UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“UTILIDAD DE LAS REDES LAN”

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

LUIS ALBERTO RAMÍREZ ARMADILLO

ASESOR:

M. en E. IMELDA DE LA LUZ FLORES DÍAZ

MEXICO **MAYO, 2010**

Algunas personas nunca aprenden nada, porque lo comprenden todo demasiado pronto.

Alexander Pope

Largo es el camino de la enseñanza por medio de teorías; breve y eficaz por medio de ejemplos.

Séneca

Un hombre sin estudio es un ser incompleto.

Simón Bolivar

La ambición sin conocimientos es como un barco fuera del agua.

Mark Lee

El éxito del perseverante es alcanzar sus metas sin sacrificar sus principios.

Roberto Palomo Cea

Ser o no ser; esta es la cuestión...

Shakespeare,William

El saber es la parte principal de la felicidad.

Sócrates

Después de escalar una montaña muy alta, descubrimos que hay muchas otras montañas por escalar.

Nelson Mandela

Vive como si fueras a morir mañana. Aprende como si fueras a vivir siempre.

Mohandas Gandhi

Todo parece imposible hasta que se hace.

Nelson Mandela

ÍNDICE

INTRODUCCIÓN

La presente tesis trata el tema de las redes de área local (LAN), iniciando con él los conceptos básicos que es necesario conocer para las mismas, así como también su historia, la comunicación de datos existente en ellas, el modelo OSI, el encapsulamiento de los datos, los tipos de redes, las topologías, la normalización, los tipos de cableado y el hardware utilizado para la instalación de las mismas.

Dándonos como resultado esto el alcance del objetivo del trabajo, el cual es que cualquier tipo de usuario pueda comprender con facilidad cada una de las utilidades de las redes LAN, así como la forma en que trabajan, se comunican y los dispositivos que se utilizan para que puedan funcionar correctamente.

En la presente tesis tenemos 4 capítulos, donde en el primero tratamos el tema de los “Conceptos básicos” donde se habla desde la evolución histórica de las redes, todos los protocolos que se deben de conocer para poder manejar una red LAN, la comunicación y transferencia de los datos y las 7 capas del modelo OSI.

En el segundo capítulo tratamos el tema de los “Tipos de redes y sus topologías” donde se habla de la clasificación de las redes en base a los criterios más importantes, la normalización y los organismos encargados de ella y se concluye el capitulo con los tipos de redes locales.

En el tercer capítulo tratamos el tema de “Hardware para redes” donde se habla de todos los medios de transmisión ya sean alámbricos o inalámbricos, los modos de transmisión que existen y se concluye con la comprensión del hardware para las redes.

En el cuarto capítulo se hace un “Comparativo de la utilidad de las diferentes redes LAN” donde se habla del comparativo de las diferentes arquitecturas, el comparativo de los diferentes tipos de transmisión, el comparativo de los

diferentes medios de transmisión y finalmente un comparativo entre las diferentes redes LAN rápidas y su descripción de estas tecnologías.

OBJETIVO GENERAL

Presentar los conceptos básicos y generales de las Redes de Área Local (LAN) así como los tipos de redes y sus topologías, el hardware utilizado para ellas y finalmente un comparativo de la utilidad de las diferentes redes de área amplia.

OBJETIVOS PARTICULARES

1. Presentar los conceptos básicos de las Redes de Área Local (LAN).

2. Analizar los tipos de redes.

3. Conocer y manejar la normalización y los organismos oficiales que existen.

4. Analizar los elementos inherentes a una Red de Área Local (LAN). Tales como sus Topologías y el Hardware utilizado en las redes.

5. Presentar la descripción y comparación de las Redes LAN.

JUSTIFICACIÓN

La presente investigación se justifica porque con ella se puede ayudar a los docentes y alumnos de todos los niveles educativos con una mejor, excelente y actualizada información de lo que es una red de área local (LAN).

La inspiración más importante de justificación es que como estudiante de la carrera de Ingeniería en Computación debo poner en práctica todo lo que con

esfuerzo de mis docentes y mío, logre aprender en el día a día en cada una de las aulas educativas.

Otro motivo de justificación es que con la presente investigación lograré conseguir experiencia, para que en el futuro pueda ser un excelente profesional y que pueda desempeñarme muy bien en cualquier ámbito ya sea laboral o académico.

CAPITULO I

CONCEPTOS BÁSICOS

1.1 EVOLUCIÓN HISTÓRICA DE LAS REDES

Antes de empezar a hablar de la evolución histórica de las redes tenemos que entender y comprender el concepto de red.

Red: Es un sistema de interconexión de ordenadores que permite compartir recursos e información.

También se puede definir como estructura formada por un conjunto de elementos tanto físicos como lógicos, con el fin de conseguir la interconexión de varias estaciones y poder así llevar la información de unas a otras.

Una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación[1].

Una red debe cumplir con lo siguiente:

- Un medio de comunicación donde transfiera información. Existen los medios inalámbricos e inalámbricos
- Un recurso que compartir Discos, impresoras, archivos, scanners, CD-ROMs, etc.
- Un lenguaje o reglas para comunicarse. Existen los protocolos de red: Ethernet, TCP/IP, X.25, IPX, etc.

También podemos clasificar a las redes en diferentes tipos, cada una de las clasificaciones se verán en el capitulo 2.

No es posible entender el estado actual de las telecomunicaciones y la transmisión de datos sin conocer cuál ha sido su evolución histórica y la sucesión de avances tecnológicos en la materia. Los primeros conceptos de

[1] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

redes aparecidos en el mundo de la informática se remontan al año 1983 y su evolución ha seguido un lento proceso de maduración.

La evolución de la tecnología ha posibilitado que la informática haya conseguido avances espectaculares en un tiempo relativamente corto. Desde la construcción de la primera computadora electrónica de propósito general durante la segunda guerra mundial (llamada ENIAC, construida por J. Presper Eckert y John Mauchly) hasta nuestros días apenas a transcurrido medio siglo.

De hecho, gran parte de los conceptos aplicados a los ordenadores actuales aparecen en un memorando escrito por John von Neumann en 1944.

El gran impulso a la informática se dio en 1961 cuando la empresa norteamericana Fairchild comercializó el primer circuito integrado. Hasta entonces, las computadoras se construían utilizando válvulas de vacío de gran tamaño (cilindros de 3 cm x 5 cm). Con esta revolución, las válvulas eran sustituidas por transistores integrados de menos de un milímetro cuadrado de tamaño.

Hasta 1977, todos los ingenieros estaban centrados en el diseño y construcción de supercomputadoras y maquinas más rápidas. En este mismo año, Steve Jobs y Steve Wozniak presentaron la computadora más barata y pequeña del mundo.

Otro elemento muy importante que ha sufrido una gran evolución en su concepción desde sus inicios es el programa informático. En sus inicios, se trataba de un conjunto de normas escritas en papel o tarjetas perforadas que indicaban como debían realizarse las conexiones internas de la circuitería del sistema. Estas normas expresaban el tipo de proceso que debía realizarse con la información.

Los diseñadores pronto se dieron cuenta de la existencia de un conjunto de fragmentos de programas que se repetían siempre en todas las aplicaciones: rutinas para lecturas de datos, chequeo del sistema, etc. Esos fragmentos

comenzaron a archivarse para copiarlos en nuevos programas, lo que dio lugar a lo que se conoce actualmente como sistema operativo. Este programa se utiliza fundamentalmente para ayudar a programar el sistema y facilitar el uso del mismo.

El primer elemento aparecido con el objetivo de compartir dispositivos fue el conmutador ABC. Se trata de una especie de interruptor que permite conectar dos canales de comunicación (que normalmente son conexiones de puerto paralelo). Con este dispositivo, dos ordenadores pueden compartir el uso de un dispositivo, como una impresora, o también se permite que dos dispositivos sean compartidos por un mismo ordenador. Las limitaciones son obvias: tanto en numero de dispositivos y equipos, como en la necesidad de pelearse con un mecanismo completamente manual para seleccionar el dispositivo u ordenador, además de que no permite que se compartan otros elementos físicos, como los discos duros.

Para solucionar los problemas anteriores, los ordenadores empezaron a dotarse de puertos en serie de comunicaciones. A partir de estos puertos, se podían conectar directamente varios equipos, y podía configurarse uno de ellos con el propósito de compartir el espacio de su disco duro con el resto. Todos los ordenadores veían ese disco como una unidad local, y no existían restricciones acerca de su uso.

Paralelamente a la evolución de la informática, desde 1876 (año en el que Alexander Graham. Bell invento el teléfono) también se dio un gran desarrollo de las comunicaciones terrestres, con el auge de las compañías telefónicas[2].

En 1957 se lanzo el primer satélite artificial (Sputnik I), y las comunicaciones en la tierra se han ido mejorando gracias a la utilización de los satélites que orbitan alrededor de nuestro planeta. La fusión posterior de las computadoras y las comunicaciones ha tenido una profunda influencia en la forma de organización de los sistemas informáticos.

[2] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

Entre 1983 y 1984 surgieron los primeros entornos servidores de ficheros para redes de área local. Entre las compañías destacadas, cabe citar a Novell Inc., 3Com Corp., AT&T e IBM. Aunque todas ellas diferían en la gestión e implementación, se trataba de entornos centralizados, donde un ordenador hacía las veces de servidor (con el sistema operativo de red instalado en él y los datos compartidos) y el resto de equipos funcionaban con una versión de sistema operativo más "ligero", como MS DOS. Hacia 1990, este tipo de redes locales triunfo en el mundo de la empresa y la industria de las redes creció a velocidades impresionantes.

Hoy en día, las redes de ordenadores son algo más que un entorno centralizado de gestión de ficheros. El desarrollo de la tecnología ha posibilitado el incremento en velocidad de transmisión y fiabilidad, lo que ha supuesto una extensión en sus capacidades. La principal tiene que ver con las redes de altas prestaciones, donde una aplicación compleja se ejecuta de forma distribuida en los equipos de la red. La tendencia actual se orienta hoy en día hacia las redes distribuidas (en lugar de centralizadas) donde cada ordenador es cliente, pero también puede ser servidor de datos o dispositivos.

La moderna tecnología digital permite que diferentes sectores, como por ejemplo telecomunicaciones, datos, radio y televisión se fusionen en uno solo[3].

Esta circunstancia, conocida comúnmente como convergencia, está ocurriendo a escala global y está cambiando drásticamente la forma en que se comunican tanto las personas como los dispositivos. En el centro de este proceso, formando la red troncal y haciendo posible la convergencia, están las redes IP.

Los servicios y los dispositivos integrados de los consumidores para propósitos como son telefonía, entretenimiento, seguridad e informática personal se están desarrollando constantemente y están siendo diseñados y convergen hacia un estándar de comunicación que es independiente de la conexión física subyacente.

[3] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

1.2 PROTOCOLOS TCP/IP

Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red[4].

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre computadoras de cualquier tipo de red o fabricante, respetando los protocolos de cada red individual.

Los protocolos TCP/IP se estructuran en 5 niveles funcionales:

APLICACIÓN
TRANSPORTE
INTERNET
RED
FÍSICO

Tabla. 1.1 Protocolos TCP/IP

- **El nivel físico:** corresponde al hardware. Puede ser un cable coaxial, un cable par trenzado, cable de fibra óptica o una línea telefónica. TCP/IP no considera oficialmente el nivel físico como componente especifico de su modelo y tiende a agrupar el nivel físico con el nivel de red. Los protocolos principales de este nivel son: ARP y RARP.

- **El nivel de red:** Independientemente del medio físico que se utilice, necesitara una tarjeta de red especifica que, a su vez, dependerá de un software llamado controlador de dispositivo proporcionado por el sistema operativo o por el fabricante. Proporciona fiabilidad (aunque no necesariamente) en la distribución de datos que pueden adoptar diferentes formatos. Aunque TCP/IP no especifica ningún protocolo para este nivel, los protocolos más notables son: SLIP, PPP y PPTP.

[4] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

- **El nivel Internet:** se superpone a la red física creando un servicio de red virtual independiente de aquella. No es fiable ni orientado a conexión. Se encarga del direccionamiento y encaminamiento de los datos hasta la estación receptora. El protocolo específico de este nivel es IP.

- **El nivel de transporte:** suministra a las aplicaciones servicios de comunicaciones desde la estación emisora a la receptora. Utiliza dos tipos de protocolos: TCP que es fiable y orientado a conexión y UDP que no es fiable y no orientado a conexión.

- **El nivel de aplicación:** corresponde a las aplicaciones disponibles para los usuarios como pueden ser: FTP, SNMP, TELNET. etc.

Estos niveles se corresponden con los del modelo de referencia OSI de la siguiente manera:

TCP/IP	OSI
	APLICACIÓN
	PRESENTACIÓN
APLICACIÓN	SESIÓN
TRANSPORTE	TRANSPORTE
INTERNET	RED
RED	ENLACE DE DATOS
FÍSICO	FÍSICO

Tabla 1.2

Esta correspondencia es teórica por que, como los protocolos TCP/IP fueron desarrollados antes que el modelo de referencia OSI, existen sustanciales diferencias, como son:

- **El concepto de jerarquía en relación con los niveles.** Indica que una tarea de comunicaciones se divide en entidades que pueden comunicar

con otras entidades pares en otro sistema. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras. Estas entidades deben tener una relación jerárquica, de manera que una entidad solo utilice los servicios de las entidades jerárquicamente inferiores. La diferencia entre ambos modelos es consecuencia del pragmatismo con el que se desarrollaron los protocolos TCP/IP, ya que estos proporcionan a los diseñadores mayor grado de libertad para la utilización de uno u otro; mientras que OSI es más prescriptito, ya que dicta los protocolos de un nivel determinado que deben realizar unas funciones específicas.

- **La interoperación de redes.** Ya que los protocolos TCP/IP se han concebido para interconectar sistemas no conectados a la misma red.

- **La fiabilidad extremo a extremo.** El protocolo IP no es fiable, es decir, no garantiza que los paquetes entregados sean correctos y que conserven la secuencia con que fueron emitidos, ya que supone que son los protocolos de transporte los que deben garantizarlo.

- **Los servicios no orientados a conexión.** El protocolo IP tampoco es orientado a conexión, ya que esta debe proporcionarse en niveles superiores.

- **La gestión de red.** En los primeros documentos del modelo OSI no se contemplaban las funciones de gestión y, aunque actualmente ya se contemplan, no alcanzan el nivel de aceptación de los de TCP/IP.

1.2.1 PROTOCOLOS DEL NIVEL FÍSICO

Aunque TCP/IP no considera oficialmente el nivel físico como componente especifico de su modelo y tiende a agrupar el nivel físico con el nivel de red, se van a describir en este apartado los protocolos ARP y RARP.

ARP (Address Resolution Protocol) es un protocolo que se utiliza para convertir las direcciones IP en direcciones físicas que puedan ser utilizadas por los manejadores.

Para poder realizar esta conversión, existe en cada computadora un módulo ARP que utiliza una tabla de direcciones ARP, que en la mayoría de las computadoras trata como si fuera una memoria intermedia (caché), de forma que la información que lleva mucho tiempo sin utilizarse se borra.

Si encuentra la correspondencia entre la dirección IP y la dirección física se procede a la transmisión[5].

Si no la encuentra en la tabla, se genera una petición ARP que se difunde por toda la red. Si alguna de las computadoras de la red reconoce su propia dirección IP en la petición ARP, envía un mensaje de respuesta indicando su dirección física y se graba en la tabla de direcciones ARP.

RARP (Reverse Address Resolution Protocol) se utiliza cuando, al producirse el arranque inicial, las computadoras no conocen su dirección IP.

Requiere que exista en la red, al menos, un servidor RARP. Cuando una computadora desea conocer su dirección IP, envía un paquete que contiene su propia dirección física.

El servidor RARP, al recibir el paquete, busca en su tabla RARP la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete a la computadora origen con esta información.

A diferencia del protocolo ARP que se incorpora normalmente en los productos TCP/IP, el protocolo RARP solo se incorpora en unos pocos productos.

[5] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

1.2.2 PROTOCOLOS DEL NIVEL DE RED

Aunque TCP/IP no especifica ningún protocolo para este nivel, se van a describir los protocolos SLIP y PPP[6].

SLIP (Serial-Line Internet Protocol) es, históricamente, el primero desarrollado para satisfacer la necesidad de establecer una conexión TCP/IP empleando únicamente una línea serie.

La utilización actual más común de este protocolo es la conexión (a Internet, por ejemplo) a través de una línea telefónica aunque también puede utilizarse para conectar dos computadoras próximas mediante un cable serie.

Se describe en el RFC 1055 y es un mecanismo muy sencillo de transmisión de paquetes. De hecho, su único cometido es el envió de datagramas en formato IP a través de una línea serie.

Sus inconvenientes más significativos son los siguientes:

- Carece de métodos de corrección de errores, delegando estas funciones en las capas superiores del software.

- Es incapaz de realizar tareas de gestión de enlace.

- Carece de métodos de autentificación.

- Es incapaz de negociar parámetros fundamentales de la comunicación (direcciones de red, tamaño de los paquetes o el empleo de algoritmos de compresión de datos). Todas estas características deben establecerse antes de efectuar la conexión, y deben coincidir en ambos extremos de enlace.

[6] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

Existe una versión de SLIP denominada CSLIP que, según las recomendaciones del RFC 1144 es capaz de comprimir las cabeceras TCP, con el aumento de eficiencia que esto supone por la menor cantidad de datos que es preciso transmitir.

PPP (Point-to-Point Protocol) es un protocolo SLIP mejorado con control y recuperación de errores.

Funcionalmente, es mucho más completo y robusto que SLIP. Además de asumir todas sus funciones, incorpora múltiples mejoras:

- Es posible negociar el tamaño máximo de los paquetes entre los dos extremos o la utilización de técnicas de compresión.
- Existe posibilidad de autentificación.
- Puede monitorizarse la calidad del enlace.

Una característica que hace a PPP aun mas interesante es la posibilidad de conexión a través de RDSI.

Existe una gran cantidad de software comercial y de dominio publico disponible para PPP.

PPTP (Point to Point Tunneling Protocol) no es un protocolo propio de TCP/IP, se va a describir en esta sección, ya que es un nuevo protocolo de red, incorporado en windows, que utiliza redes privadas multiprotocolo para permitir a los usuarios remotos tener acceso de forma segura, a través de Internet, a redes de empresas (Extranet).

Ofrece las siguientes ventajas:

- **Costes de transmisión más bajos.** Ya que usa Internet para la conexión en lugar de una llamada normal a través de la línea telefónica.

