego pasa por C, y así consecutivamente.

El Token se mantiene circulando constantemente a través de todo el anillo mientras ninguna estación necesita transmitir. Cuando alguna maquina desea enviar o solicitar datos hacia la red debe esperar a que le llegue el Token vacío, cuando le llega adjunta el mensaje al Token y este activa una señal indicando que el bus esta ocupado. El mensaje continúa su recorrido en orden, hasta llegar a la estación destino. La estación que mandó puede chequear si el Token encontró a la estación destino y si entregó la información correspondiente (Acuse de recibo), en estos casos cuando la otra computadora recibe la información el Token regresa a la estación origen que envió el mensaje con un mensaje de que fue recibida la información. Luego se libera el Token para volver a ser usado por cualquiera otra computadora. Un dispositivo tiene que esperar hasta que el token llega a

ese lugar para poder adjuntar el mensaje que desea mandar hacia otra estación de trabajo.

Si en un momento dado el Token está ocupado atendiendo una llamada y otra maquina desea ocupar la red, envía un comando de espera antes de darle entrada a la nueva petición (por lo general, transcurren solo unas fracciones de segundo).

Aquí debido a que una computadora requiere el Token para enviar información no hay colisiones.

El Token es un paquete físico especial, que no debe confundirse con un paquete de datos. Ninguna estación puede retener el Token por más de un tiempo dado (10 ms).

El problema reside en el tiempo que debe esperar una computadora para obtener el Token sin utilizar. El Token circula muy rápidamente, pero obviamente esto significa que la mayor parte de las veces, los dispositivos tendrán que esperar algo antes de poder mandar un mensaje.

La eficiencia en este sistema se debe a que las comunicaciones siempre viajan en una misma dirección y el sistema únicamente permite que una información este viajando por el cable en un momento dado.

Cabe mencionar que si algún nodo de la red se cae (termino informático para decir que esta en mal funcionamiento o no funciona para nada) la comunicación en todo el anillo se pierde.

Igual a como sucede en la tecnología Ehernet, el sistema Token Ring también utiliza paquetes de información o tramas en las cuales se incluye la información de control de la comunicación.

El problema con Ethernet es que la distribución del acceso al medio es aleatoria, por lo que puede ser injusta, perjudicando a un computador durante un periodo de tiempo. En algunos casos es muy importante garantizar un acceso igualitario al medio, de modo de garantizar que siempre podremos transmitir, independientemente de la carga. Por razones de justicia en el acceso, típicamente estas redes se organizan en anillo, de modo de que el Token pueda circular en forma natural.

En cada anillo hay una estación supervisora que se encarga de inspeccionarlo. Cualquier estación puede llegar a ser supervisora. La responsabilidad de ésta es: vigilar el testigo,

tomar decisiones en caso de ruptura del anillo, limpieza del anillo de tramas mutiladas, observar la presencia de tramas huérfanas. [R4]

La unidad de acceso multiestación (MAU) es un dispositivo que permite establecer la topología física en estrella a partir del anillo lógico La MAU es un concentrador de dispositivos en estrella. (Vea figura 5.1)

Estas unidades pueden ser pasivas o activas, existiendo versiones para par trenzado blindado o sin blindar. Las unidades más utilizadas tienen ocho puertos para conectar terminales y otros dos, una de entrada y otra de salida, para extender el anillo. Cuando se supera el número máximo de dispositivos conectables a una MAU se añaden otras MAU conectándolas entre sí en anillo.