- **Menores costos de hardware.** Ya que permite separar los módems y las tarjetas RDSI, así como colocarse en un servidor de comunicaciones.

- **Mayor nivel de seguridad.** Funciona con cifrado de datos y actúa con cualquier protocolo.

Los datos enviados por PPTP se encapsulan en paquetes PPP cifrados que se envían a través de Internet. Pero también, puede ser usado para transportar el tráfico de acceso remoto IPX y NetBEUI.

1.2.3 PROTOCOLOS DEL NIVEL INTERNET

En este nivel se encuentran los protocolos ICMP e IP[7].

ICMP (Internet Control Message Protocol) es un protocolo de mantenimiento/gestión de red que ayuda a supervisar la red.

Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

El objetivo principal de ICMP es proporcionar la información de error o control entre nodos. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP.

Los mensajes de error de este protocolo normalmente los genera y los procesa TCP/IP y no el usuario.

Existen cuatro tipos de mensajes ICMP:

- Mensajes de destino no alcanzable.
- Mensajes de control de congestión.
- Mensajes de redireccionamiento.

[7] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

- Mensajes de tiempo excedido.

Una de las utilidades de diagnostico que utiliza este protocolo es la utilidad PING (se utiliza para comprobar si un equipo esta conectado a la red).

IP (Internet Protocol) Se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por donde se deben de encaminar los datagramas salientes pudiendo llevar a cabo tareas de fragmentación y reensamblado.

Este protocolo, que no es fiable ni esta orientado a conexión, no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

IP no se encarga de controlar que sus datagramas, que envía a través de la red, puedan perderse, llegar desordenados o duplicados. Para ello, tendrán que ser contempladas por protocolos del nivel de transporte.

Los datagramas IP contienen una cabecera con información para el nivel IP y datos. Estos datagramas se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada.

Cuando los datagramas viajan de unos equipos a otros pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Unidad Máxima de Transmisión) y ninguna red puede transmitir ningún paquete cuya longitud exceda del MTU de dicha red.

Debido a este problema, es necesario reconvertir los datagramas IP en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina fragmentación y reensamblado.

La fragmentación divide los paquetes en fragmentos de menor longitud (se realiza en el nivel mas inferior posible y de forma transparente al resto de los niveles) y el reensamblado realiza la operación contraria.

1.2.4 PROTOCOLOS DEL NIVEL DE TRANSPORTE

En este nivel se encuentran los protocolos TCP y UDP[8].

TCP (Transmisión Control Protocol) es un protocolo orientado a conexión que utiliza los servicios del nivel Internet.

Al igual que cualquier protocolo orientado a conexión consta de tres fases:

1. **Establecimiento de la conexión.** Se indica con el intercambio de tres mensajes, garantiza que los dos extremos de transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iniciales de secuencia (cada extremo elige un numero de forma aleatoria).

2. **Transferencia de los datos.** La unidad de datos que utiliza es el segmento y su longitud se mide en octetos. La transmisión es fiable ya que permite la recuperación ante datos perdidos, erróneos o duplicados, así como garantiza la secuencia de entrega, para lo que se añade a la cabecera del segmento de datos un numero de secuencia y un código de control. La fiabilidad de la recepción se consigue mediante la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.

3. **Liberación de la conexión.** Cuando una aplicación comunica que no tiene más datos que transmitir, TCP finaliza la conexión en una dirección. Desde ese momento, TCP no vuelve a enviar datos en ese

[8] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

sentido, permitiendo que los datos circulen en el sentido contrario hasta que el emisor cierra también esa conexión.

TCP permite multiplexación, es decir, una conexión TCP puede ser utilizada simultáneamente por varios usuarios.

Como normalmente existe más de un proceso de usuario o aplicación utilizando TCP de forma simultanea, es necesario identificar los datos asociados a cada proceso. Para ello, se utilizan los puertos. Un puerto es una palabra de 16 bits que identifica hacia que aplicación o proceso han de dirigirse los datos.

Hay aplicaciones que tienen asignado el mismo numero de puerto, ya que realizan funciones de servidores normalizados que utilizan los servicios TCP/IP.

Estos puertos reservados se encuentran en el archivo SERVICES que se encuentra en el directorio ETC y corresponden a números superiores a 1, indicando también si corresponden al protocolo TCP o UDP.

Algunos ejemplos de puertos son los expuestos en la tabla 1.3:

N° de puerto	**Servicio**
21	FTP
23	TELNET
25	SMTP
69	TFTP
111	RFC
161	SNMP

Tabla 1.3

Un socket esta compuesto por un par de números que identifican de manera única a cada aplicación. Cada socket se compone de dos campos:

1. La dirección IP de la computadora en la que se esta ejecutando la aplicación.

2. El puerto a través del cual la aplicación se comunica con TCP/IP.

UDP (User Datagram Protocol) es un protocolo que se basa en el intercambio da datagramas. UDP permite el envió de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El inconveniente de esta forma de actuación es que no hay confirmación de recepción ni de haber recibido los datagramas en el orden adecuado, debiendo ser la aplicación la que se encargue de controlarlo.

Al igual que el protocolo TCP, utiliza puertos y sockets y, también, permite la multiplexación.

1.2.5 PROTOCOLOS DEL NIVEL DE APLICACIÓN

Todas las aplicaciones TCP/IP utilizan el modelo cliente/servidor[9].

En este nivel se encuentran un buen número de protocolos de los cuales se van a describir los siguientes: FTP, HTTP, NFS, NTP, RPC, SMTP, SNMP, TELNET y TFTP.

FTP (File Transfer Protocol) es el mas utilizado de todos los protocolos de aplicación y uno de los mas antiguos.

Se utiliza para la transferencia de archivos proporcionando acceso interactivo, especificaciones de formato y control de autentificación (aunque es posible conectarse como el usuario anonymous que no necesita contraseña).

[9] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

HTTP (HyperText Transfer Protocol) es uno de los protocolos mas recientes. Se utiliza para manejar la consulta de hipertexto y el acceso de datos con World Wide Web (WWW). El tráfico generado por este protocolo ha pasado, debido a la influencia de Internet, a ser muy grande.

NFS (Network File System) ha sido desarrollado por Sun Microsystems Incorporated y autoriza a los usuarios el acceso en línea a archivos que se encuentran en sistemas remotos (accede a un archivo remoto como si se tratara de un archivo local). La mayoría del tráfico NFS es ahora un caso especial del protocolo RPC.

NTP (Network Time Protocol) permite que todos los sistemas sincronicen su hora con un sistema designado como servidor horario.

RPC (Remote Procedure Call) es una llamada a un procedimiento que se ejecuta en un sistema diferente del que realiza la llamada.

El proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Este, al recibir la llamada, estudia los procedimientos del proceso llamado, obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta.

Existen dos tipos de servidores:

1. **El servidor iterativo** que recibe una llamada proporciona el servicio y vuelve al estado de espera.

2. **El servidor concurrente** que recibe la llamada contesta al mensaje enviado al cliente un número de puerta, arranca un proceso paralelo para prestar el servicio requerido por el cliente y vuelve al estado de espera. Cuando el proceso paralelo haya finalizado el servicio requerido, acaba su ejecución.

SMTP (Simple Mail Transfer Protocol) es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente debe enviar desde una computadora al servidor de otra, pero no especifica como debe almacenarse el correo ni con que frecuencia se debe intentar el envió de los mensajes.

SNMP (Simple Network Management Protocol) sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el trafico de la red desde una o varias estaciones de trabajo llamadas administradores SNMP.

Los elementos de la red que puede administrar y monitorizar son dispositivos como computadoras, puertas de enlace (gateways), encaminadotes (routers), mainframes, hubs, etc.

SNMP minimiza el número y la complejidad de las funciones realizadas por el administrador y cuenta con las siguientes ventajas:

- Reduce el coste de desarrollo de software del agente de administración necesario para soportar este protocolo.

- Aumenta el grado de las funciones de administración utilizadas de forma remota, permitiendo un uso completo de los recursos de Internet en dichas tareas.

- Permite que las funciones de administración sean de fácil comprensión y uso por parte de los desarrolladores de herramientas de administración de la red.

Utiliza una arquitectura distribuida que consiste en agentes y sistemas de administración.

- Un agente es una computadora que ejecuta el software de agente SNMP o un encaminador.

La obligación principal de un agente es ejecutar las tareas indicadas por los comandos SNMP que han sido requeridas por un sistema de administración.

Los comandos SNMP que se utilizan pertenecen a los tipos siguientes:

- **GetRequest:** Este es el comando que utiliza el sistema de administración para solicitar información a un agente.

- **GetNextRequest:** También es empleado por el sistema de administración para solicitar información al agente y se utiliza si la información deseada se encuentra en forma de tabla o matriz (se usa en forma repetitiva hasta que se hayan conseguido todos los datos de la matriz).

- **GetResponse:** El agente consultado utiliza este comando para contestar una solicitud hecha por el sistema de administración.

- **SetRequest:** El sistema de administración lo utiliza para cambiar el valor de un parámetro del MIB (Management Information Base).

- **Trap:** Este comando lo utiliza un agente para informar al sistema de administración de un suceso determinado que se ha producido.

- Un **sistema de administración** es una computadora que ejecuta un software de administración SNMP. Puede iniciar las operaciones de los comandos GetRequest, GetNextRequest y SetRequest.

Un agente únicamente puede iniciar el comando Trap para informar al sistema de administración de un suceso extraordinario y contestar al sistema de administración con el comando GetResponse.

La forma en la que actúa el protocolo SNMP es la siguiente:

1. El sistema de administración envía primero una solicitud al agente para obtener el valor de una variable de MIB.

2. El agente contesta a la solicitud en función del nombre de la comunidad que acompaña a la solicitud.

Una comunidad comprende un grupo de computadoras que ejecutan el servicio SNMP. El uso de un nombre de comunidad proporciona una seguridad mínima para los agentes que reciben solicitudes e inician capturas (traps) así como para las tareas iniciadas por los sistemas de administración.

Un agente no responderá a una solicitud de un sistema de administración distintos a aquellos que tenga configurados (un agente puede pertenecer a varias comunidades a la vez).

MIB describe los objetos que están incluidos en la base de datos de un agente SNMP.

Los objetos que haya en MIB deben estar definidos para que los desarrolladores de software para la administración de las estaciones de trabajo los conozcan, así como sus valores respectivos.

MIB registra y almacena información sobre la computadora en la que se esta ejecutando. Un administrador SNMP puede solicitar y recoger información de un agente MIB así como revisar o alterar los objetos que contiene.

TELNET permite que un usuario, desde un Terminal, acceda a los recursos y aplicaciones de otras computadoras.

Una vez que la conexión queda establecida, actúa de intermediario de ambas computadoras.

Se fundamenta en tres principios:

- **El concepto de Terminal virtual de red (NVT).** Corresponde a la definición de cómo han de ser los datos, caracteres de control y las secuencias de los mandatos que han de circular por la red para permitir una heterogeneidad de los sistemas.

- **La simetría entre terminales y procesos.** La comunicación puede ocurrir entre dos terminales, dos procesos o entre un Terminal y un proceso.

- **Permite que el cliente y el servidor negocien sus opciones.** La conexión comienza con una fase de negociación de opciones en las que se utilizan cuatro mandatos: WILL, WONT, DO y DONT.

WILL se envía para mostrar el deseo de comenzar una opción (que se ha de indicar) y se contesta con DO (respuesta positiva) o DONT (respuesta negativa).

WONT se envía para mostrar el deseo de no comenzar una opción (que se ha de indicar) y se contesta con DONT (mostrando el acuerdo de no utilización).

DO se envía para indicar que comience a utilizar una opción (que se a de indicar) y se contesta con WILL (respuesta positiva) o WONT (respuesta negativa).

DONT se envía para indicar que no comience a utilizar una opción (que se a de indicar) y se contesta con WONT (mostrando el acuerdo de no utilización).

TFTP es un protocolo destinado a la transferencia de archivos aunque sin permitir tanta interacción entre cliente y servidor como la que existe en FTP.

Además, existe otra diferencia, en lugar de utilizar el protocolo TCP, utiliza UDP.

Sus reglas son muy sencillas. En el envió del primer paquete se establece una interacción entre cliente y servidor.

Se empieza una numeración de los bloques (empezando desde 1). Cada paquete de datos contiene una cabecera que especifica el bloque que contiene. Un bloque de menos de 512 bytes indica que es el último y corresponde al final del archivo.

1.3 INTRODUCCIÓN A LA COMUNICACIÓN DE DATOS

Internet se ha convertido en el factor más potente que guía el proceso de convergencia. Esto es debido principalmente al hecho de que la suite del protocolo Internet se ha erigido como un estándar utilizado en casi cualquier servicio.

La suite del protocolo Internet está compuesto principalmente por el protocolo Internet (IP), y el protocolo de control del transporte (TCP); consecuentemente el término TCP/IP refiere a la familia del protocolo al completo.

Las redes basadas en IP tienen una gran importancia en la sociedad de la información actual.

A primera vista esta tecnología puede parecer un poco confusa y abrumadora pero empezaremos por presentar los componentes de red subyacentes sobre los que está construida esta tecnología.

Una red se compone de dos partes principales, los nodos y los enlaces. Un nodo es cualquier tipo de dispositivo de red como un ordenador personal. Los nodos pueden comunicar entre ellos a través de enlaces, como son los cables.

Hay básicamente dos técnicas de redes diferentes para establecer comunicación entre dos nodos de una red: las técnicas de redes de conmutación de circuitos y las de redes de conmutación de paquetes.

La primera es la más antigua y es la que se usa en la red telefónica y la segunda es la que se usa en las redes basadas en IP.

Una red de conmutación de circuitos crea un circuito cerrado entre dos nodos de la red para establecer una conexión. La conexión establecida está dedicada a la comunicación entre los dos nodos. Uno de los problemas inmediatos de los circuitos dedicados es la pérdida de capacidad, dado que casi ninguna transmisión usa el 100% del circuito todo el tiempo.

Además, si un circuito falla en el medio de una transmisión, la conexión entera se pierde y debe establecerse una nueva.

Por otra parte las redes basadas en IP utilizan la tecnología de conmutación de paquetes, que usa la capacidad disponible de una forma mucho más eficiente y que minimiza el riesgo de posibles problemas como la desconexión. Los mensajes enviados a través de una red de conmutación de paquetes se dividen primero en paquetes que contienen la dirección de destino.

Entonces, cada paquete se envía a través de la red y cada nodo intermedio o router de la red determina a donde va el paquete. Un paquete no necesita ser enrutado sobre los mismos nodos que los otros paquetes relacionados. De esta forma, los paquetes enviados entre dos dispositivos de red pueden ser transmitidos por diferentes rutas en el caso de que se caiga un nodo o no funcione adecuadamente.

Para que dos ordenadores puedan intercambiar información, es necesario que existan unos dispositivos que la transporten desde el equipo origen al destino.

1.3.1 CONCEPTOS BASICOS

Desde los primeros tiempos de la informática, en un ordenador se han distinguido dos partes fundamentales: el hardware y el software. Aunque estas dos palabras se usan ampliamente, quizá sea preferible utilizar sus

equivalentes en castellano: dispositivos y programas. Si realizamos la comparación con el ser humano, estos conceptos podrían corresponder al cuerpo y al alma de la persona.

Todos los dispositivos de un ordenador son “elementos físicos”, es decir, todo aquello que resulta visible y tangible en el mundo real. Ejemplos de dispositivos físicos son el teclado, la pantalla, etc.

Por su parte, los programas de un ordenador definen su comportamiento: constan de información (datos) y ciertas operaciones definidas que le indican la forma de manipular esos datos. Estos programas no existen en la realidad, aunque están almacenados en la memoria del ordenador como unos y ceros (en realidad, como tensiones eléctricas). Aunque no son tangibles, su importancia radica en el hecho de que los programas controlan a todos los dispositivos del ordenador[10].

- **Dispositivos de red:** Se corresponde con el conjunto de elementos físicos que hacen posible la comunicación entre el emisor y el receptor. Estos dispositivos son:

- **Canal de comunicación:** Es el medio por el que circula la información.

- **Nodos intermedios:** Son los elementos encargados de realizar la selección del mejor camino por el que circulara la información (en caso de que exista mas de un camino). También funciona como emisores o receptores y, en este caso, se asemejan más a un teléfono, ordenador o fax.

- **Programas de red:** A este tipo pertenecen todos los programas que permiten controlar el funcionamiento de la red, para hacerla mas fiable. Las primeras redes de computadoras se diseñaron pensando en los dispositivos y dejando en un segundo plano los programas: hoy en dia el software de redes es un elemento muy importante y esta altamente estructurado

[10] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

El nivel básico de información por computador se compone de dígitos binarios o bits (0 y 1). Los computadores que envían uno o dos bits de información, sin embargo, no serían demasiado útiles, de modo que se necesitan otras agrupaciones: los bytes, kilobytes, megabytes y gigabytes. Para que los computadores puedan enviar información a través de una red, todas las comunicaciones de una red se inician en el origen, luego viajan hacia su destino.

La información que viaja a través de una red se conoce como paquete, datos o paquete de datos (vease en la figura 1.1). Un paquete de datos es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación.

Incluye la información de origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los dispositivos de destino. La dirección origen de un paquete especifica la identidad del computador que envía el paquete. La dirección destino específica la identidad del computador que finalmente recibe el paquete.

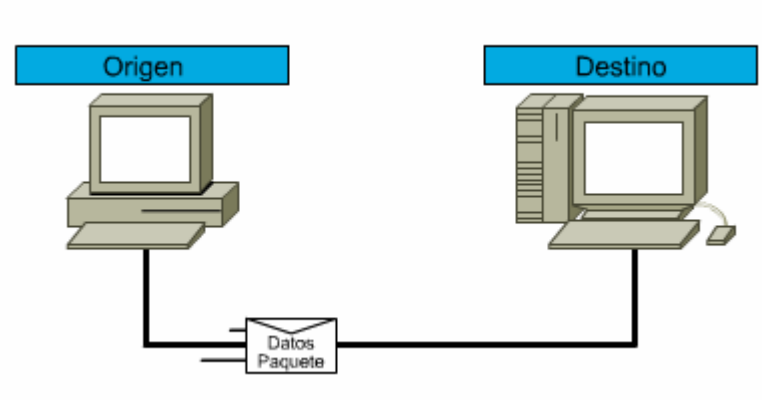

Figura 1.1 Comunicación en red

1.3.2 Fundamentos de transmisión

Las soluciones de redes basadas en IP son sustitutos flexibles y económicos para soluciones que utilizan tecnologías de red antiguas. Las diversas

propiedades entre estas tecnologías consisten en como se representa, gestiona y transmite la información.

La información se estructura simplemente en colecciones de datos y entonces tiene sentido para la interpretación que le damos. Hay dos tipos principales de datos, analógicos y digitales y ambos poseen diferentes características y comportamientos.

Los datos analógicos se expresan como ondas continuas variables y por tanto representan valores continuos. Los ejemplos incluyen la voz y el vídeo.

Por otra parte los datos digitales se representan como secuencias de bits, o de unos y ceros.

Esta digitalización permite que cualquier tipo de información sea representada y medida como datos digitales. De esta forma, el texto, sonidos e imágenes pueden representarse como una secuencia de bits. Los datos digitales pueden también comprimirse y puede ser encriptada para su transmisión segura.

Además una señal digital es exacta y ningún tipo de ruido relacionado puede filtrarse. Los datos digitales pueden ser transmitidos a través de tres tipos generales de medios: metal, como es el cobre, fibra óptica u ondas de radio.

Las técnicas representadas debajo ofrecen el primer bloque de construcción para las comunicaciones digitales, el nivel de cable y antena. Este nivel nos permite enviar y recibir datos digitales sobre una amplia variedad de medios. En todo caso, se precisan más bloques de construcción para las comunicaciones digitales seguras.

1.4 MODELO DE REFERENCIA OSI

El modelo OSI (Open Systems Interconnection, “Interconexión de Sistemas Abiertos”) esta basado en una propuesta establecida en el año 1983 por la organización internacional de normas ISO (ISO 7498) como un avance hacia la

normalización a nivel mundial de protocolos. El modelo se llama modelo de referencia OSI de la ISO, puesto que se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están preparados para la comunicación con otros diferentes.

OSI emplea una arquitectura en niveles a fin de dividir los problemas de interconexión en partes manejables. Posteriores estándares de ISO definieron las implementaciones en cada nivel para asegurar que se consigue una compatibilidad entre equipos diferentes.

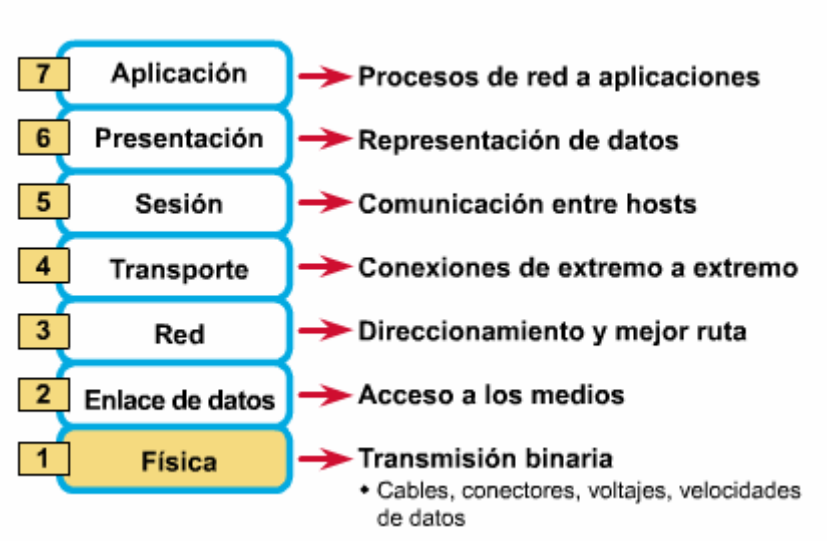

Figura 1.2 Las siete capas del modelo OSI.

Los principios teóricos en los que se basaron para la realización de OSI fueron[11]:

✓ Cada capa de la arquitectura esta pensada para realizar una función bien definida.

✓ El número de niveles debe ser suficiente para que no se agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.

[11] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

✓ Debe crearse una nueva capa siempre que se necesite realizar una función bien diferenciada del resto.

✓ Las divisiones en las capas deben establecerse en forma que se minimice el flujo de información entre ellas, es decir, que la interfaz sea mas sencilla.

✓ Permitir que las modificaciones de funciones o protocolos que se realicen en una capa no afecten a los niveles contiguos.

✓ Utilizar la experiencia de protocolos anteriores. Las fronteras entre niveles deben situarse donde la experiencia ha demostrado que son convenientes.

✓ Cada nivel debe interaccionar únicamente con los niveles contiguos a el (es decir, el superior y el inferior).

✓ La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

OSI esta definido más bien como un modelo, y no como una arquitectura. La razón principal es que la ISO definió solamente la función general que debe realizar cada capa, pero no menciono en absoluto los servicios y protocolos que se deben usar en cada una de ellas. Esto quiere decir que, al contrario que el resto de arquitecturas de redes, el modelo OSI se definió antes que se diseñaran los protocolos.

Las funciones encomendadas a cada una de las capas de OSI son las siguientes[12]:

[12] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

- **Nivel Físico:** Tiene que ver con la transmisión de dígitos binarios por un canal de comunicación. Las consideraciones de diseño tienen que ver con el propósito de asegurarse de que, cuando un lado envié un “1” se reciba en el otro lado como “1”, no como “0”. Aquí las consideraciones de diseño tienen mucho que ver con las interfases mecánica, eléctrica y de procedimientos, y con el medio de transmisión físico que esta bajo la capa física.

- **Nivel de Enlace:** Su tarea principal es detectar y corregir todos los errores que se produzcan en la línea de comunicación. También se encarga de controlar que un emisor rápido no sature a un receptor lento, ni se pierdan datos innecesariamente. Finalmente, en redes donde existe un único medio de compartido por el que circula la información, este nivel se encarga de repartir su utilización entre las estaciones. La unidad misma de datos que se transfiere entre entidades pares a este nivel se llama trama o marco.

- **Nivel de Red:** Se ocupa de determinar y selecciona cual es la mejor ruta y debe controlar también la congestión de la red, intentando repartir la carga lo mas equilibrada posible entre las distintas rutas. También a este nivel se realiza gran parte del trabajo de convertir y adaptar los mensajes que circulan entre redes heterogéneas. La unidad misma de información que se transfiere a este nivel se llama paquete.

- **Nivel de Transporte:** Es el nivel mas bajo que tiene independencia total del tipo de red utilizada, y su función básica es tomar los datos procedentes del nivel de sesión y pasarlos a la capa de red, asegurando que lleguen correctamente al nivel de sesión del otro extremo. A este nivel, la conexión es realmente de extremo a extremo ya que no se establece ninguna conversación con los niveles de transporte de todas las maquinas intermedias.

- **Nivel de Sesión:** A este nivel se establecen sesiones (conexiones) de comunicación entre los dos extremos para el transporte ordinario de datos. A diferencia del nivel de transporte, a este nivel se proporcionan algunos servicios mejorados, como la reanudación de la conversación después de un fallo en la red o una interrupción, etc.

- **Nivel de Presentación:** A este nivel se controla el significado de la información que se transmite, lo que permite la traducción de los datos entre las estaciones. Por ejemplo, Si una estación trabaja con un código concreto y la estación del otro extremo maneja uno diferente, el nivel de presentación es el encargado de realizar esta conversación. Para conversaciones confidenciales, este nivel también codifica y encripta los datos para hacerlos incomprensibles a posibles escuchas ilegales.

- **Nivel de Aplicación:** Es el nivel que esta en contacto directo con los programas o aplicaciones informáticas de las estaciones y contiene los servicios de comunicación mas utilizados en las redes. Como ejemplos de servicios a este nivel se puede mencionar la transferencia de archivos, el correo electrónico, etc.

1.4.1 Encapsulamiento

Todos sabemos que todas las comunicaciones de una red parten de un origen y se envían a un destino, y que la información que se envía a través de una red se denomina datos o paquete de datos. Si un computador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

Para ver cómo se produce el encapsulamiento, examine la forma en que los datos viajan a través de las capas. Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendiente. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus

servicios a los usuarios finales. Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos[13]:

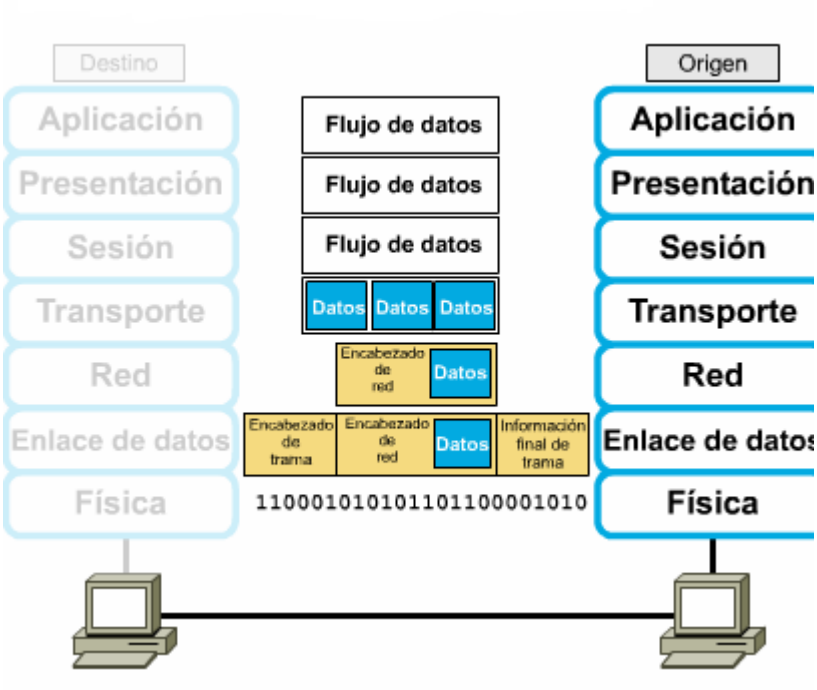

Figura 1.3 Encapsulamiento de datos

1. **Crear los datos.** Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.

2. **Empaquetar los datos para ser transportados de extremo a extremo.** Los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. **Anexar (agregar) la dirección de red al encabezado.** Los datos se colocan en un paquete o datagrama que contiene el encabezado de red con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los

[13] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

4. **Anexar (agregar) la dirección local al encabezado de enlace de datos.** Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. **Realizar la conversión a bits para su transmisión.** La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico puede originarse en una LAN, cruzar el backbone de un campus y salir por un enlace WAN hasta llegar a su destino en otra LAN remota. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.

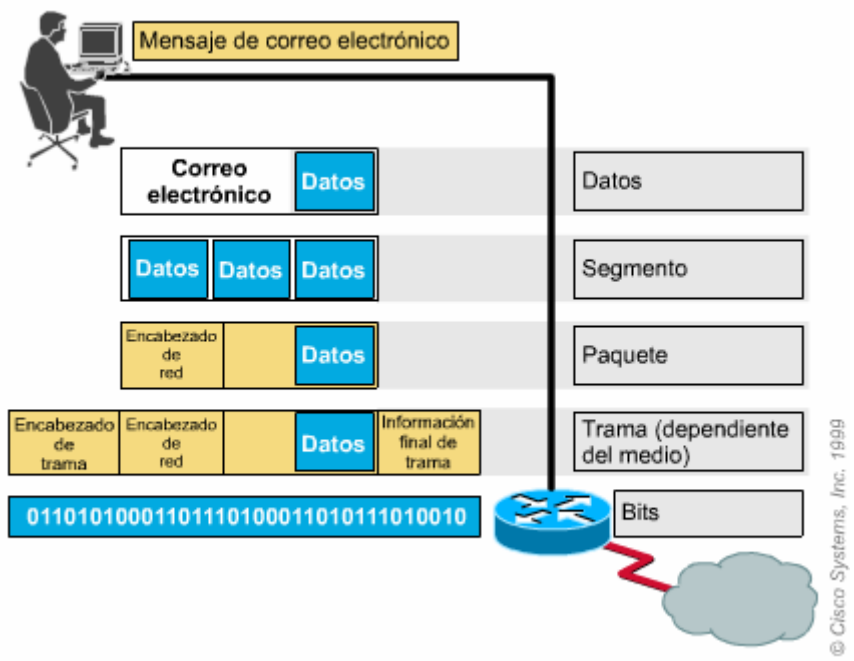

Figura 1.4 Ejemplo de encapsulamiento de datos

1.4.2 Nombres de los datos en cada capa del modelo OSI

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino[14]. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Durante este proceso, cada protocolo de capa intercambia información, que se conoce como unidades de datos de protocolo (PDU), entre capas iguales. Cada capa de comunicación, en la computadora origen, se comunica con un PDU específico de capa y con su capa igual en la computadora destino.

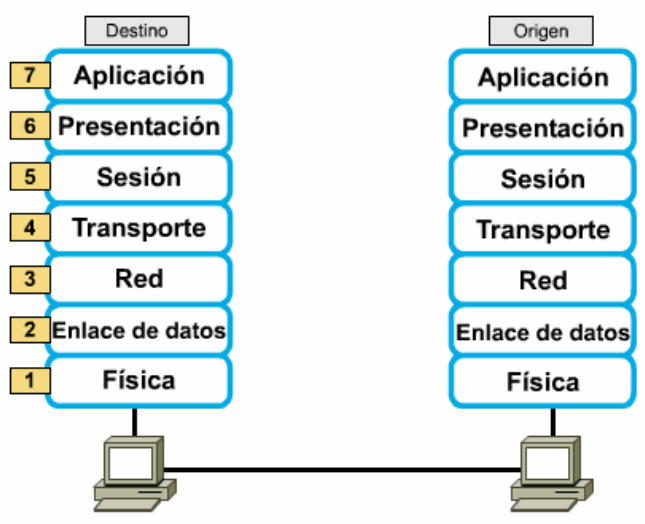

Figura 1.5 Comunicación de igual a igual (par a par).

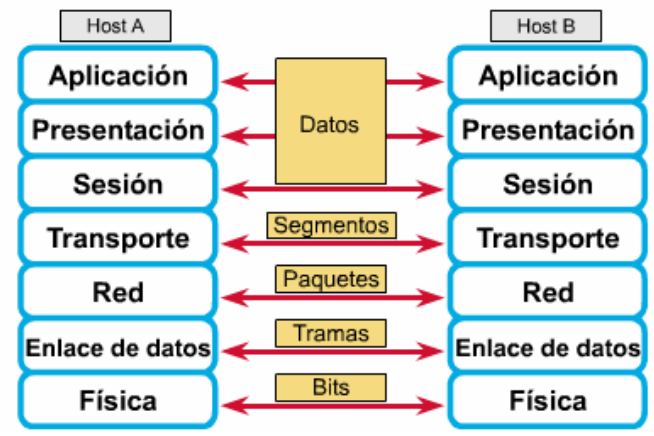

Figura 1.6 Comunicación de igual a igual (par a par).

[14] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales. Después de que las Capas 7, 6 y 5 han agregado la información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de Capa 4, se denomina segmento.

Por ejemplo, la capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (PDU de Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de Capa 2); el encabezado de la trama contiene información (por ej., direcciones físicas) que es necesaria para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.

La capa física también suministra un servicio a la capa de enlace de datos. La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1.

CAPITULO II

TIPOS DE REDES

Y

SUS TOPOLOGÍAS

2.1 INTRODUCCIÓN A LAS REDES LOCALES

El concepto de información del que se habla hoy en día y al que se le ha concedido tanta importancia, resulta a primera vista un tanto complejo de definir.

Podemos decir que información es todo aquello que a través de nuestros sentidos penetra en nuestro sentido nervioso y produce un aumento en nuestros conocimientos. Así pues, la información expresa el saber en sentido amplio.

El funcionamiento de todas las comunidades animales y humanas es posible gracias a la comunicación. Esta consiste en un acto por el cual un individuo establece con otros un contacto que le permite intercambiar información[15]. Para que esa comunicación sea posible, la información deberá representarse mediante unos símbolos que todos los individuos que están involucrados en esa comunicación deben ser capaces de traducir para poder interpretarlos correctamente. Para nosotros los humanos, este intercambio de información se realiza a través de la voz o de palabras escritas (lenguaje).

El concepto de información que se ha repasado en los párrafos anteriores resulta de gran importancia para la informática. Esta es la ciencia que estudia el tratamiento automático de la información, es decir, los instrumentos y métodos que permiten automatizar determinadas tareas repetitivas y así liberar al ser humano de esas pesadas labores.

Por su parte, un sistema informático es aquel que realiza algún tipo de tratamiento de la información. Puede ser tan sencillo como calcular la suma de dos números, o tan complejo como obtener las fechas y horas de los eclipses totales de sol que se producirán en los próximos años.

---

[15] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

Si aumentamos el nivel de detalle, podremos observar que, además de información de entrada o de salida, dentro del sistema de información pueden existir datos de carácter fijo que no varían durante el proceso de elaboración de la información, además de datos de carácter temporal que se utilizan para obtener resultados intermedios y que se eliminan una vez que se han obtenido los resultados y datos de tipo variable que pueden modificar el estado actual del sistema. El ejemplo mas sencillo lo encontramos en una calculadora, donde la información fija la constituyen las tablas de logaritmos o trigonométricas; los resultados intermedios se almacenan temporalmente para realizar operaciones complejas y existe una memoria que puede almacenar números, modificando así su estado interno.

El sistema necesita conocer como debe procesar la información.

Esta característica la obtiene a través de un programa que tiene almacenado y que contiene todas las instrucciones para la elaboración de los datos. En la calculadora, por ejemplo, el programa indica que la operación numérica debe realizarse (suma, resta, etc.) y puede seleccionarse por el usuario.

Según la Unión Internacional de Telecomunicaciones, se define formalmente telecomunicación como toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos o informaciones de cualquier tipo que se transmiten por hilos, medios ópticos, radioeléctricos u otros sistemas electromagnéticos.

Por su parte, una red de transmisión de datos es una estructura formada por determinados medios físicos (dispositivos reales) y lógicos (programas de transmisión y control) desarrollada para satisfacer las necesidades de comunicación de una determinada zona geográfica. Se trata, pues, de un soporte que permite la conexión de diversos equipos informáticos (o cualquier otro dispositivo electrónico) con el objetivo de suministrarles la posibilidad de que intercambien informaciones.

La señal recibida por el receptor es la suma de la señal enviada por el emisor mas el ruido, todos los errores producidos no pueden ser corregidos, pero si la mayoría de ellos. El límite se sitúa teniendo en cuenta el máximo aceptable por el usuario y el coste de la instalación de la red.

Señal_recibida = Señal_enviada + Ruido

Hay que tener en cuenta que una red de transmisión de datos no esta formada única y exclusivamente por el medio de transmisión. El problema fundamental consiste en organizar toda la estructura cuando existe una gran cantidad de usuarios; En el caso del sistema telefónico es evidente que todos los abonados deben de estar conectados, pero resulta absurdo conectar a todos con todos (por la gran cantidad de cableado que esto supone). En este caso, es necesario un mecanismo que sea capaz de establecer comunicaciones entre usuarios, incluso a través de un mismo cable.