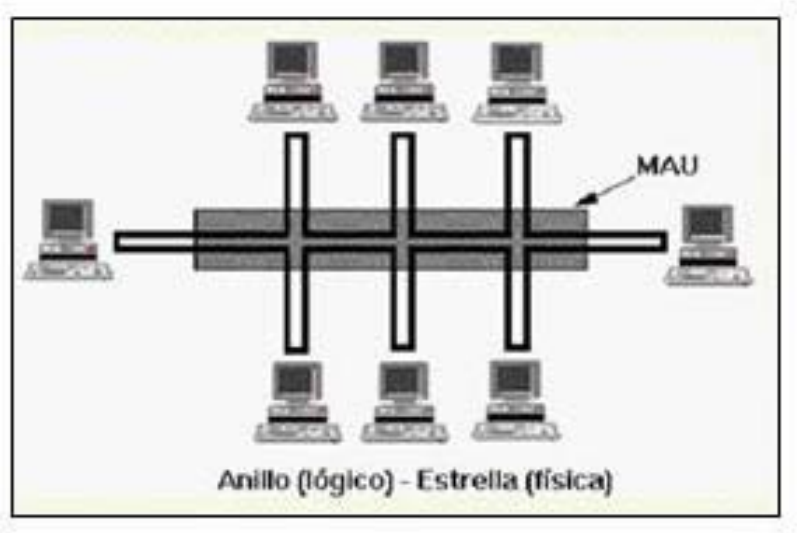

Figura 5.1 Unidad de acceso multiestación

Una MAU puede soportar hasta 72 computadoras conectadas y el cable de el MAU a la computadora puede ser hasta de 100 metros utilizando Par Trenzado Blindado, o 45 metros sin blindaje. El Token-Ring es eficiente para mover datos a través de la red. En redes pequeñas a medianas con tráfico de datos pesado el Token Ring es más eficiente que Ethernet. Por el otro lado, el ruteo directo de datos en Ethernet tiende a ser un poco mejor en redes que incluyen un gran número de computadoras con tráfico bajo o moderado.

Conexión de cableado

Las estaciones en redes Token Ring se conectan directamente a MAUs, las cuáles pueden ser cableadas a través del anillo (como se muestra en la figura). Los Patch cables

sirven para interconectar las MAUs. Los Lobe cables conectan a las estaciones con las MAUs.

Las tarjetas Token Ring están disponibles en modelos de 4 Mbits/sec y 16 Mbits/sec. Si una tarjeta de 16 Mbits/sec es usada en una red de 4 Mbits/sec, ésta opera a 4 Mbits/sec.

Un conector MAU conecta 8 o más estaciones de trabajo usando algún tipo de cable de red como medio. Se pueden interconectar más de 12 dispositivos MAU.

Los cables Token ring típicamente tienen conectores de 9 pines como terminales para conectar una tarjeta de red a un tipo especial, un conector especial que se conecta a la MAU, se pueden utilizar patch cables para extender los cables hasta 150 pies.

Los Patch cables extienden la distancia de una workstation hacia un dispositivo MAU. En los sistemas IBM, debe ser de tipo 6 para una longitud arriba de 150 pies. Ya que éste tipo de cable tiene el potencial suficiente para soportar grandes distancias.

El conector Tipo 1 los usa IBM en sus sistemas de cableado conectores de datos tipo A que son hermafroditas.

Cuando se usa par trenzado tipo 3, se requiere un filtro de medios para las workstations, éste convierte los conectores de cable y reduce el ruido.

Medios de Transmisión

El cable que se emplea normalmente para la transmisión de datos en esta red es el par trenzado, con o sin blindaje, aunque también se puede utilizar el cable coaxial o la fibra óptica.

Las estaciones se unen al anillo mediante RIU o unidades de interfase al anillo. Pueden estar en dos estados:

Repetidor: reenvía lo que le llega.

Transmisor: envía y lee del anillo.

Si el cable se llega a romper en algún lugar el anillo desaparece, esto se resuelve utilizando centro de cableado en estrella, llamados MAU que pueden detectar y corregir automáticamente fallos en el cableado. Si llegara a romperse al anillo, se puede

continuar operando si se puntea el segmento dañado. Con estos se mejora la fiabilidad y el mantenimiento de la red.

Token ring velocidad de funcionamiento y la popularidad

Aunque el proceso puede parecer complicado, la velocidad de transmisión de datos es extremadamente rápido y el movimiento de la razón se mide en microsegundos. Token ring también lleva incorporados en el sistema de gestión y recuperación para asegurar que el sistema no ceder el paso a los defectos o problemas.

Aunque el sistema de red Token ring parece ser fiable y rápido, sus primeras etapas de desarrollo se vieron afectadas con los problemas y las cuestiones que hicieron parecen ser menos confiable y eficiente que el sistema de red Ethernet. Estas condujeron a su posterior declive, con Ethernet en el lugar en la actualidad se estima que un 70 por ciento de las configuraciones de LAN en todo el mundo. [R4]

5.3 Redes Arcnet

Arquitectura de red de área local desarrollado por Datapoint Corporation ARCNET (Conocido también como Camel Cased, ARCnet, siglas de Attached Resource Computer NETwork) Arcnet era el primer sistema extensamente disponible del establecimiento de una red para los microordenadores y llegó a ser popular en los años 80.

Utiliza una técnica de acceso de paso de testigo como el Token Ring. La topología física es en forma de estrella, utilizando cable coaxial RG-62. Las estaciones de trabajo y el servidor están conectados a través de elementos de conexión llamados repetidores.