Por lo tanto, los elementos de una red de comunicación son los siguientes[16]:

- **Sistema de transmisión**: Es la estructura básica que soporta el transporte de las señales por la red.

- **Sistema de conmutación**: Mecanismo que permite el encaminamiento de la información hacia su destino. Normalmente va a existir un medio limitado para la comunicación, por lo que este deberá ser compartido por varios emisores y receptores. El ejemplo más simple de un sistema lo constituye un operador de telefonía (centralita) que se encarga de conectar a dos usuarios que deseen comunicarse.

[16] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

- **Sistema de señalización**: Para que la comunicación sea posible, es necesario que exista un sistema de inteligencia distribuido por la red que sincronice todos los recursos que se encuentren en ella. Este control se lleva a cabo enviando señales a los distintos elementos que intervienen en la comunicación. Estos dispositivos de señalización se encargan, por ejemplo, de indicar a un usuario que esta recibiendo una llamada (cuando suena el timbre) que se encuentra ocupado, etc.

Una red de computadoras es un conjunto de ordenadores que poseen dos características diferenciadoras:

- Se encuentran interconectadas mediante algún medio de transmisión (es decir, pueden intercambiar información).

- Son autónomas, es decir, tienen cierta potencia de calculo (pueden realizar procesado de datos) y no son controladas por otras computadoras centrales. Los primeros comienzos de la informática estaban dominados por los grandes ordenadores centrales y los usuarios accedían a ellos a través de terminales formadas únicamente por monitor y teclado. Esa estructura no es una red por que los terminales son “bobos”, es decir, no realizan ningún tipo de calculo y se limitan a enviar o recibir datos.

2.2 CLASIFICACION DE LAS REDES

Existe multitud de redes, cada una de ellas con unas características especificas que las hacen diferentes del resto. Podemos clasificar a las redes en diferentes tipos, atendiendo a diferentes criterios. La clasificación que se expone a continuación esta ordenada según los criterios más importantes.

2.2.1 TITULARIDAD DE LA RED

Esta clasificación atiende a la propiedad de la red, por lo que se puede hacer una división en dos tipos de redes: redes privadas dedicadas y redes compartidas[17].

- **Redes dedicadas:** Una red dedicada es aquella en la que sus líneas de comunicación son diseñadas e instaladas por el usuario o administrador, o bien, alquiladas a las compañías de comunicaciones que ofrecen este tipo de servicios (en el caso de que sea necesario comunicar zonas geográficas alejadas), y siempre para su uso exclusivo. Ejemplo de este tipo de red puede ser la red local de un aula de informática de instituto o facultad.

- **Redes compartidas:** Las redes compartidas son aquellas en las que las líneas de comunicación soportan información de diferentes usuarios. Se trata en todos los casos de redes de servicio público ofertadas por las compañías de telecomunicaciones bajo cuotas de alquiler en función de la utilización realizada o bajo tarifas por tiempo limitado. Pertenecen a este grupo las redes telefónicas conmutadas y las redes especiales para transmisión de datos. Ejemplos de este tipo de redes son: la red de telefonía fija, la red de telefonía móvil, RDSI, Iberpac, las redes de fibra óptica, etc.

2.2.2 TOPOLOGÍA

Esta clasificación tiene en cuenta la arquitectura de la red, es decir, la forma en que se interconectan los diferentes nodos o usuarios de ella:

---

[17] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

- **Malla:** Es una interconexión total de todos los nodos, con la ventaja de que, si una ruta falla, se puede seleccionar otra alternativa. Este tipo de red es más costoso de construir, ya que hace falta más cable.

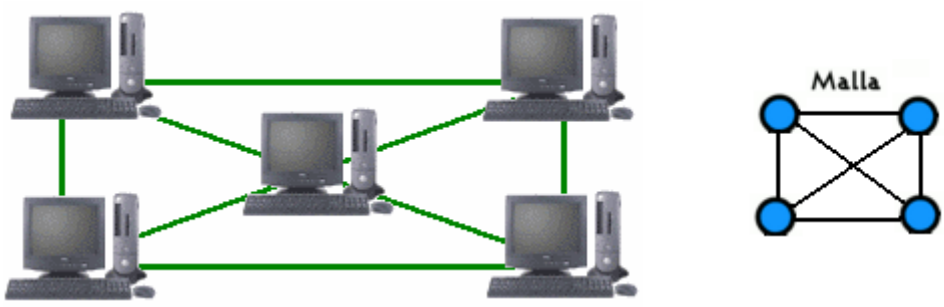

Figura 2.1 Red con topología en malla.

- **Estrella:** Los equipos se conectaran a un nodo central con funciones de distribución, conmutación y control. Si el nodo central falla, quedara inutilizada toda la red; si es un nodo de los extremos, solo este quedara aislado. Normalmente, el nodo central no funciona como estación, sino que más bien suele tratarse de dispositivos específicos.

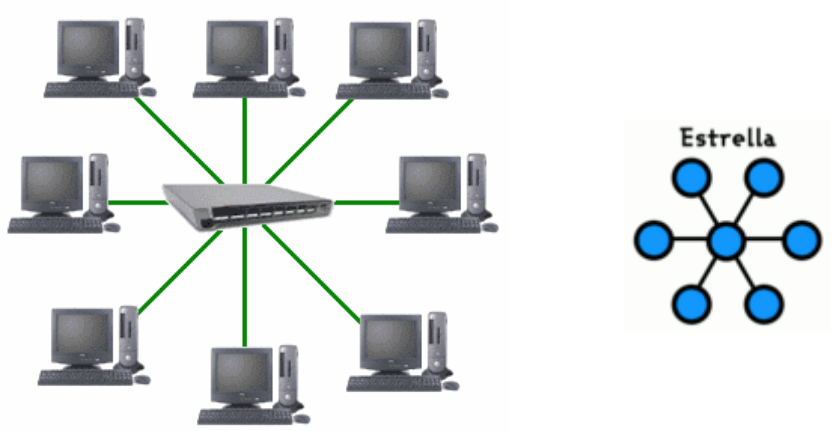

Figura 2.2 Red con topología en estrella.

- **Bus:** Utiliza un único cable para conectar los equipos. Esta configuración es la que requiere menos cableado, pero tiene el inconveniente de que, si falla algún enlace, todos los nodos quedan aislados (ya que se rompe el bus).

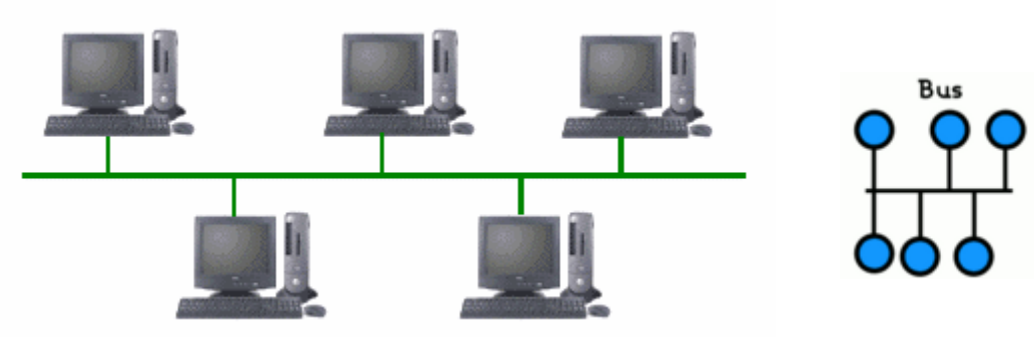

Figura 2.3 Red con topología en bus.

- **Árbol:** Es una forma de conectar nodos como una estructura jerarquizada. Esta topología es la menos utilizada, y se prefiere la topología irregular, ya que el fallo de un nodo o un enlace deja a conjuntos de nodos intercomunicados entre si.

Figura 2.4 Red con topología en árbol.

- **Anillo:** Todos los nodos están conectados a una única vía con sus dos extremos unidos. Al igual que ocurre con la topología bus, si falla algún enlace, la red dejara de funcionar completamente.

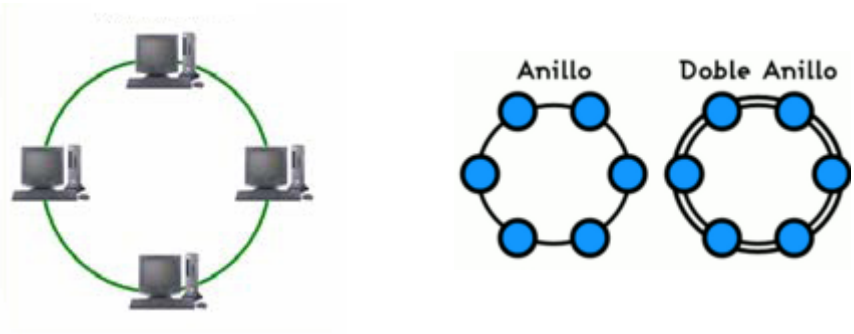

Figura 2.5 Red con topología en anillo.

- **Intersección de anillo:** Varios anillos conectados por nodos comunes. El inconveniente de esta topología es que, si fallan los nodos comunes de los anillos, toda la red dejara de funcionar.

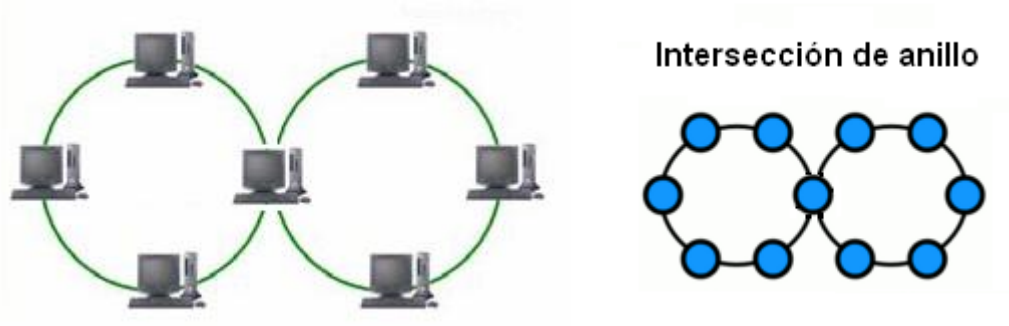

Figura 2.6 Red con topología en intersección de anillo.

- **Irregular:** Cada nodo debe de estar conectado, como mínimo, por un enlace, pero no existen más restricciones. Esta topología es la más utilizada en redes que ocupan zonas geográficas amplias. Esta topología permite la búsqueda de rutas alternativas cuando falla alguno de los enlaces.

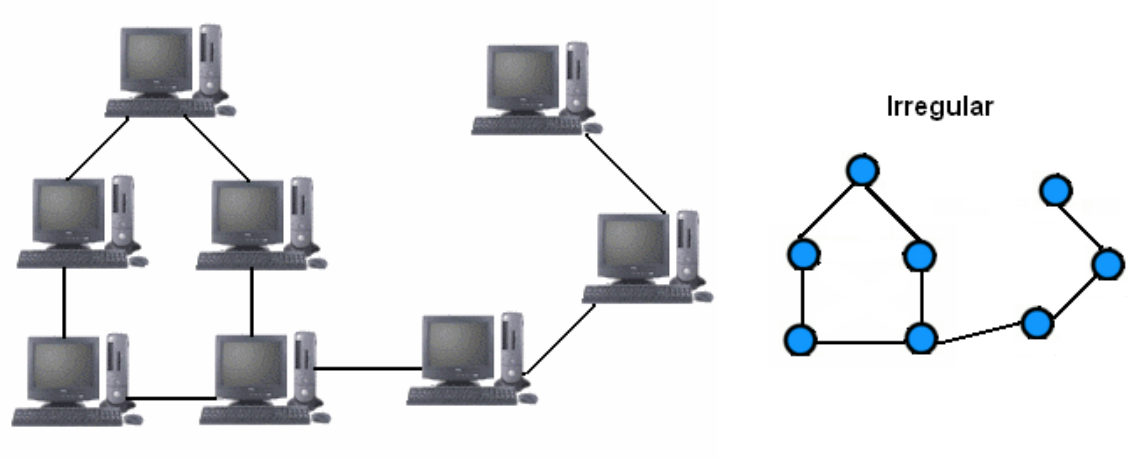

Figura 2.7 Red con topología irregular.

2.2.3 TRANSFERENCIA DE LA INFORMACIÓN

Esta clasificación tiene en cuenta la técnica empleada para transferir la información desde el origen al destino. Por lo tanto, también depende de la topología de la red y, si se ha separado de la clasificación anterior, ha sido por que existen diferentes topologías que comparten el mismo método de transmisión[18].

- **Redes conmutadas (punto a punto):** En este tipo de redes, un equipo origen (emisor) selecciona un equipo con el que quiere conectarse (receptor) y la red es la encargada de habilitar una vía de conexión entre los dos equipos. Normalmente puede seleccionarse varios caminos candidatos

[18] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

para esta vía de comunicación que puede o no dedicarse exclusivamente a la misma. Existen tres métodos para la transmisión de la información y la habilitación de la conexión:

- **Conmutación de circuitos:** En este de comunicación, se establece un camino único dedicado. La ruta que sigue la información se establece durante todo el proceso de comunicación, aunque existan algunos tramos de esa ruta que se comportan con otras rutas diferentes. Una vez finalizada la comunicación, es necesario liberar la conexión. Por su parte, la información se envía integra desde el origen al destino, y viceversa, mediante una línea de transmisión bidireccional. En general, se seguirán los siguientes pasos: 1° Establecimiento de la conexión, 2° Transferencia de la información y 3° Liberación de la conexión. Este método es el empleado en una llamada telefónica normal.

- **Conmutación de paquetes:** En este caso, el mensaje se divide en fragmentos cada uno de los cuales es enviado a la red y cada fragmento se enruta a su destino por separado, a cada uno de estos fragmentos se les denomina paquetes, cada paquete tiene parte de la información a transmitir, información de control, además de los números o direcciones que identifican al origen y al destino.

- **Conmutación de mensajes:** La información que envía el emisor se aloja en un único mensaje con la dirección del destino y se envía al siguiente nodo. Este almacena la información hasta que hay un camino libre, dando lugar, a su vez, al envió al siguiente nodo, hasta que finalmente el mensaje llega a su destino.

➢ **Redes de difusión (multipunto):** En este caso, un equipo o nodo envía la información a todos los nodos y es el destinatario el encargado de

seleccionar y captar esa información. Esta forma de transmisión de la información esta condicionada por la topología de la red, ya que esta se caracteriza por disponer de un único camino o vía de comunicación que debe ser compartido por todos los nodos o equipos. Esto quiere decir que la red debe tener una topología en bus o anillo, o debe estar basada en enlaces por ondas de radio.

2.2.4 LOCALIZACIÓN GEOGRÁFICA

La localización geográfica de la red es un factor a tener en cuenta a la hora de diseñarla y montarla. No es lo mismo montar una red para un aula de informática que interconectar las oficinas de dos sucursales que la misma empresa tiene instaladas en diferentes países. Sin embargo, esta clasificación muchas veces resulta confusa o arbitraria, ya que se basa en criterios vagamente definidos[19].

- **Subred o segmento de red:** Un segmento de red esta formado por un conjunto de estaciones que comparten el mismo medio de transmisión. El segmento esta limitado en espacio al departamento de una empresa, un aula de informática, etc. Se considera al segmento como la red de comunicación más simple y todas las redes de mayor tamaño están constituidas por la unión de varios segmentos de red.

- **Red de área local (LAN):** Es un término vago que se refiere a uno o varios segmentos de red conectados mediante dispositivos especiales. Normalmente se le da este calificativo a las redes cuya extensión no sobrepasa el mismo edificio (o incluso la misma habitación).

[19] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

- **Red de campus:** Una red de campus se extiende a otros edificios dentro de un mismo campus o polígono industrial. Generalmente, las diversas redes de cada edificio se conectan a un tendido de cable principal. Generalmente, la empresa es propietaria del terreno por el que se extiende el cable y tiene libertad para poner cuantos cables sean necesarios sin solicitar permisos especiales.

- **Red de área metropolitana (MAN):** Generalmente, una MAN esta confinada dentro de una misma ciudad y se haya sujeta a regulaciones locales. Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica. Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana.

- **Red de área extensa (WAN) y redes globales:** Las WAN y las redes globales abarcan varias ciudades, regiones o países. Los enlaces WAN son ofrecidos generalmente por empresas de telecomunicaciones públicas o privadas que utilizan enlaces de microondas, fibra óptica o vía satélite. Actualmente, el método empleado para conectar una WAN utiliza líneas telefónicas modificadas para ofrecer un servicio mas rápido.

2.2.5 SISTEMAS OPERATIVOS

Esta clasificación de redes locales, se basa en los tipos de sistemas operativos instalados en las estaciones y la relación existente entre ellos.

Dentro de esta clasificación, encontramos dos tipos de LAN diferentes:

- **Redes con servidor:** En este tipo de redes existe al menos una maquina llamada servidor donde se encuentran todos los recursos a compartir. El resto de máquinas, llamadas clientes o estaciones de trabajo, solamente pueden usar los recursos locales o del servidor (no los de otras estaciones de trabajo). Dependiendo del tipo de sistema operativo instalado en el servidor, éste puede ser dedicado (utilizado únicamente para gestionar los recursos de la red) o no dedicado (además de llevar la gestión de la red puede funcionar como estación de trabajo).

- **Redes entre iguales:** Cada maquina puede compartir sus recursos con el resto, de forma que pueden ser clientes o servidores a la vez.

Aunque esta clasificación define con claridad como se administran los recursos de una red, cuando hablamos de sistemas operativos comerciales, hay que reconocer que existen pequeños matices respecto a esos tipos y, de hecho, algunos de ellos toman características de los otros. Por ejemplo, existen redes basadas en un servidor donde es posible administrar parte de los recursos que poseen las estaciones clientes (como su disco duro, alguna impresora conectada, etc.).

En una red con servidor es normal que exista más de uno para distribuir la carga entre ellos; también se utilizan estaciones solamente para dar servicio a usuarios en una red entre iguales, por lo que podrían convertirse en servidores dedicados.

Las ventajas y desventajas del uso de un modelo u otro dependen de la centralización o distribución de recursos. En una red basada en servidor, existe la figura del administrador, que se encarga de gestionar los recursos del servidor de forma conveniente. En una red entre iguales, cada usuario decide como gestionar

sus recursos locales, permitiendo o no el acceso de otros usuarios. Las ventajas de utilizar una red basada en un servidor son las siguientes[20]:

- Un servidor dedicado tiene más capacidad de proceso de datos que una máquina que opera además como estación. Resulta mucho mas económico comprar una sola máquina de gran capacidad aunque las estaciones clientes no sean tan rápidas.

- Tener la información almacenada en una o unas pocas máquinas permite tener mayor control de la seguridad contra accesos no autorizados.

- Las tareas de administración se simplifican, ya que el administrador tiene todos los recursos centralizados.

- No es necesario que los usuarios tengan conocimientos avanzados de administración, ya que ellos no están autorizados a realizar esas tareas.

- Resulta mucho más sencillo realizar actualizaciones de programas y copias de seguridad cuando toda esa información y aplicaciones están centralizadas en los servidores.

- No existe el riesgo de que la caída o mal funcionamiento de una estación pueda bloquear al resto (aunque sí la caída del servidor).

Sin embargo, las redes entre iguales también ofrecen ventajas sobre las redes con servidor:

[20] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

- El sistema operativo es de menor costo (ya que es más ligero). Un sistema operativo de servidor es mucho más caro y suele estar limitado a un número máximo de estaciones a las que le puede dar servicio.

- La gestión de las impresoras se descentraliza, lo que permite instalarlas en las estaciones para que los usuarios no tengan que caminar hasta los servidores para recoger sus trabajos.

- Aunque los usuarios deben disponer de mayores conocimientos para compartir sus recursos, a los administradores les resulta mucho más fácil reconfigurar este tipo de sistemas.

2.3 NORMALIZACIÓN Y ORGANISMOS

Las primeras redes de computadoras que se construyeron, tanto comerciales como militares, utilizaban sus propias normas de diseño y funcionamiento. Han llegado a existir compañías (como es el caso del gigante IBM) que utilizaban normas de comunicación diferentes para sus propios productos. Con esta situación ocurrió que la mayoría de las grandes empresas que contrataban redes de computadoras llegaron a instalar en sus sucursales y edificios grupos de redes de diferentes fabricantes. Cuando necesitaron comunicar esas redes, surgieron los problemas: los sistemas de transmisión no eran compatibles y era necesario deshacerse de todo lo instalado hasta la fecha y montar redes nuevas, todas ellas del mismo tipo. La otra solución consistía en desarrollar equipos capaces de convertir y adaptar las señales de comunicación entre redes, alternativa de costo mas elevado.

A partir de entonces, se comprobó que era necesario definir un conjunto de normas estandarizado, lo que permitiría coordinar a todos los fabricantes y proveedores. Estos estándares no solo posibilitan la comunicación entre diferentes

computadoras, sino que también permiten que los productos fabricados tengan un menor costo y una mayor aceptación[21].

Las normas se dividen en dos categorías:

- **Estándares de facto:** Viene de la palabra que en latín significa de hecho y a este grupo pertenecen los estándares que simplemente aparecieron y se impusieron en el mercado por su extensa utilización. El ordenador personal (PC) de IBM y sus sucesores son normas de facto por que la mayoría de los fabricantes copiaron los equipos de IBM con mucha exactitud.

- **Estándares de iure:** Viene del latín que significa por ley y, comparado con el tipo anterior, son estándares formales y legales acordados por algún organismo internacional de estandarización autorizado. Estos organismos son de dos tipos: los creados por tratados entre varios países y las organizaciones voluntarias.

Existen varias organizaciones internacionales dedicadas a tareas de normalización y estandarización. Entre ellas, destacaremos:

- **ITU (Unión Internacional de Telecomunicaciones).** Organización de las naciones unidas constituida, en principio, por las autoridades de correos, telégrafos y teléfonos (PTT) de los países miembros. Estados Unidos esta representado por el departamento de estado. Se encarga de realizar recomendaciones técnicas sobre teléfono, telégrafo e interfaces de comunicación de datos que, a menudo, se reconocen como estándares. Trabaja en colaboración con ISO, que en la actualidad es miembro del ITU. Tiene tres sectores principales: sector de radiocomunicaciones (ITU-R), sector

[21] Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. México, D.F.: Alfaomega, Ra-Ma. 2005.

de desarrollo (ITU-D), y sector de telecomunicaciones (ITU-T), que antes de 1993 se denominaba CCITT (Comité Consultivo Internacional Telegráfico y Telefónico).

- **ISO (Organización Internacional de Normalización).** Agrupa a 89 países y se trata de una organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia OSI y protocolos estándares para varios niveles de ese modelo.

- **ANSI (Instituto Americano de Normas Nacionales).** Asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense de ISO, que adopta con frecuencia los estándares ANSI como normas internacionales.

- **IEEE (Instituto de Ingenieros Eléctricos y Electrónicos).** Además de publicar revistas y preparar conferencias, esta organización se encarga de elaborar estándares en las áreas de ingeniería eléctrica y computación (como es el estándar IEEE 802 para redes de área local).

- **IAB (Consejo de Arquitectura de Internet).** Comité informal encargado de supervisar la aparición de nuevos estándares y protocolos para Internet. Los acuerdos alcanzados aparecen en una serie de documentos que se publican a toda la comunidad denominados RFC (Request Ford Comments). Los documentos RFC superan actualmente los 2000 e incluyen todas lña especificaciones de la arquitectura TCP/IP de Internet.

2.4 NORMAS ESTANDARIZADAS

Se expondrá de forma general algunos servicios y protocolos que por su uso y popularidad se han convertido en estándares en la industria de las redes. Introduciremos aquí una breve referencia a los protocolos ARCnet, IEEE 802, X.25, RDSI, ADSL y Frame Relay[22].

2.4.1 ARCnet

La red ARCnet (Attached Resource Computer Net) fue desarrollada por la empresa Datapoint Corporation y durante algunos años ha sido un estándar popular en redes de área local

Esta red establece los protocolos a nivel físico y nivel MAC, aunque no se ha especificado una arquitectura por niveles formal. ARCnet define el cableado, la velocidad de transmisión, la topología, los elementos de interconexión, etc.

También permite cierta flexibilidad a la hora de instalar el cableado, y se pueden elaborar diferentes topologías, como son bus, estrella y árbol, solamente modificando la interconexión del cableado y sus elementos adicionales.

2.4.2 IEEE 802

El estándar IEEE 802 es posterior a ARCnet y fue elaborado en 1990 por la organización IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) para la comunicación en redes locales.

Dentro de este estándar se han definido varios tipos de redes locales en lo que se refiere al tipo de cableado utilizado, velocidad de transmisión, formato de los

[22] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

bloques de información enviados, reparto del medio, etc. Estos aspectos están definidos a nivel físico y a nivel enlace, por lo que IEEE 802 solo cubre los protocolos de estas dos capas.

IEEE 802 esta dividido en varias especificaciones diferentes. Por un lado esta IEEE 802.1, que define la interfaz con los niveles superiores (normalmente, con el nivel de red). En IEEE 802.2 se encuentra normalizada la parte superior desnivel de enlace (llamado LLC o Control de Enlace Lógico). El resto de especificaciones, que van desde la IEEE 802.3 a la IEEE 802.12, tiene que ver con la parte inferior del nivel de enlace (llamada MAC o Subcapa de Acceso al Medio) y la capa física.

Cada una de ellas establece un tipo de LAN diferente, que resultan incompatibles entre si. IEEE 802.5 es el estándar mas parecido a ARCnet, aunque no son compatibles.

2.4.3 X.25

X.25 fue desarrollado en 1970 por el CCITT (hoy ITU-T) y define un conjunto de protocolos para la comunicación en redes de área extensa. Estos protocolos están a tres niveles: nivel físico, nivel de enlace y nivel de red, Como se muestra en la tabla.

RED
ENLACE DE DATOS
FÍSICO (X,21)

Tabla 2.1 Niveles de la red X.25

Los protocolos de X.25 están incluidos dentro de la arquitectura OSI y resultan bastante fiables en su funcionamiento debido a que todos ellos realizan control de errores. Sin embargo, esta táctica hace que la transmisión sea lenta y que en las capas envié mucha información de control redundante. Por esta ultima razón, en un futuro próximo se prevé sea sustituido por Frame Relay.

Para que otros dispositivos no compatibles con X.25 puedan conectarse a esta red se han definido varios protocolos de comunicación adicional. Por ejemplo, el protocolo X.28 y el protocolo X.32 están definidos para interconectar X.25 con la red telefónica conmutada. Para que este tipo de adaptación sea posible, es necesario utilizar un dispositivo especial denominado PAD (Packet Assembler Disassembler o Ensamblador y Desensamblador de Paquetes), definido en la norma X.3.

En España, la red de conmutación de paquetes X.25 se llama Iberpac. Para conectar esta red con las redes X.25 de otros países, hay que seguir la recomendación X.75. Aunque Iberpac se esta empezando a sustituir por redes mas modernas, todavía se sigue utilizando hoy en día.

2.4.4 RDSI

El estándar RDSI (Red Digital de Servicios Integrados) también conocido como ISDN surgió en 1984 como una solución a las necesidades de comunicación modernas. La idea de RDSI consiste en ofrecer todo tipo de servicios: transmisión de voz, transmisión de datos, transmisión de imagen y sonido en tiempo real, etc.

La red RDSI dispone de su propio cableado, se utiliza como red de área extensa y no puede funcionar sobre las redes telefónicas estándar (RTC). Además, esta red dispone de servicios a velocidades y capacidades diferentes, dependiendo del contrato que realice el usuario.

La arquitectura de RDSI define todos los protocolos de la red a nivel físico, enlace de datos y red y, si un usuario cambia su instalación de RTC a RDSI, necesitara de unos adaptadores especiales para que su teléfono, fax, etc, funcionen. Así mismo, también se ofrecen terminales especiales para su uso en RDSI.

Cuando un usuario desea conectar su ordenador a la RDSI, debe instalar en éste un adaptador específico. Algunos de estos adaptadores incorporan incluso un MODEM analógico que garantiza la compatibilidad con el sistema telefónico antiguo. La configuración del adaptador RDSI necesita de los siguientes elementos:

- Controlador de dispositivo (driver) del adaptador.
- Protocolo V110, a nivel físico de RDSI.
- Protocolo HDLC, a nivel de enlace de datos.
- Protocolo X.75, a nivel de red y similar a X.25.
- Librería CAPI (Common IDSN API o API Común de RDSI), una librería estándar para que las aplicaciones puedan acceder a la red.

2.4.5 ADSL

La red ADSL (Asymetric Digital Subscriber Line o Línea Asimétrica Digital de Suscriptor) esta basada en la idea de utilizar la red telefónica básica (RTC) para transmitir información a alta velocidad. Puesto que hoy en día la mayoría de la población dispone en sus casas de una toma telefónica de dos hilos, se plantea utilizar toda esa red sin necesidad de instalar otra nueva.

El problema que se plantea consiste en utilizar una red telefónica de baja calidad para transmitir datos a alta velocidad. La solución de ADSL consiste en utilizar circuitos integrados ASP (Advanced Signal Processor o Procesador de Señales Avanzado) para eliminar electrónicamente todas las interferencias producidas en la comunicación.

ASDL debe verse como una solución de compromiso, que se instala en los hogares de forma rápida, mas que una solución a largo plazo. Hoy en día ya se ha implantando por muchas compañías de comunicaciones, y la mayoría de los usuarios la utilizan como acceso rápido a Internet.

2.4.6 FRAME RELAY

Las redes Frame Relay (Retransmisión de Trama) son redes empleadas para transmitir información a una velocidad razonable con un costo bajo. Ésta implementa un conjunto de protocolos de comunicaciones para redes de área extensa.

El estándar Frame Relay surgió como respuesta a la necesidad de determinados usuarios y empresas que solicitaban una red de transmisión de datos con una capacidad y velocidad de transmisión superiores a X.25. La velocidad de Frame Relay es superior a X.25 por que el protocolo no realiza detección ni corrección de errores en los nodos intermedios; este control es responsabilidad solamente de los dos extremos que se comunican. Esta red funciona sobre líneas telefónicas rápidas donde la tasa de error es baja.

2.5 TIPOS DE REDES LOCALES

Hay muchos tipos distintos de redes locales, pudiéndose lograr múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de

transmisión e incluso los protocolos utilizados. Estos factores van a determinar la arquitectura de la red local.

Sin embargo, de todas las posibles soluciones hay tres que ya están establecidas y que, al mismo tiempo, cuentan con una gran difusión dentro del mundo de las redes locales[23].

- Ethernet
- Token Ring
- Arcnet

2.5.1 ETHERNET

Esta red fue desarrollada por Xerox Corporation para enlazar un grupo de microcomputadores que estaban distribuidos por los laboratorios de investigación de Palo Alto en California, para poder intercambiar programas y datos, así como compartir los periféricos.

En un principio, se creo para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cable.

Si se utiliza cable coaxial grueso, se pueden tener hasta cuatro tramos de cable (unidos con repetidores) y los computadores se conectan al cable por medio de transceptores. Se pueden conectar computadores en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

Si se utiliza cable coaxial fino, no es necesario utilizar transceptores, pudiéndose conectar el cable al computador por medio de una conexión BNC en forma de T.

---

[23] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

El número máximo de tramos es de cinco, y la longitud máxima de cada tramo es, aproximadamente, de un tercio de la longitud máxima conseguida con el cable coaxial grueso (550 metros). Así mismo, el número máximo de estaciones es de 30 por cada uno de los tres tramos en los que se pueden conectar computadores.

Los datos se transmiten a una velocidad de 10 megabytes (bytes por segundo) a una distancia máxima de dos kilómetros.

Utiliza una topología en bus con protocolo de contienda CSMA/CD (acceso múltiple por detección de portadora con detección de colisiones). Cualquier estación puede intentar transmitir en cualquier momento, pero como todas utilizan un canal único, solo una estación puede transmitir datos simultáneamente.

El tamaño del bloque de datos puede oscilar desde 72 hasta 1526 bytes (con un tamaño normal de 256 bytes).

Todas las estaciones tienen asignada una dirección de 48 bytes, que permite que cuando se cambia de lugar una estación no haya posibilidad de conflictos, y por tanto se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

2.5.2 TOKEN RING

Esta arquitectura de red fue creada por IBM en octubre de 1985, aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 kilobytes y para un máximo de 64 computadoras y una red de banda ancha a 2 megabytes para un máximo de 72 computadoras.

Emplea una topología de anillo con protocolo de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica.

Los datos se transmiten a una velocidad de 4 megabytes pudiéndose conectar hasta un máximo de 8 computadoras y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (MAU) si se utiliza con cable coaxial (si se utiliza con fibra óptica, puede llegar hasta una velocidad de 16 megabytes).

No obstante, como se puede conectar hasta 12 unidades de acceso multiestación, el número de computadoras conectadas y la distancia máxima pueden aumentar considerablemente.

2.5.3 ARCNET

Este tipo de arquitectura comenzó siendo un sistema de proceso distribuido de Datapoint.

Es una red en banda base que utiliza una topología mixta estrella/bus con protocolo de paso de testigo.

Transmite a una velocidad de 2,5 megabytes y todas las computadoras han de estar conectadas a un concentrador, HUB activo no puede sobre pasar los 650 metros.

No obstante, se puede conectar más de un hub activo, por lo que el número máximo de estaciones puede llegar a ser de 255.

2.6 OTROS TIPOS DE REDES

Entre otros tipos de arquitecturas de redes se encuentran las redes inalámbricas.

Una red local se denomina inalámbrica cuando los medios de unión entre las estaciones no son cables.

Las principales ventajas de este tipo de redes son:

- Permiten una amplia libertad de movimientos.

- Sencillez en la reubicación de las estaciones de trabajo evitando la necesidad de establecer un cableado.

- Rapidez en la instalación.

Sus principales inconvenientes son:

- Dudas sobre si afecta la salud de los usuarios.

- Faltan normas estándar.

- Poca compatibilidad con las redes fijas.

- Problemas con la obtención de licencias para aquella que utilizan el espectro radioeléctrico.

Su utilización esta especialmente recomendada para la instalación de redes en aquellos lugares donde no pueda realizarse un cableado o en lugares con una movilidad de las estaciones de trabajo muy grande.

Actualmente existen cuatro técnicas para su utilización en redes inalámbricas: infrarrojos, radio en UHF, microondas y láser.

2.6.1 INFRARROJOS

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta y que pueden ser interrumpidas por cuerpos opacos.

Todas las redes sin hilos por infrarrojos operan usando un rayo de luz infrarroja para transportar los datos entre dispositivos. Estos sistemas necesitan generar señales muy fuertes, debido a que las señales de transmisión dispersas son susceptibles a la luz desde fuentes como ventanas.

Puede transmitir señales con alta velocidad debido al alto ancho de banda de la luz infrarroja (puede emitir a 10 Mbps).

Hay 4 tipos de redes de infrarrojos[24]:

- **Redes en línea de vista (Line-of-sight).** Como su propio nombre indica, este tipo dolo transmite si el transmisor y el receptor se ven limpiamente.

- **Redes por dispersión de infrarrojos (Scatter).** Este tipo emite transmisiones para que reboten en las paredes y techos, y eventualmente contacten con el receptor.

[24] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

- **Redes por reflexión (Reflective).** En este tipo, los transceptores ópticos situados cerca de las computadoras transmiten hacia un punto común que redirige las transmisiones a la computadora apropiada.

- **Telepunto óptico de banda ancha.** Este tipo proporciona servicios de banda ancha. Es capaz de manejar requerimientos de alta calidad multimedia que pueden coincidir con los proporcionados por una red de cable.

No se ven afectados por interferencias externas y puede alcanzar hasta 200 metros entre el emisor y el receptor. No es necesaria la obtención de una licencia administrativa para su uso.

2.6.2 RADIO UHF

Una red basada en equipos de radio en UHF necesita para su instalación la obtención de una licencia administrativa. No se ve interrumpida por cuerpos opacos gracias a su cualidad de difracción.

Hay dos tipos de redes que utilizan esta técnica[25]:

- **PureLAN.** Es una red compatible con Novell NetWare, LAN Manager, LAN Server y TCP/IP.

- **WaveLAN.** Es compatible con Novell NetWare.

[25] Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.

2.6.3 MICROONDAS

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las súper-altas frecuencias, utilizándose para las redes inalámbricas la banda de los 18-19 Ghz.

La red Rialta de motorota es una red de este tipo.

2.6.4 LÁSER

Esta tecnología para redes inalámbricas, que esta en base de investigación, es util actualmente para conexiones punto a punto con visibilidad directa, y se utiliza fundamentalmente para interconectar segmentos distantes de redes locales convencionales (ETHERNET y TOKEN RING), llegando a cubrir distancias de hasta 1000 metros.