La velocidad de transmisión 2.5 Mbps. Las redes Arcnet son una de las redes más flexibles en su arquitectura. Pueden manejar topologías en estrella y bus, o una combinación que puede ser descrita como una estrella ramificada.

Utiliza repetidores pasivos o repetidores activos. Los repetidores activos permiten una distancia entre repetidor y estación de trabajo de 600 metros. Regularmente estos repetidores poseen 8 puertos y un repetidor pasivo solo 4 puertos permitiendo una distancia de 30 metros. La distancia máxima que soporta esta red es de 6 kilómetros.

Protocolo de datos de tipo Arcnet

Cuando un nodo recibe un Token éste puede ya sea iniciar la secuencia de transmisión a otro nodo o enviar la invitación a transmitir a otro. Si se desea transmitir, la estación envía un FBE (Free Buffer Enquiry) al destino para confirmar la disponibilidad de aceptar el mensaje. Ya sea que haya sido retornado un reconocimiento (ACK) o un no reconocimiento (NACK). Y si es recibido un reconocimiento de un FBE, el paquete entonces es transmitido.

Tiempos de respuesta de la red Arcnet

Arcnet siendo una red con el protocolo paso de testigo tiene la ventaja de calcular fácilmente los parámetros de la red que dan completamente los tiempos de respuesta. En Arcnet existen cinco tipos de transmisiones:

1. Invitación a transmitir (ITT)
2. Solicitud de memoria temporal libre (FBE)
3. Paquetes (PAC)
4. Reconocimiento positivo (ACK)
5. Reconocimiento negativo (NACK)

Cada una de las anteriores transmisiones inicia con una ráfaga de alerta (seis unos) y continúa con una transmisión de 11 bits por carácter.

Direccionamiento de Arcnet

Cada tarjeta de red (NIC) debe ser asignada con una dirección única entre 1 y 255, para que el anillo lógico funcione, cada NIC debe conocer su propia dirección (SID), más la dirección de la siguiente tarjeta en el anillo lógico.

El anillo lógico debe ser modificado cada vez que un nodo desea entrar o salir de la red. Cualquier nodo que es encendido, o un nodo que no haya recibido la invitación a transmitir dentro de 840 ms, causan la reconfiguración de la red.

Esta transmisión desbarata el paso normal del Token, y causando que todas las estaciones coloquen su registro NID a su propio registro fuente, tal que NID=SID.

Entonces el nodo de dirección más alta envía la primera invitación a transmitir, y si no hay respuesta dentro de 74 ms., el nodo asume que la dirección NID no existe, entonces incrementa el NID y prueba otra vez. El tiempo de reconfiguración depende del número total de nodos, el retardo de propagación del cable, y varía de 24 a 61 ms.

Características

- Aunque utilizan topología en bus, suele emplearse un HUB para distribuir las estaciones de trabajo usando una configuración de estrella.
- El cable que usan suele ser coaxial, aunque el par trenzado es el más conveniente para cubrir distancias cortas.
- Usa el método de paso de testigo, aunque físicamente la red no sea en anillo. En estos casos, a cada máquina se le da un número de orden y se implementa una simulación del anillo, en la que el Token utiliza dichos números de orden para guiarse.
- El cable utiliza un conector BNC giratorio. [R2]

CAPÍTULO 6

TARJETA DE INTERFACE DE RED

6 TARJETA DE INTERFACE DE RED

La tarjeta de interface de red constituyen la interfaz física entre la computadora y el cable de red, ésta se instala en una ranura de expansión de cada computadora que conformará la red. Las tarjetas de red ó NICs (Network Interface Card), son también llamadas adaptadores de red, Una vez instalado el adaptador de red, el cable de red se conecta al puerto del adaptador para conectar físicamente el equipo a la red.

Después de instalar la tarjeta de red, el cable de red se une al puerto de la tarjeta para realizar la conexión física entre el equipo y el resto de la red.

La función de la tarjeta de red es:

- Preparar los datos del equipo para el cable de red.
- Enviar los datos a otro equipo.
- Controlar el flujo de datos entre el equipo y el sistema de cableado.
- Recibir los datos que llegan por el cable y convertirlos en bytes para que puedan ser comprendidos por la unidad de procesamiento central del equipo (CPU).

La tarjeta de red contiene el hardware y la programación firmware (rutinas software almacenadas en la memoria de sólo lectura, ROM) que implementa las funciones de Control de acceso al medio. Cada adaptador de red tiene una dirección exclusiva, denominada dirección de control de acceso al medio (*media access control*, MAC), incorporada en chips de la tarjeta.