CAPITULO III

HARDWARE PARA REDES

3.1 MEDIOS DE TRANSMISIÓN

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos.

Distinguimos dos tipos de medios: guiados y no guiados. En ambos casos, la transmisión se realiza por medio de ondas electromagnéticas. Los medios guiados conducen las ondas a través de un campo físico (cables). Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen (como es el aire).

La naturaleza del medio, junto con la de la señal que se transmite a través de él, constituye un factor determinante de las características y la calidad de la transmisión. En el caso de medios guiados, es él mismo el que determina las limitaciones de la transmisión. Así, cada uno de los medios que se verán a continuación cumple unas determinadas características en cuanto a[26]:

- Velocidad de transmisión de los datos.
- Ancho de banda que puede soportar.
- Espacio entre repetidores.
- Fiabilidad en la transmisión.
- Costo.
- Facilidad de instalación.

Sin embargo, a la hora de obtener la velocidad de transmisión máxima que puede soportar un medio no guiado, resulta mas determinante el espectro de

[26] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

frecuencia de la señal utilizado que las características del propio medio (aunque también están influenciados por las condiciones atmosféricas).

Puesto que existen muchas formas de instalar redes locales en organizaciones y universidades, y todo depende del cableado que se utilice, los conectores, la forma en que se interconectan los dispositivos, etc., para ayudar a tomar todas esas decisiones, existen varios estándares de cableado estructurado. La más utilizada es la EIA/TIA-568, desarrollada por la Asociación de Industrias de Electrónica y la Asociación de Industrias de Telecomunicaciones, aunque existen otras muy importantes como EN 50173 y ISO/IEC-11801.

3.1.1 PAR SIN TRENZAR (PARALELO)

Este medio de transmisión esta formado por dos hilos de cobre paralelos recubiertos de un material aislante (plástico). Este tipo de cableado ofrece muy poca protección frente a interferencias. Normalmente se utiliza como cable telefónico para transmitir voz analógica y las conexiones se realizan mediante un conector denominado RJ-11. Es un medio semidúplex ya que la información circula en los dos sentidos por el mismo cable pero no se realiza al mismo tiempo.

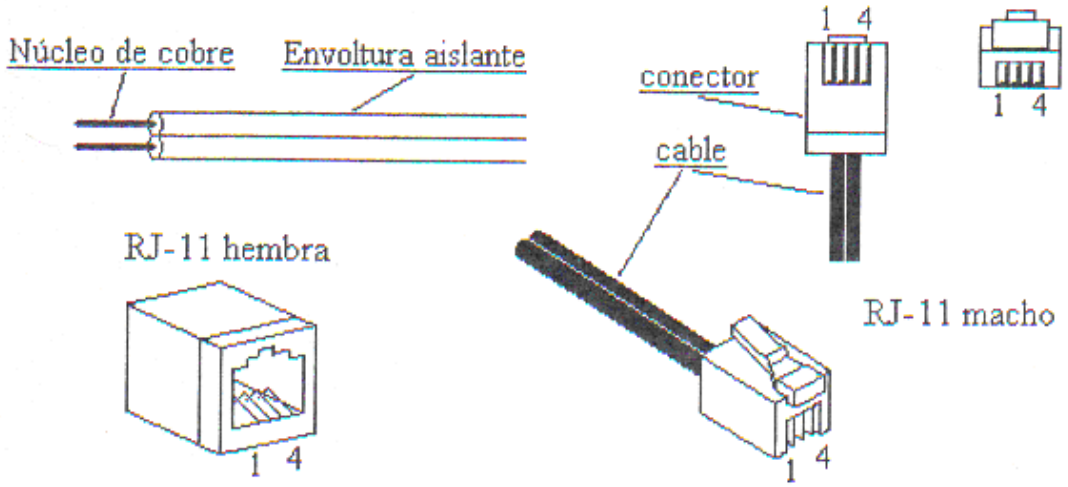

Figura 3.1 Cable paralelo categoría 1.

El cable paralelo se utiliza fundamentalmente en tendido eléctrico de alta tensión y también para transmisión de datos a corta distancia (apenas unos metros), ya que las interferencias afectan mucho a este tipo de transmisiones.

El cable paralelo “en bus” se utiliza comúnmente dentro del ordenador para comunicar entre si los diferentes elementos internos de el, ya que la distancia que los separa es muy corta y, por lo tanto, no es necesaria la protección frente al ruido. También se utiliza en los cables serie, paralelo y cables telefónicos que conectan el Terminal a la caja de conexiones del usuario. Según los estándares de cableado estructurado, a este tipo de cable también se le conoce como cable de categoría 1.

3.1.2 PAR TRENZADO

El par trenzado consiste en dos cables de cobre aislados, normalmente de 1 mm de espesor, enlazados de dos en dos de forma helicoidal, semejante a la estructura del ADN. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos y a otras interferencias procedentes del exterior.

En un par trenzado, normalmente uno de los cables esta marcado con una línea longitudinal que indica que se utiliza como masa. Esto es debido a que, a diferencia del cable paralelo, el cable de par trenzado se utiliza también para transmisión digital, y es necesario seguir el orden en ellos cuando se engasta al conector.

La figura 3.2 muestra la forma de un par trenzado y los conectores habituales para este tipo de configuración. Debido a su fácil instalación, velocidad de transmisión de hasta varios Mbps y bajo costo, los pares trenzados se utilizan ampliamente y es probable que se siga utilizando por mucho tiempo.

Los pares trenzados suelen agruparse en cables de mayor grosor, recubiertos por un material aislante, ya que su transmisión suele ser símplex. Dependiendo de la forma en la que se agrupan estos pares, tenemos varios tipos[27]:

- **Pares trenzados no apantallados (UTP).** Son los más simples y no tienen ningún tipo de pantalla conductora. Su impedancia característica es de 100 Ω y es muy sensible a interferencias. El par trenzado UTP categoría 5 esta recubierto de una malla de teflón que no es conductora.

- **Pares trenzados apantallados individualmente (STP).** Son iguales que los anteriores, pero en este caso se rodea a cada par de una malla conductora, que se conecta a las diferentes tomas de tierra de los equipos. Son los que poseen una mayor inmunidad al ruido.

- **Pares trenzados apantallados (FTP).** Son unos cables de pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias y su impedancia es de 120 Ω.

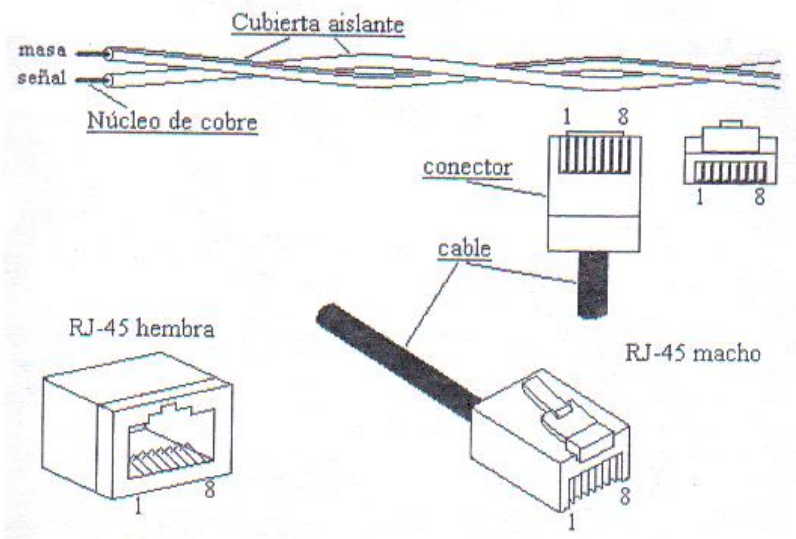

Figura 3.2 Cable de par trenzado y conector RJ-45.

[27] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

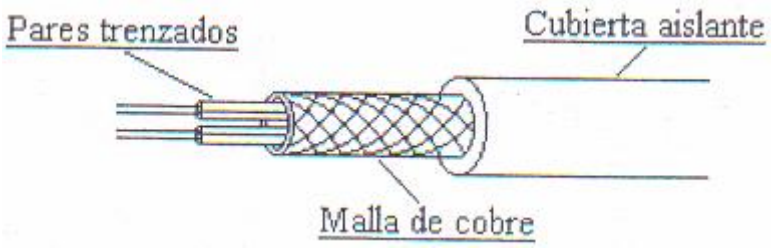

Figura 3.3 Pares trenzados apantallados FTP.

Así mismo, dependiendo del numero de pares que tenga un cable, el numero de vueltas por metro que posee su trenzado y los materiales utilizados, los estándares de cableado estructurado clasifican a los tipos de pares trenzados por categorías: categoría 1 (cable paralelo), categoría 2, categoría 3, categoría 4, categoría 5, categoría 5e, categoría 6, y categoría 7 (estas dos ultimas todavía en fase de desarrollo).

3.1.3 CABLE COAXIAL

El cable coaxial es otro típico medio de transmisión. Este cable tiene mejor blindaje que el par trenzado, por lo que puede alcanzar velocidades de transmisión mayores y los tramos entre repetidores o estaciones pueden ser más largos.

El cable coaxial consta de un alambre de cobre duro en su parte central por donde circula la señal, el cual se encuentra rodeado por un material aislante.

Este material esta rodeado por un conductor cilíndrico presentado como una malla de cobre trenzado que hace de masa. El conductor externo esta cubierto por una capa de plástico protector. Esta construcción le confiere un elevado ancho de banda y excelente inmunidad al ruido.

La figura 3.4 muestra la estructura del cable coaxial. La velocidad de transmisión de este cable depende de su longitud y en cables de 1 km es posible entre 1 y 2 Gbps. Los cables telefónicos solían usarse en el sistema telefónico, pero ahora se les ha reemplazado por fibra óptica en rutas de largo

recorrido y troncales de gran ancho de banda. Sin embargo, el cable coaxial todavía se utiliza para la televisión por cable y en redes de área local.

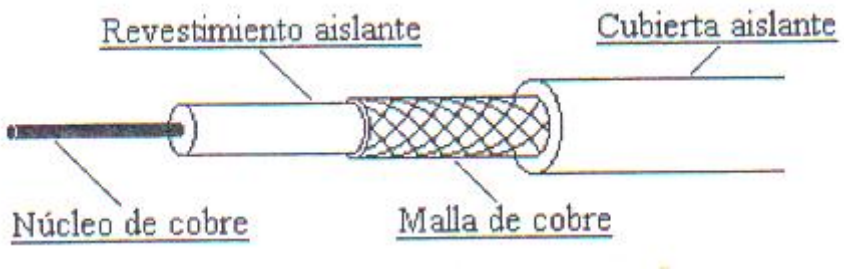

Figura 3.4 El cable coaxial.

Hay dos tipos fundamentales de cable coaxial: el cable coaxial de banda base (para transmisión digital) y el cable coaxial de banda ancha (utilizado para transmisión analógica), cuyas características son las siguientes[28]:

- **Coaxial de banda base (50 ohms):** Se utiliza en la transmisión digital. El ancho de banda máximo que se puede obtener depende de la longitud del cabe, para cables de 1 Km, por ejemplo, es factible obtener velocidades de transmisión de datos de hasta 10 Mbps y, en cables de longitudes menores, es posible obtener velocidades superiores. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de largas distancias, aunque utilizar cables de mayor longitud hace reducir la velocidad de transmisión. Existen dos tipos:

    - **Coaxial grueso:** Comenzó a utilizarse en redes locales y hoy en día solo se emplea para realizar la estructura troncal de distribución de la red. Hay dos tipos:

        - **RG-100:** Es el mas utilizado. Su núcleo es de 2.6 mm, mientras que la malla es de 9.5 mm (dando lugar a un cable de 1 cm de diámetro aproximadamente).

[28] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

- **RG-150:** Posee una secuencia de capas trenzadas que protegen mejor de las interferencias electromagnéticas. Su núcleo es de 3.7 mm, mientras que la malla es de 13.5 mm (dando lugar a un cable de 1.5 cm de diámetro).

- **Coaxial de banda ancha (75 ohms):** se utiliza para transmisión analógica, comúnmente para el envió de la señal de televisión por cable. Dado que las redes de banda ancha utilizan la tecnología patrón para envió de señales de televisión por cable, los cables pueden enviarse para aplicaciones que necesiten hasta los 300 Mhz (y en algunos casos hasta los 450 Mhz) y extenderse a longitudes que alcanzan casi los 100 Km, gracias a la naturaleza analógica de la señal (es menos critica que la digital). Un cable típico de 300 MHz, por lo general, puede mantener velocidades de transmisión de datos de hasta 150 Mbps.

Los conectores que se utilizan para el cableado coaxial aparecen representados gráficamente en las figuras 3.5 y 3.6. Cuando se utiliza cable coaxial delgado, las conexiones se realizan de forma más sencilla. Cada estación se enchufa a través de su tarjeta de red a un conector BNC en T.

Estos, a su vez, están enlazados con el cable coaxial mediante los conectores BNC soldados a el. Finalmente, es necesario que existan terminadores BNC en los extremos (para cerrar el circuito), compuestos de una resistencia que tenga la misma impedancia que el cable. La figura 3.7 muestra en detalle esta conexión.

Las conexiones en cable coaxial grueso son un poco mas complejas, ya que existe un dispositivo llamado transceptor que es el que conecta la estación con el cable y el aéreo (en el cable coaxial delgado va integrado en la propia tarjeta). La conexión entre la estación y el transceptor se hace a través de un cable digital llamado cable transceptor, que utiliza unos conectores llamados AUI macho y AUI hembra. Los conectores machos serie-N están soldados al cable coaxial y se unen a los transceptores para formar la red. En los extremos

también deben conectarse terminadores serie-N para cerrar el circuito. La figura 3.8 muestra estas conexiones.

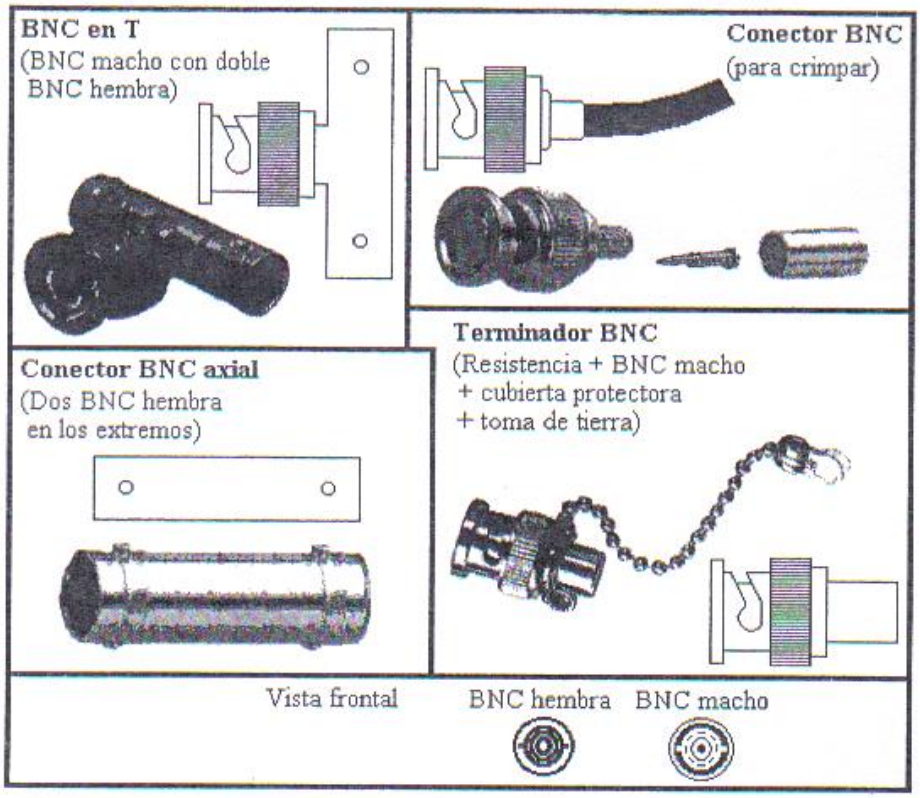

Figura 3.5 Conectores empleados en el cable coaxial delgado.

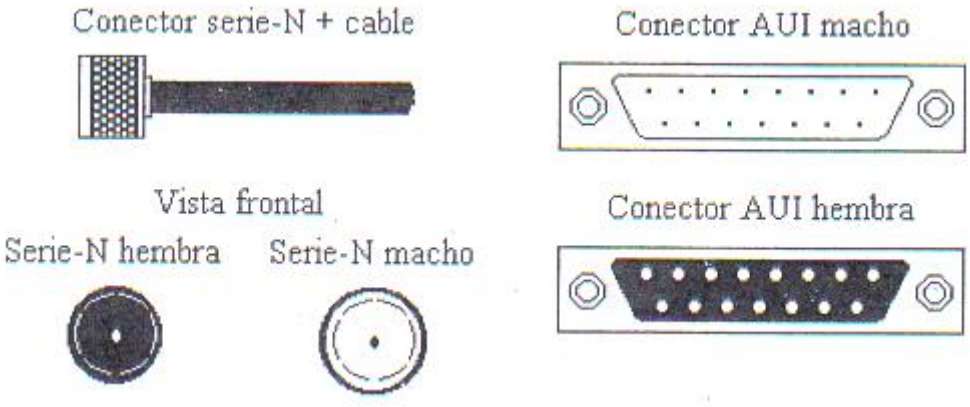

Figura 3.6 Conectores utilizados en el cable coaxial grueso.

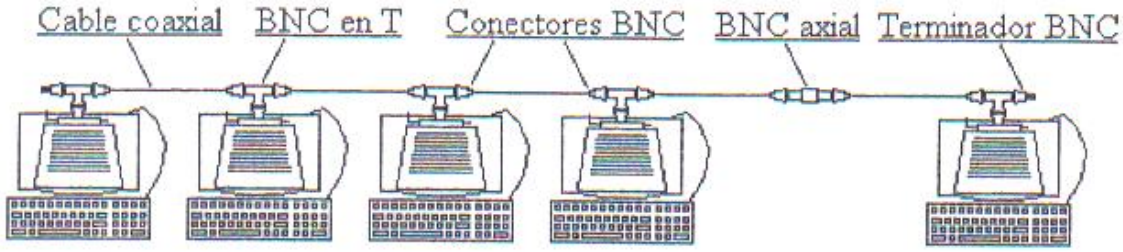

Figura 3.7 Conexión de una red con cable coaxial delgado.

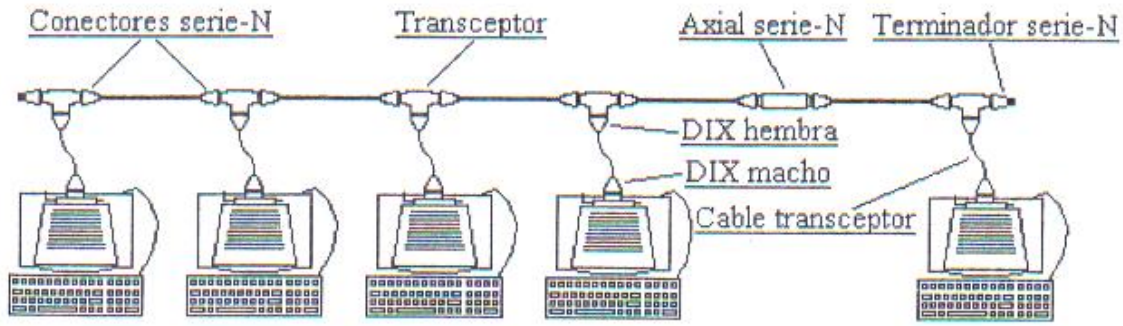

Figura 3.8 Conexión de una red con cable coaxial grueso.

Es una misma red se puede utilizar cable coaxial delgado y grueso; para ello se necesitan adaptadores. Estos conectan, por un extremo, un cable coaxial delgado (con un BNC macho o hembra) y, por el otro, el coaxial grueso (un conector serie-N macho o hembra). Puesto que estas redes utilizan los mismos métodos y señales para transmitir, no es necesario utilizar dispositivos adicionales que realicen adaptación de protocolos.

En comparación con el par trenzado, el cable coaxial es más inmune a interferencias, lo que permite unas longitudes de cable mayores. El par trenzado utiliza la transmisión balanceada, consiste en que cada par forma un circuito cerrado de transmisión; por ellos circula la misma corriente, pero en sentidos opuestos. En un cable coaxial se utiliza la transmisión no balanceada por que la señal circula por el núcleo de cobre y vuelve a tierra.

3.1.4 FIBRA ÓPTICA

La fibra óptica esta basada en la utilización de las ondas de luz para transmitir información binaria. Un sistema de transmisión óptico tiene tres componentes[29]:

- **La fuente de luz:** Se encarga de convertir una señal digital eléctrica (ceros y unos) en una señal óptica. Típicamente se utiliza un pulso de luz para representar un “1” y la ausencia de luz para representar un “0”, o se modifica su longitud de onda.

- **El medio de transmisión:** Se trata de una fibra de vidrio ultra delgada que transporta los pulsos de luz.

- **El detector:** Se encarga de generar un pulso eléctrico en el momento en el que la luz incide sobre él.

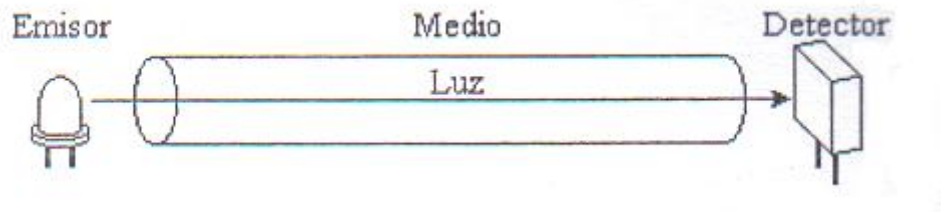

Figura 3.9 Elementos básicos de un sistema de transmisión por ondas de luz.

Al conectar una fuente de luz en un extremo de una fibra óptica y un detector en el otro, tenemos un sistema de transmisión de datos símplex que acepta una señal eléctrica, la convierte y transmite en pulsos de luz y, después, reconvierte la salida a una señal eléctrica en el extremo del receptor.

[29] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

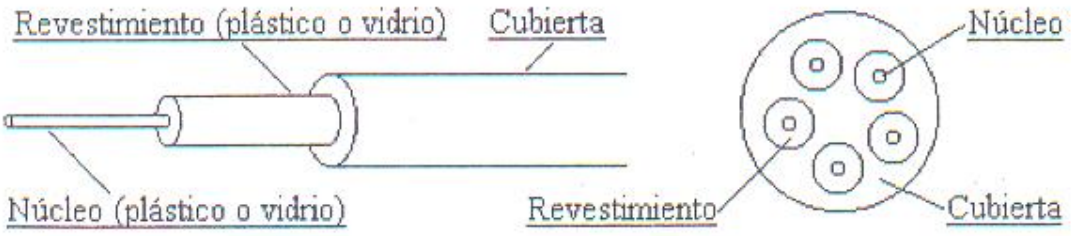

Figura 3.10 Estructura de la fibra óptica.

La fibra óptica esta cuidadosamente diseñada para transportar señales de luz. Se trata de un cilindro de pequeña sección flexible (diámetro del orden de 2 a 125 µm[22]) por el que se transmite la luz, recubierto de un medio con un índice de refracción menor que el del núcleo a fin de mantener toda la luz en el interior de él. A continuación viene una cubierta plástica delgada para proteger el revestimiento e impedir que cualquier rayo de luz del exterior penetre en la fibra. Finalmente, varias fibras suelen agruparse en haces protegidos por una funda exterior, como se muestra en la figura 3.10.

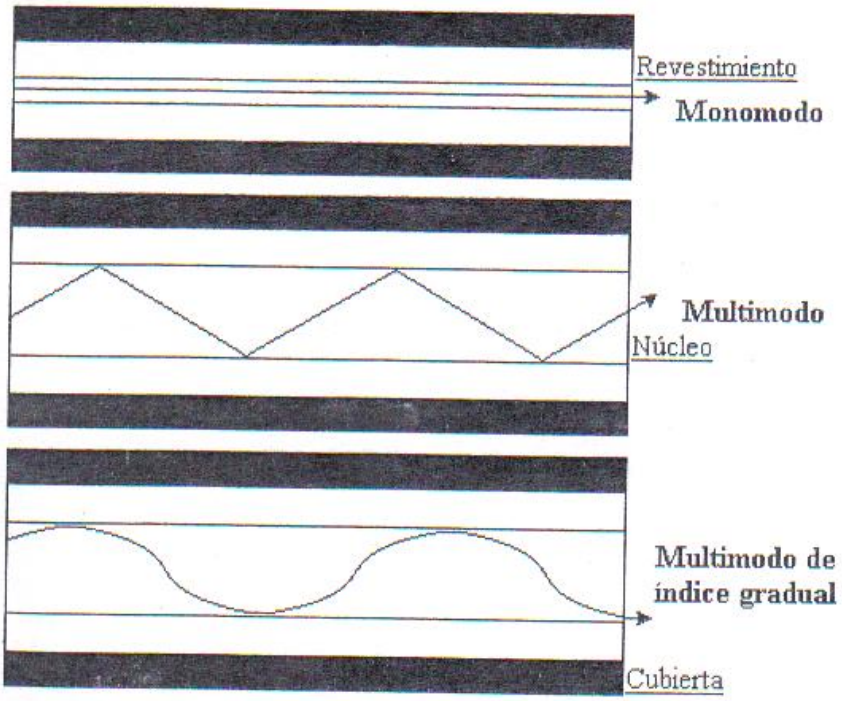

Figura 3.11 Tipos transmisión en cables de fibra óptica.

Los cables de fibra óptica pueden transmitir la luz de tres formas diferentes[30]:

- **Monomodo:** En este caso, la fibra es tan delgada que la luz se transmite en línea recta. El núcleo tiene un radio de 10 µm y la cubierta, de 125 µm.

- **Multimodo:** La luz se transmite por el interior del núcleo incidiendo sobre su superficie interna, como si se tratara de un espejo. Las perdidas de luz en este caso también son prácticamente nulas. El núcleo tiene un diámetro de 100 µm y la cubierta, de 140 µm.

- **Multimodo de índice gradual:** La luz se propaga por el núcleo mediante una refracción gradual. Esto es debido a que el núcleo se construye con un índice de refracción que va en aumento desde el centro a los extremos. Suele tener el mismo diámetro que las fibras multimodo.

Con la tecnología actual, la fibra óptica permite una velocidad de transmisión experimental en el laboratorio que sobrepasa los 50.000 Gbps (50 Tbps). El limite practico se encuentra cerca de 1 Gbp, y es debido a la incapacidad que los dispositivos tienen para convertir con mayor rapidez las señales eléctricas a ópticas y al revés (tanto los emisores como los detectores).

Frente a la velocidad de transmisión tan elevada que tiene la fibra, el inconveniente principal es su gran costo. No tiene tanto que ver con el precio por metro de fibra, sino que más bien esta relacionado con el montaje. El cable de fibra óptica no se puede doblar demasiado y las conexiones son muy costosas y complicadas. Muchas veces sale más rentable desechar varios kilómetros de fibra antes que hacer una unión de varios tramos.

[30] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

Existen tres formas de unir dos cables de fibra óptica[31]:

- **Utilizando conectores:** Cada tramo de fibra puede venir de fábrica con enchufes en los extremos. Esta forma de conectarlos es muy sencilla, pero adolece de una perdida de entre un 10% y un 20% de la luz que circula a través de la conexión.

- **Realizando empalmes de forma mecánica:** Se realiza un corte cuidadoso del extremo de cada tramo y se unen ambos mediante una manga especial que los sujeta en su lugar. Se puede mejorar la alineación haciendo pasar luz por la unión y efectuando pequeños ajustes hasta alcanzar su posición idónea. Los empalmes mecánicos resultan de una pérdida de luz entorno al 10%.

- **Fundiendo los dos extremos:** Se realiza una fusión de los dos tramos para formar una conexión sólida. Este empalme es casi tan bueno como una fibra de hilado único, pero aun así existe un poco de atenuación.

Las ventajas que tiene el uso de la fibra óptica frente a los cables de cobre convencionales son las siguientes:

- Puede manejar anchos de banda muchos más grandes que el cobre.

- Debido a su baja atenuación, solo se necesita repetidores cada 30 Km (en el cobre se necesitan repetidores cada 5 Km).

- No es interferida por las ondas electromagnéticas.

- Es delgada y ligera, sobre todo comparada con cables de cobre de igual capacidad de transmisión.

[31] Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

- Las fibras no tienen fugas y es muy difícil intervenirlas. Hay que cortar el cable o desviar parte de la luz, tarea nada sencilla que requiere el uso de costosos dispositivos.

3.2 MEDIOS INALÁMBRICOS

La comunicación inalámbrica (que no necesita de ningún tendido de cable entre el emisor y el receptor) resulta indispensable para aquellos usuarios móviles que necesitan estar continuamente “en línea”. También es de mucha utilidad cuando resulta muy costoso tender hilos de comunicación en zonas geográficas de difícil acceso.

Las comunicaciones inalámbricas consisten en el envió y recepción de electrones (o fotones) que circulan por el espacio libre (el aire). Estos electrones viajan en forma de ondas electromagnéticas que se propagan del mismo modo que las ondas del agua en un estanque. La distancia que separa dos “picos” o máximos consecutivos de esas ondas se llama longitud de onda y se designa universalmente con la letra griega λ (lambda). Hay que decir que para las ondas electromagnéticas que circulan por el aire no se utiliza la medida del periodo de la señal. La relación entre la frecuencia (f) y la longitud de onda (λ) de la señal viene expresada por la siguiente ecuación:

$$c = \lambda * f$$

Dependiendo de la frecuencia de la señal (y, por extensión, de su longitud de onda), existen diferentes tipos de enlaces inalámbricos, exhibiendo diferentes propiedades.

3.2.1 ONDAS DE RADIO

Las ondas de radio son fáciles de generar, pueden viajar largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora. Sin embargo, por la capacidad que tienen de viajar a largas

distancias, es necesario realizar un control estricto por parte de los gobiernos para que las diferentes transmisiones no se interfieran entre si.

Existen dos tipos de ondas de radio:

- **Ondas de radio de baja frecuencia:** Se caracterizan por que en su recorrido siguen la curvatura de la tierra y pueden atravesar con facilidad los edificios. Sin embargo, su ancho de banda solo permite velocidades de transmisión bajas.

- **Ondas de radio de alta frecuencia:** Estas ondas tienden a ser absorbidas por la tierra, por lo que deben ser enviadas a la ionosfera donde son reflejadas y devueltas de nuevo, con lo que se consigue transmitir a largas distancias.

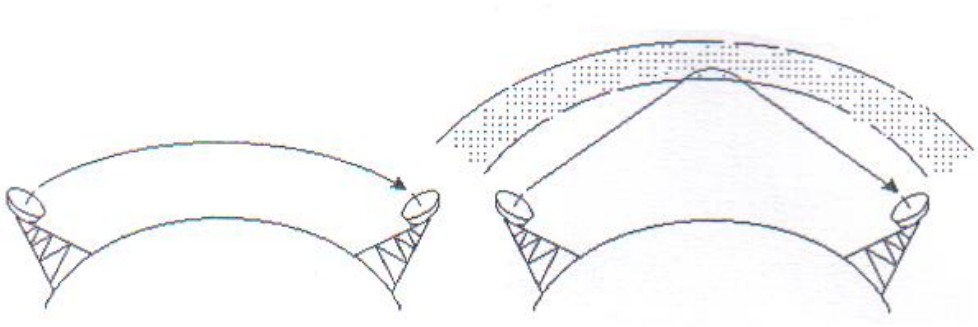

Figura 3.12 Tipos de ondas de radio.

3.2.2 MICROONDAS

Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 1 y 10 Ghz y posibilitan velocidades de transmisión aceptables, del orden de 10 Mbps. Por encima de los 1000 Hz, las microondas viajan en línea recta y, por tanto, se pueden enfocar en un haz de pequeña anchura. Concentrar toda la energía en un haz pequeño con una antena parabólica produce una relación señal/ruido muy alta (es decir, la amplitud del ruido puede ser muy pequeña),

pero las antenas del emisor y el receptor deben estar muy bien alineadas entre sí.

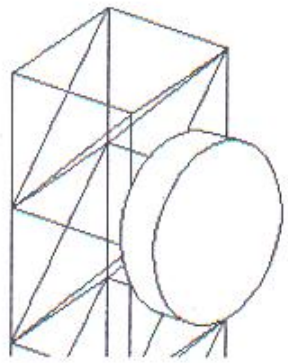

Figura 3.13 Enlaces de microondas.

A diferencia de las ondas de radio, las microondas no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias. En el caso de las comunicaciones por satélite, hay que tener en cuenta que siempre existe un pequeño retardo en las transmisiones debido a que la señal tarda aproximadamente 0,3 segundos en llegar y volver. Para algunas aplicaciones de envió y recepción de datos, este tiempo de espera puede resultar inaceptable.

3.2.3 ONDAS INFRARROJAS

Las ondas infrarrojas y milimétricas se utilizan mucho para la comunicación de corto alcance, en controles remotos de televisores, grabadoras de video, estéreos, etc. También es frecuente encontrar un puerto de comunicación infrarroja en los ordenadores portátiles. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. Este inconveniente también resulta a veces una ventaja en el sentido de que ofrecen más seguridad, precisamente por que la comunicación no atraviesa las paredes de un edificio.

Además, no es necesario obtener licencia del gobierno para operar un sistema de transmisión infrarrojo.

3.2.4 ONDAS DE LUZ

Es posible comunicar dos edificios mediante un láser montado en cada azotea.

La señalización óptica coherente mediante láser es unidireccional, de modo que cada edificio necesita un emisor láser y un receptor. Este esquema ofrece un costo muy bajo, es fácil de instalar y posee una elevada velocidad de transmisión. Por su parte las desventajas de este sistema son:

- Es difícil colocar correctamente los emisores y los receptores.
- El rayo láser no puede penetrar la lluvia y la niebla densa.
- Las corrientes de convección (aire caliente que sube del edificio) interfieren también en el haz de láser.

3.3 TIPOS DE TRANSMISIÓN

Una transmisión de datos tiene que ser controlada por medio del tiempo, para que el equipo receptor conozca en que momento se puede esperar que una transferencia tenga lugar.

Hay tres principios de transmisión para hacer esto posible:

- Transmisión Síncrona.
- Transmisión Asíncrona.
- Transmisión Plesincrona.

3.3.1 TRANSMISIÓN SÍNCRONA

La transmisión síncrona se hace con un ritmo que se genera centralizadamente en la red y es el mismo para el emisor como para el receptor. La información útil es transmitida entre dos grupos, denominados genéricamente delimitadores.

Este tipo de transmisión se lleva a cabo en tiempos iguales como por ejemplo: Frame Relay, ISDN y SDH.

Algunas de las características de la transmisión síncrona son:

Los bloques a ser transmitidos tienen un tamaño que oscila entre 128 y 1,024 bytes.

La señal de sincronismo en el extremo fuente, puede ser generada por el equipo terminal de datos o por el módem.

El rendimiento de la transmisión síncrona, cuando se transmiten bloques de 1,024 bytes y se usan no más de 10 bytes de cabecera y terminación, supera el 99%.

Ventajas y desventajas de la transmisión síncrona:

Posee un alto rendimiento en la transmisión.

Los equipamientos necesarios son de tecnología más completa y de costos más altos.

Son especialmente aptos para ser usados en transmisiones de altas velocidades.

El flujo de datos es más regular.

3.3.2 TRANSMISIÓN ASÍNCRONA

En la transmisión asíncrona es el emisor el que decide cuando se envía el mensaje de datos a través de la red. En una red asíncrona el receptor por lo consiguiente no sabe exactamente cuando recibirá un mensaje. Por lo tanto cada mensaje debe contener, aparte del mensaje en sí, una información sobre cuando empieza el mensaje y cuando termina, de manera que el receptor conocerá lo que tiene que decodificar.

En el procedimiento asíncrono, cada carácter a ser transmitido es delimitado por un bit denominado de cabecera o de arranque, y uno o dos bits denominados de terminación o de parada.

El bit de arranque tiene dos funciones de sincronización de los relojes del transmisor y del receptor.

El bit o bits de parada, se usan para separar un carácter del siguiente.

Normalmente, a continuación de los bits de información se acostumbra agregar un bit de paridad (par o impar).

Este tipo de transmisión se realiza en tiempos diferentes como por ejemplo Ethernet, ATM y X.25.

Algunas de las características de la transmisión asíncrona son:

Los equipos terminales que funcionan en modo asíncrono, se denominan también “terminales en modo carácter”.

La transmisión asíncrona también se le denomina arrítmica o de “start-stop”.