6.1 Preparación de los datos

Antes de enviar los datos por la red, la tarjeta de red debe convertirlos de un formato que el equipo puede comprender a otro formato que permita que esos datos viajen a través del cable de red.

Los datos se mueven por el equipo a través de unos caminos denominados buses. Realmente éstos son varios caminos de datos colocados uno al lado del otro. Como los caminos están juntos (paralelos), los datos se pueden mover en grupos en lugar de ir de forma individual (serie).

A los buses más antiguos, como aquellos utilizados en el primer equipo personal de IBM, se les conoce como buses de 8 bits porque en un momento dado podían mover 8 bits de datos. El equipo PC/AT utilizó un bus de 16 bits, lo que significa que en un momento dado podía mover 16 bits de datos. Los equipos actuales utilizan buses de 32 bits. Cuando los datos circulan en un bus del equipo, se dice que están circulando de forma paralela porque los 32 bits se están moviendo juntos. Piense en un bus de 32 bits como en una autovía de 32 carriles con 32 coches circulando juntos (de forma paralela), cada uno llevando un bit de datos.

Sin embargo, en un cable de red, los datos deben circular en un solo flujo de bits. Cuando los datos circulan en un cable de red se dice que están circulando en una transmisión en serie, porque un bit sigue a otro. En otras palabras, el cable es una autovía de un solo carril, y los datos siempre circulan en una sola dirección. El equipo puede estar enviando o recibiendo datos, pero nunca podrá estar haciendo las dos cosas al mismo tiempo.

La tarjeta de red toma los datos que circulan en paralelo y los reestructura, de forma que circulen por el cable de la red, que es un camino en serie de un bit. Esto se consigue convirtiendo las señales digitales del equipo en señales ópticas o eléctricas que pueden circular por los cables de la red. La componente responsable de esto es el transceptor (transmisor/receptor).

6.2 Direcciones de red

Además de la transformación de los datos, la tarjeta de red también tiene que anunciar su propia localización, o dirección, al resto de la red para diferenciarla de las demás tarjetas de red.

Una comisión del Institute of Electrical and Electronics Engineers (IEEE) asigna bloques de direcciones a cada fabricante de tarjetas de red. Los fabricantes graban las direcciones en los chips de la tarjeta mediante un proceso conocido como «marcado» de la dirección en la tarjeta. Con este proceso, cada tarjeta de red (y, por tanto, cada equipo) tiene una dirección única en la red.

6.3 Envío y control de datos

Antes de que la tarjeta de red emisora envíe datos a la red, mantiene un diálogo electrónico con la tarjeta de red receptora, de forma que ambas tarjetas se pongan de acuerdo en lo siguiente:

- Tamaño máximo de los grupos de datos que van a ser enviados.
- Cantidad de datos que se van a enviar antes de que el receptor de su confirmación.
- Intervalos de tiempo entre las cantidades de datos enviados.
- Cantidad de tiempo que hay que esperar antes de enviar la confirmación.
- Cantidad de datos que puede tener cada tarjeta antes de que haya desbordamiento.
- Velocidad de la transmisión de datos.

Si una tarjeta de red más moderna, rápida y sofisticada necesita comunicarse con una tarjeta de red más lenta y antigua, ambas necesitan encontrar una velocidad de transmisión común a la que puedan adaptarse. Algunas tarjetas de red más modernas incorporan circuitos que permiten que las tarjetas más rápidas se ajusten a la velocidad de las tarjetas más lentas.

Cada tarjeta de red le indica a la otra sus parámetros, aceptando o rechazando los parámetros de la otra tarjeta. Después de haber determinado todos los detalles de comunicación, las dos tarjetas comienzan a enviar y a recibir datos.

6.4 Opciones y parámetros de configuración

Las tarjetas de red a menudo tienen una serie de opciones que se deben configurar para que la tarjeta funcione apropiadamente. Algunos de los diseños más antiguos utilizan interruptores DIP externos. Algunos ejemplos de opciones que se pueden configurar:

Interrupción (IRQ).

Las tarjetas de red más antiguas se configuran por medio de software, jumpers, o una combinación de los dos; consulte la documentación de la tarjeta para ver la configuración software o jumpers apropiados. Las tarjetas más modernas utilizan la tecnología Plug and Play (PnP) ; como consecuencia, las tarjetas más antiguas que necesitan una configuración manual, han quedado obsoletas.

Líneas de petición de interrupción (IRQ)

Las líneas de petición de interrupción (IRQ) son líneas hardware por las que dispositivos como puertos de E/S, teclado, unidades de disco y tarjetas de red, pueden enviar interrupciones o peticiones al microprocesador del equipo.

Las líneas de petición de interrupción se incorporan en el hardware interno del equipo, y se les asignan diferentes niveles de prioridad, de forma que el microprocesador pueda determinar la importancia de las peticiones de servicios recibidas.

Cuando la tarjeta de red envía una petición al equipo, utiliza una interrupción (envía una señal electrónica a la CPU del equipo). Cada dispositivo del equipo debe utilizar una línea de petición de interrupción diferente. La línea de interrupción se especifica cuando se configura el dispositivo. (Vea figura 6.1)

IRQ	Equipo con un procesador 80486 (o superior)
2 (9)	EGA/VGA (Adaptador de gráficos mejorado/adaptador de gráficos de víde).
3	Disponible (A menos que sea utilizado como segundo puerto serie [COM2, COM4] o ratón de bus).
4	COM1, COM3.
5	Disponible (A menos que sea utilizado como segundo puerto paralelo [LPT2] o como tarjeta de sonido).
6	Controlador de disquete.
7	Puerto paralelo (LPT1).
8	Reloj de tiempo real.
10	Disponible
11	Disponible
12	Ratón (PS/2).
13	Coprocesador matemático.
14	Controlador de disco duro.
15	Disponible (A menos que sea utilizado para controlador secundario de disco duro).

Figura 6.1 Configuración manual de una tarjeta de red por medio de jumpers

Para la tarjeta de red se pueden utilizar IRQ3 o IRQ5, en la mayoría de los casos. Si se encuentra disponible, se recomienda IRQ5, y es la que se utiliza por omisión para la mayoría de los sistemas. Para conocer qué IRQ están siendo utilizadas, utilice una herramienta de diagnóstico del sistema.

6.5 Compatibilidad de tarjetas, buses y cables

Para asegurar la compatibilidad entre el equipo y la red, la tarjeta debe tener las siguientes características:

Coincidir con la estructura interna del equipo (arquitectura del bus de datos).

Tener el tipo de conector de cable apropiado para el cableado.

Por ejemplo, una tarjeta que funciona en la comunicación de un equipo Apple en una red en bus, no funcionará en un equipo de IBM en un entorno de anillo: el anillo de IBM necesita tarjetas que son físicamente diferentes de las utilizadas en un bus; y Apple utiliza un método de comunicación de red diferente.

6.6 Arquitectura del bus de datos

En un entorno de equipos personales, existen cuatro tipos de arquitecturas de bus: ISA, EISA, Micro Channel y PCI. Cada uno de los tipos es físicamente diferente a los demás. Es imprescindible que la tarjeta de red y el bus coincidan.

6.6.1 Arquitectura estándar de la industria (ISA)

ISA es la arquitectura utilizada en equipos IBM PC, XT y AT, así como en sus clones. Permite incorporar al sistema varios adaptadores por medio de conectores de placas que se encuentran en las ranuras o slots de expansión. En 1984 ISA se amplió de 8 bits a 16 bits cuando IBM introdujo el equipo IBM PC/AT. ISA hace referencia a la propia ranura de expansión (una ranura de 8 bits o de 16 bits). Las ranuras de 8 bits son más pequeñas que las de 16 bits, que realmente constan de dos ranuras o conectores, una junto a la otra. Una tarjeta de 8 bits podría estar en un slot de 16 bits, pero una de 16 bits no podría estar en una de 8 bits.

ISA fue la arquitectura estándar de equipos personales hasta que Compaq y otras compañías desarrollaron el bus EISA.

6.6.2 Arquitectura estándar ampliada de la industria (EISA)

Es el estándar de bus introducido en 1988 por una asociación de nueve compañías de la industria de los equipos: AST Research, Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse Technology y Zenith.

EISA ofrece un camino de datos de 32 bits y mantiene la compatibilidad con ISA, además de ofrecer una serie de características adicionales introducidas por IBM en su Bus de Arquitectura Micro Channel.

6.6.3 Arquitectura Micro Channel

En 1988, IBM introdujo este estándar al tiempo que se anunció su equipo PS/2. La arquitectura Micro Channel es física y eléctricamente incompatible con el bus ISA. A diferencia del bus ISA, las funciones Micro Channel son buses de 16 o 32 bits y se pueden controlar de forma independiente por varios procesadores de control (master) del bus.

6.6.4 Interconexión de componentes periféricos (PCI)

Es un bus local de 32 bits utilizado en la mayoría de los equipos Pentium y en las Apple Power Macintosh. La arquitectura de bus PCI actual posee la mayoría de los requerimientos para ofrecer la funcionalidad Plug and Play. Plug and Play es una filosofía de diseño y un conjunto de especificaciones de la arquitectura de un equipo personal. El objetivo de Plug and Play es permitir los cambios realizados en la configuración de un equipo personal, sin intervención del usuario.

6.7 Conectores y cableado de red

La tarjeta de red realiza tres funciones importantes coordinando las actividades entre el equipo y el cableado:

- Realiza la conexión física con el cable.
- Genera las señales eléctricas que circulan por el cable.
- Controla el acceso al cable siguiendo unas reglas específicas.

Para seleccionar la tarjeta de red apropiada para la red, primero es necesario determinar el tipo de cable y los conectores que tendrá.

Cada tipo de cable tiene características físicas diferentes, a las que la tarjeta de red debe adaptarse. Cada tarjeta se ha construido para aceptar al menos un tipo de cable. Actualmente el cable de par trenzado y el de fibra óptica son los tipos de cables más comunes.

Algunas tarjetas de red tienen más de un conector de interfaz. Por ejemplo, es común que una tarjeta de red tenga un conector Thinnet, uno Thicknet y uno para par trenzado.

Una conexión de par trenzado utiliza un conector RJ-45,. El conector RJ-45 es similar al conector telefónico RJ-11, pero tiene un tamaño mayor y tiene ocho conductores; un RJ-11 sólo tiene cuatro conductores.

6.8 Rendimiento de la red

Debido al efecto que causa en la transmisión de datos, la tarjeta de red produce un efecto bastante significativo en el rendimiento de toda la red. Si la tarjeta es lenta, los datos no se moverán por la red con rapidez. En una red en bus, donde no se puede utilizar la red hasta que el cable esté libre, una tarjeta lenta puede incrementar el tiempo de espera para todos los usuarios.

Después de identificar los requerimientos físicos de la tarjeta de red (el bus del equipo, el tipo de conector que necesita la tarjeta, el tipo de red donde operará), es necesario considerar otros factores que afectarán a las posibilidades de la tarjeta.

Aunque todas las tarjetas de red se ajustan a ciertos estándares y especificaciones mínimas, algunas características de las tarjetas mejoran de forma importante el servidor, el cliente y todo el rendimiento de la red.

Se puede incrementar la velocidad de los datos a través de la tarjeta incorporando las siguientes mejoras:

- Acceso directo a memoria (DMA). Con este método, el equipo pasa los datos directamente desde el búfer de la tarjeta de red a la memoria del equipo, sin utilizar el microprocesador del equipo.
- Memoria de tarjeta compartida. En este método, la tarjeta de red contiene RAM que comparte con el equipo. El equipo identifica esta RAM como si realmente estuviera instalada en el equipo.
- Memoria del sistema compartida. En este sistema, el procesador de la tarjeta de red selecciona una parte de la memoria del equipo y la utiliza para procesar datos.
- Bus mastering (Control de bus). Con el bus mastering, la tarjeta de red toma temporalmente el control del bus del equipo, evitando la CPU del equipo y llevando los datos directamente a la memoria del sistema del equipo. Esto incrementa la velocidad de las operaciones del equipo, liberando al procesador del equipo para realizar otras tareas. Las tarjetas con bus mastering pueden ser caras, pero pueden mejorar el rendimiento de la red de un 20 a un 70 por 100. Las tarjetas de red EISA, Micro Channel y PCI ofrecen bus mastering.
- RAM buffering. A menudo el tráfico en la red va demasiado deprisa para que la mayoría de las tarjetas de red puedan controlarlo. Los chips de RAM en la tarjeta de red sirven de búfer. Cuando la tarjeta recibe más datos de los que puede procesar inmediatamente, el buffer de la RAM guarda algunos de los datos hasta que la tarjeta de red pueda procesarlos. Esto acelera el rendimiento de la tarjeta y ayuda a evitar que haya un cuello de botella en la tarjeta.
- Microprocesador de la tarjeta. Con un microprocesador, la tarjeta de red no necesita que el equipo le ayude a procesar los datos. La mayoría de las tarjetas incorporan sus propios procesadores que aceleran las operaciones de la red.

6.9 Tarjetas de red especializadas

En la mayoría de las situaciones, bastará con utilizar tarjetas estándar para conectar el equipo con la red física, pero existen algunas situaciones que requieren el uso de conexiones de red especializadas y, por tanto, necesitarán tarjetas de red especializadas.

6.9.1 Tarjetas de red inalámbricas

Algunos entornos requieren una alternativa a las redes de equipo cableadas. Existen tarjetas de red sin hilos que soportan los principales sistemas operativos de red.

Las tarjetas de red inalámbricas suelen incorporar una serie de características. Éstas incluyen:

- Antena omnidireccional interior y cable de antena.
- Software de red para hacer que la tarjeta de red funcione en una red en particular.
- Software de diagnóstico para localización de errores.
- Software de instalación.

Estas tarjetas de red se pueden utilizar para crear una LAN totalmente sin inalámbricas, o para incorporar estaciones sin hilos a una LAN cableada.

Normalmente, estas tarjetas de red se utilizan para comunicarse con un componente llamad concentrador inalámbrico que actúa como un transceptor para enviar y recibir señales.

Un concentrador es un dispositivo de comunicaciones que combina señales de varias fuentes, como terminales en la red, en una o más señales antes de enviarlas a su destino.

6.9.2 Tarjetas de red de fibra óptica

Conforme la velocidad de transmisión aumenta para acomodarse a las aplicaciones con un gran ancho de banda y los flujos de datos multimedia son comunes en las intranets actuales, las tarjetas de red de fibra óptica permiten conexiones directas a redes de fibra óptica de alta velocidad. Recientemente, estas tarjetas han llegado a tener un precio competitivo, y su uso es cada vez más corriente.

6.10 PROM de inicialización remota

En algunos entornos, la seguridad es tan importante que las estaciones de trabajo no tienen unidades de disquete individuales. Sin éstas, los usuarios no pueden copiar la

información en un disquete o disco duro y, por tanto, no pueden sacar los datos de su lugar de trabajo.

Sin embargo, como los equipos normalmente se arrancan desde una unidad de disquete o desde un disco duro, tiene que existir otra fuente para que el software inicie (arranque) el equipo y lo conecte a la red. En estos entornos, la tarjeta de red puede ser equipada con un chip especial llamado PROM (memoria programable de sólo lectura) de inicialización remota que contenga el código que inicie el equipo y conecte al usuario a la red.

Con las PROM de inicialización remota, las estaciones de trabajo sin disco se pueden unir a la red cuando se inician. [R6]

CONCLUSIONES

De acuerdo a la investigación para desarrollar este trabajo y analizando cada uno de los aspectos necesarios para el uso de las redes de área local podemos concluir que:

El gran desarrollo que ha tenido la tecnología en el campo de la computación, sobre todo en el campo de la conectividad que son las redes, no nos da el tiempo suficiente para reflexionar acerca de las implicaciones que en todos los lugares sucederán por el impacto de éstos avances.

Diferentes disciplinas, tanto de las ciencias exactas, la administración, no solo se ven afectadas por el auxilio que proporcionan las nuevas herramientas de conectividad, sino que además el propio quehacer profesional está sufriendo cambios estructurales.

La arquitectura, la ingeniería, el diseño, la administración, la aviación son algunos ejemplos que podemos mencionar dentro del campo de aplicación de las redes. En estas carreras, las redes de área local, no solo proporcionan apoyo a través de los programas y equipos computacionales, sino que ésta se convierte en el mismo objeto de trabajo.

Este es el caso de los edificios inteligentes. La conectividad está determinando la tendencia que se debe considerar ya también en los diseños arquitectónicos y los proyectos de ingeniería civil, si quieres construir edificios modernos, que respondan a las nuevas necesidades de las organizaciones e instituciones. Ahora no basta diseñar edificios agradables funcionales y cómodos para el usuario. Se requiere también que sean lo suficientemente adaptables a los cambiantes requerimientos de comunicación que toda organización.

El profundo cuestionamiento que se plantea en el campo de las redes de área local en la competitividad de las empresas, es otro de caso de la influencia de las tecnologías computacionales en otros terrenos disciplinarios.

Para algunos el principal reto se encuentra no tanto en el establecimiento y soporte de una red de área local, sino en la interoperabilidad de aquellas que utilizan medios y protocolos distintos. De ahí la búsqueda de un fundamento común del cual partir. De nuevo una referencia de implantar estándares.

El decidir por una red y administrarla impone tareas de responsabilidades múltiples, ya que además de mantenerla en óptimas condiciones de funcionamiento debe elegir de entre una muy amplia gama de dispositivos, aquellos que le permitan el manejo justo de la red, sin caer en los extremos de hacer selecciones económicas que, por baratas, resulten insuficientes o de adquirir equipos sofisticados que, aunque costosos, no satisfacen las necesidades específicas de la empresa.

En resumen una red de área local posibilita:

- Una verdadera comunicación entre usuarios
- Compartir los recursos tanto software como hardware
- Organización de los grupos de trabajo
- Mejoras en la administración de los equipos y programas
- Mejoras en la integridad de datos
- Mayor seguridad para acceder a la información

GLOSARIO

- **Ancho de banda**

  Medida de la capacidad de un sistema de transmisión. Éste se mide en hertz.

- **ARPANET**

  Red pionera de gran alcance fundada por ARPA (Advanced Research Projects Agency) después DARPA. Sirvió de 1969 a 1990 como base para las primeras investigaciones de red durante el desarrollo de Internet. ARPANET consiste en nodos individuales conmutadores de paquetes interconectados por líneas arrendadas.

- **Cable coaxial**

  Cable usado por las redes de cómputo al igual que en la televisión por cable. El nombre se debe a su estructura; un blindaje metálico rodea a un alambre central. El blindaje protege la señal del alambre interior contra interferencias eléctricas.

- **Cliente**

  Cuando dos programas se comunican por una red, el cliente es el que inicia la comunicación, mientras que el programa que espera ser contactado es el servidor. Cualquier programa puede actuar como servidor para un servicio y como cliente para otro.

- **Conmutación de paquetes**

  Método que consiste en dividir toda la información que sale de un ordenador para ser trasmitida por la red en bloque de determinada longitud (Paquetes) que contienen la información relacionada con el origen y destino del paquete así como el orden que ocupa dentro de la división realizada. Esto permite que cada paquete se mueva de forma independiente en la red y al llegar a su

destino puedan ser reensamblados para construir nuevamente la información enviada.

- **Ethernet**

Tecnología de red de área local que usa una topología de bus y acceso CSMA/CD

- **Hardware** (maquinaria)

  Componentes físicos de una computadora o de una red, a diferencia de los programas o elementos lógicos que los hacen funcionar.

- **Hub** (concentrador)

  Dispositivo electrónico al que se conectan varios ordenadores, por lo general mediante un cable de par trenzado. Un concentrador simula en la red que interconecta a los ordenadores conectados.

- **Internet**

  Conjunto de redes para formar una sola red con una cobertura nacional e internacional

- **LAN (Local Área Network, red de área local)**

  Red que usa tecnología diseñada para abarcar un área geográfica pequeña. Por ejemplo la red Ethernet es una tecnología de LAN adecuada para uso dentro de un edificio.

- **Protocolo**

  Descripción formal de formatos de mensajes y reglas que dos o más ordenadores deben seguir para intercambiar mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de ordenador a ordenador o el intercambio entre programas de aplicación.

- **Sistema Operativo**

  Conjunto de programas o software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera eficiente.

- **Software**

  Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica de una computadora.

- **Switch** (interruptor o conmutador)

  Dispositivo de interconexión de redes de ordenadores. Un switch interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo con la dirección de destino de los datagramas en la red. Los switches se utilizan cuando se desea conectar múltiples redes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las mismas.

- **Token Ring (anillo)**

  Red de topología de anillo que se sirve del paso de testigo para el control de acceso. La frase también se aplica a una topología específica definida por IBM Corporation.

BILIOGRAFÍA

[R1] APUNTES DE REDES:_http://www.ignside.net/man/redes._junio, 2005
COMER, DOUGLAS E. Redes Globales de información con Internet y TCP/IP. Principios básicos, protocolos y arquitectura: T. I y II.—La Habana: Ed. Pueblo y Educación,2005

[R2] http://es.wikipedia.org/wiki/ARCNET

[R3] http://es.wikipedia.org/wiki/CSMA/CD

[R4] http://es.wikipedia.org/wiki/TOKENRING

[R5] http://fmc.axarnet.es/redes/tema_02.htm

[R6] FUNDAMENTOS DE REDES PLUS DE MICROSOFT. Edición 2001. Traductor Antonio Becerra Terón. Ed. McGrawHill

[R7] GIRALT VICTORIANO. Las Redes._ http://vgg.sci.uma.es/redes._marzo 2004
Introducción a los protocolos._http://fmc.axarnet.es/redes/tema_06.htm._enero 2002

[R8] Tutoriales para profesores (Microsoft Corporation)
http://www.tutorialparaprofesores.com/default.aspx

[R9] WALES, JIMMY. Wikipedia._ http://es.wikipedia.org/wiki/Topología_de red._mayo, 2001