El rendimiento de usar un bit de arranque y dos de parada, en una señal que use código de 7 bits más uno de paridad (8 bits sobre 11 transmitidos) es del 72%.

Ventajas y desventajas del modo asíncrono:

En caso de errores se pierde siempre una cantidad pequeña de caracteres, pues éstos se sincronizan y se transmiten de uno en uno.

Bajo rendimiento de transmisión, dada la proporción de bits útiles y de bits de sincronismo, que hay que transmitir por cada carácter.

Es un procedimiento que permite el uso de equipamiento más económico y de tecnología menos sofisticada.

Se adecua más fácilmente en aplicaciones, donde el flujo transmitido es más irregular.

Son especialmente aptos, cuando no se necesitan lograr altas velocidades.

3.3.3 TRANSMISIÓN PLESINCRONA

En este tipo de transmisión el reloj usado en cada nivel de multiplexación es independiente de los otros niveles.

Este tipo de transmisión se realiza en tiempos casi iguales un ejemplo de ello es PDH.

La Jerarquía Digital Plesincrona, conocida como PDH (Plesiochronous Digital Hierarchy), es una tecnología usada en telecomunicación para transportar grandes cantidades de información mediante equipos digitales de transmisión que funcionan sobre fibra óptica, cable coaxial o radio de microondas.

El término plesincrono se deriva del griego plesio, cercano y chronos, tiempo, y se refiere al hecho de que las redes PDH funcionan en un estado donde las diferentes partes de la red están casi, pero no completamente sincronizadas.

3.4 MODOS DE TRANSMISIÓN

Se denomina canal de comunicación al recorrido físico que es necesario establecer para que una señal eléctrica, óptica, electro óptica, se pueda desplazar entre dos puntos.

Los distintos tipos de transmisión de una canal de comunicaciones son de tres clases diferentes:

- Simplex.
- Semi dúplex (half-dúplex).
- Dúplex (full-dúplex).

3.4.1 SIMPLEX

Se denomina Simplex al método de transmisión en que una estación siempre actúa como fuente y la otra siempre actúa como colector. Este método permite la transmisión de información, en un único sentido. Algunos ejemplos de modo de transmisión Simplex son la Radio, T.V. y Radio Localizador.

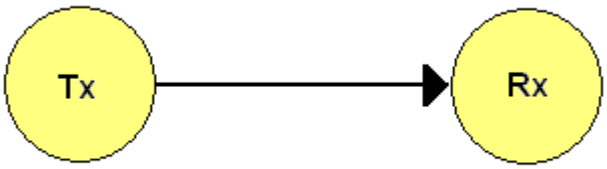

Figura 3.14 Modo de transmisión Simplex.

3.4.2 HALF DÚPLEX (SEMIDÚPLEX)

Se denomina half-dúplex (semidúplex) al método de transmisión en que una estación A en un momento de tiempo, actúa como fuente y otra estación corresponsal B actúa como colector; y en el momento siguiente, la estación B actuará como fuente y la A como colector. Este método permite la transmisión

en las dos direcciones, aunque en momentos diferentes, es decir que nunca pueden hablar ambas partes simultáneamente. Un ejemplo de este modo de transmisión es el Telegrafo.

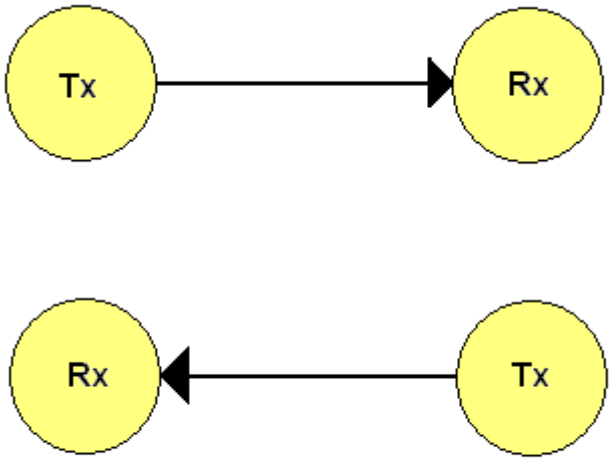

Figura 3.15 Modo de transmisión Half-dúplex (Semidúplex)

3.4.3 FULL DÚPLEX (DÚPLEX)

Se denomina full-dúplex (dúplex) al método de transmisión en que dos estaciones A y B, actúan como fuente y colector, transmitiendo y recibiendo información simultáneamente. Este método permite la transmisión en las dos direcciones, en forma simultánea. Algunos ejemplos son la Telefonía, Videoconferencia, MSN.

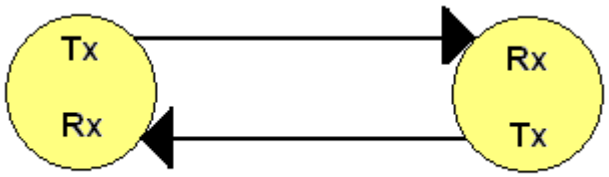

Figura 3.16 Modo de transmisión Full dúplex (Dúplex).

3.5 COMPRENSIÓN DEL HARDWARE DE LAS REDES

Los dispositivos de red que se verán a continuación que incluye los repetidores, ruteadores, concentradores y por el estilo son responsables de la transferencia de datos de un cable de la red a otro. Cada dispositivo tiene propiedades y usos diferentes. Un buen diseño de red utiliza el dispositivo correcto para cada tarea que la red debe cumplir.

En este apartado aprenderá acerca del hardware esencial para la conectividad de redes, lo cual implica lo siguiente:

- Repetidores.
- Hubs y concentradores.
- Switches.
- Puentes.
- Ruteadores.
- Compuertas.
- Paredes.
- Módems de corto alcance para conexiones pequeñas entre edificios.

3.5.1 REPETIDORES

Un repetidor es un dispositivo que extiende la distancia de un tramo de red en particular. Un repetidor toma una señal débil por un lado, la amplifica y, después, la manda por el otro lado. A menudo usted puede ver repetidores en las redes Thin Ethernet, pero se encuentran virtualmente en cualquier conexión

de red. Por ejemplo, si tiene que instalar un tramo de cable Cat-5 100Base-T que sea mayor de 100 metros, un repetidor le permitirá duplicar esta distancia.

Los repetidores operan a nivel capa física del modelo OSI de conectividad de redes[32]. Sin embargo, no poseen la inteligencia para comprender las señales que transmiten. Los repetidores solo amplifican la señal entrante de cualquier lado y la repiten por el otro lado. (Sin embargo, recuerde que también amplifica cualquier ruido que se produzca en el cable). Los repetidores se utilizan para conectar solamente el mismo tipo de medio de transmisión, como de 10Base-2 Thin Ethernet a 10Base-2 Rhin Ethernet, o Token Ring de par trenzado con Token Ring de par trenzado.

Los repetidores poseen una pequeña cantidad de inteligencia que puede ser de utilidad. Pueden aislar una de sus conexiones de la otra cuando se presenta un problema. Por ejemplo, considere dos segmentos de Thin Ethernet que se encuentren conectados mediante un repetidor. Si uno de esos segmentos se rompe, el repetidor aun permite que el segmento que esta en buenas condiciones continué operando correctamente.

Los usuarios de este segmento no podrán tener acceso a los recursos que se encuentran en el segmento roto, pero podrán continuar utilizando el segmento en buenas condiciones sin problema. (Recuerde, sin embargo, que esta capacidad no resulta del todo útil si sus servidores se encuentran en el lado roto y sus estaciones de trabajo están ubicadas en el segmento que no esta roto). La figura 3.14 muestra una extensión de red que utiliza repetidores.

[32] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

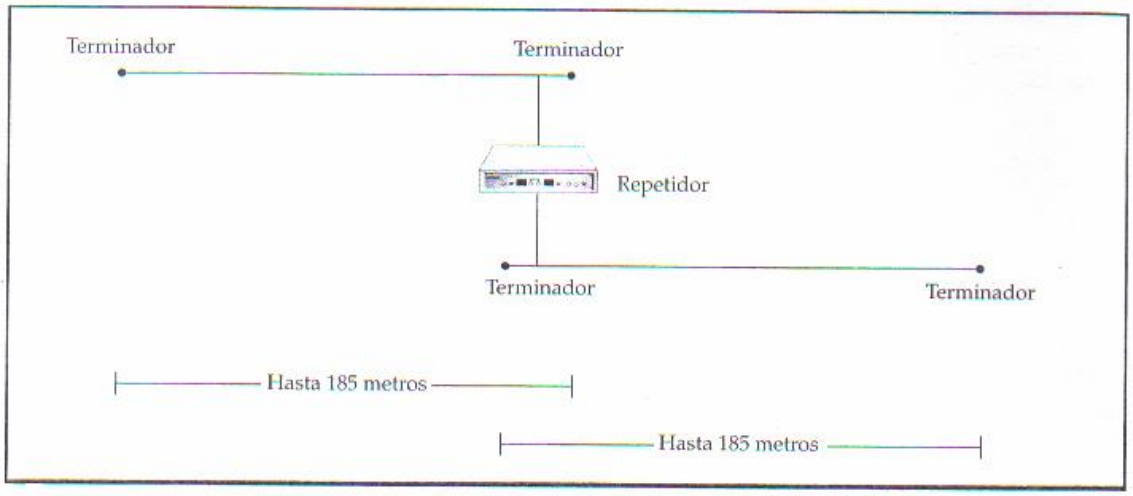

Figura 3.17 Utilización de repetidores para extender la longitud de la red.

3.5.2 HUBS Y CONCENTRADORES

Los concentradores LAN inteligentes llamados de una manera mas simple concentradores o, aun mas simple, hubs se utilizan para conectar los nodos de red a la columna dorsal de la misma. Los nodos se conectan a los hubs físicamente en forma de estrella (los cables se extienden desde el concentrador a cada nodo), ya sea que se utilicen en una red con topología estrella o con topología anillo. (Una red sencilla podría constar de uno o dos concentradores; redes mas pequeñas generalmente no requieren una red de espina dorsal).

Los hubs se encuentran disponibles para cualquier tipo de medio de transmisión que utilice módulos reemplazables para soportar diferentes tipos de medios de transmisión. Por ejemplo, puede comprar un chasis (bastidor) de concentrador en el que se puedan colocar tanto módulos Ethernet como Token Ring.

Usted puede comprar hubs en una gran variedad de tamaños que van desde los que soportan solo dos estaciones de trabajo hasta los que soportan mas de 100 estaciones. Muchos diseñadores de redes utilizan hubs apilables, los cuales, en general, soportan 24 conexiones de nodo cada una. A menudo, estos hubs, se utilizan en conjunto con switches.

Los hubs tienen dos propiedades importantes. La primera es que repiten todos los datos de cada puerto a todos los demás. Aunque están cableados en forma de estrella, en realidad trabajan eléctricamente (lógicamente) como si fuera un segmento con topología bus. Debido a esta repetición, no se presenta ningún filtrado o cualquier otra lógica para evitar las colisiones entre los paquetes que son transmitidos por cualquiera de los nodos conectados. La segunda propiedad importante que tienen los hubs es la partición automática, donde el hub puede automáticamente partir (en este contexto, cortar) cualquier nodo que tenga problema con los demás, desconectándolo. Dicha partición ocurre, por ejemplo, si se detecta un corto en el cable, si el puerto del hub recibe una cantidad excesiva de paquetes que inundan la red o si algún otro problema serio se detecta en un puerto determinado del concentrador. La partición automática previene que una conexión que no funcione de manera correcta provoque problemas a todas las demás.

A medida que transcurre el tiempo, los concentradores incrementan su nivel de complejidad[33].

- Administración integrada, que permite que el hub pueda administrarse desde un punto central de la red mediante el empleo de SNMP u otros protocolos y software de administración de redes.

- Autodetección de diferentes velocidades de conexión. Por ejemplo, son comunes los concentradores Ethernet que puedan detectar y operar, de forma automática, cada nodo a 10 Mbps (10Base-T) o 100 Mbps (100Base-T).

- Enlaces de alta velocidad que conectan el hub a una espina dorsal. Éstas, en general, operan a 10 veces la velocidad nominal del hub. (Por ejemplo, para un concentrador de 100 Mbps, los puertos de enlace deben operar a 1 Gbps).

[33] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

- Funciones integradas de puenteo y enrutamiento, las cuales hacen innecesaria la utilización de dispositivos separados para llevar a cabo el puenteo y el enrutamiento.

- Conmutación integrada que permite que los nodos del hub pueden conmutarse en vez de compartirse.

Cuando compre un concentrador, es importante saber cuantos nodos desea conectar, que cantidad de ancho de banda requiere cada uno y que tipo de bus de red se utilizara. Los buses pueden ser cualquiera, desde un bus Thin Ethernet a 10 Mbps, un bus 100Base-TX a 100 Mbps, hasta buses a mas alta velocidad. Su selección en cuanto a una determinada tecnología de bus depende de la cantidad total de ancho de banda que usted necesite y de los demás criterios de diseño de redes con los que deba cumplir.

Cada concentrador tiene un dominio de colisión separado o área de la red en la que pueden presentarse colisiones. En general, conectar todos los hubs en alguna forma resulta en un dominio de colisión más grande, que abarca todos los hubs.

La excepción a esta regla es una configuración donde todos los diferentes hubs se conectan a un switch, el cual mantiene a cada hub en su propio dominio de colisión. La figura 3.15 muestra un ejemplo de una red que utiliza hubs.

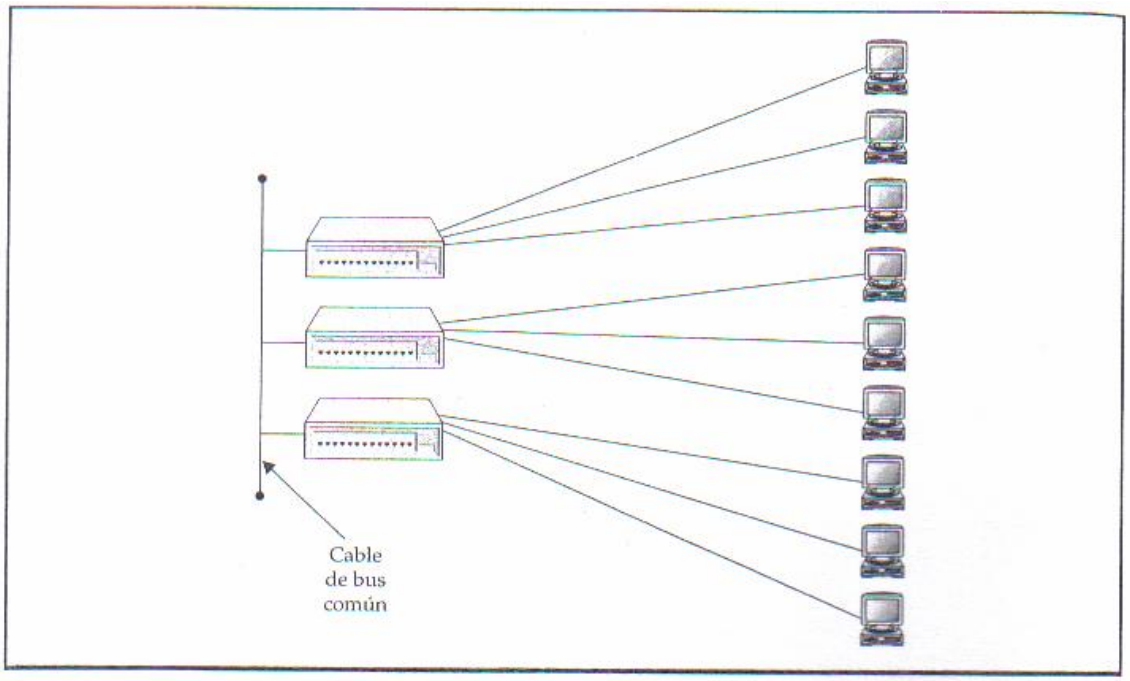

Figura 3.18 Arreglo típico de hubs.

3.5.3 SWITCHES

Los switches, como su nombre lo indica, pueden conmutar conexiones de un puerto a otro y lo pueden hacer de manera muy rápida. Están orientados a la conexión y, de forma dinámica, conmutan entre sus diferentes puertos para crear estas conexiones. Piense en un patio de ferrocarril con muchos trenes acercándose en algunas vías y alejándose en otras, y que el switch en el administrador del patio y quien ordena que la vía "se conmute", de forma que los trenes lleguen a su destino. Un switch de red es muy parecido a este tipo de administrador, excepto que el switch dirige paquetes en lugar de trenes y utiliza cableado tipo Ethernet en vez de rieles de ferrocarril para transportar la mercancía.

Debido a que los switches forman conexiones uno a uno entre cualquier par de puertos, todos los puertos que ingresan a un switch no son parte de un solo dominio de colisión[34]. En este sentido, el switch actúa como un tipo de puente gigante. A menudo los switches se utilizan para conectar un número determinado de hubs a un bus más rápido. Por ejemplo, suponga que usted tiene 10 hubs, cada uno con 24 estaciones de trabajo conectadas. Si

[34] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

simplemente conecta todos los hubs en un bus común, las 240 estaciones de trabajo compartirían un único dominio de colisión, lo cual podría afectar un poco el desempeño de la red. En lugar de hacer eso, una forma mucho mejor es instalar un switch de 12 puertos y conectar cada hub a uno de los puertos del switch. Por ejemplo, es común utilizar 100Base-T (o algún otra conexión de red mas rápida) para el bus. Este arreglo, además, permite que todo el trafico que se genere en cada uno de los 10 hubs continué operando a una velocidad de conexión de red de aproximadamente 10 Mbps hacia los servidores, a pesar de que todos los hubs estén compartiendo el bus. La figura 3.16 ilustra este método.

Los switches se han abaratado mucho y son extremadamente rápidos. En las conexiones en redes de área local, el uso de switches tiene más sentido que el de ruteadores, parcialmente debido a su costo y su relativa simplicidad. En realidad, la adquisición de puentes se ha dificultado debido a que los switches, en la actualidad, dominan el mercado ya que tienen los mismos beneficios a un costo mucho mas bajo y son mucho menos complejos. Además, la mayoría de las redes actuales evitan los hubs a favor de un diseño basado cien por ciento en switches. De hecho, es virtualmente imposible comprar hubs; todos los fabricantes típicamente ofrecen solo switches. Es importante que usted comprenda la diferencia entre los hubs y switches ya que pueden encontrar aun hubs instalados en algunas redes; sin embargo, en las redes más nuevas, encontrara exclusivamente switches. Hacer eso reduce de manera dramática la probabilidad de que se presenten colisiones entre paquetes de red, lo cual puede suceder en un arreglo basado en hubs.

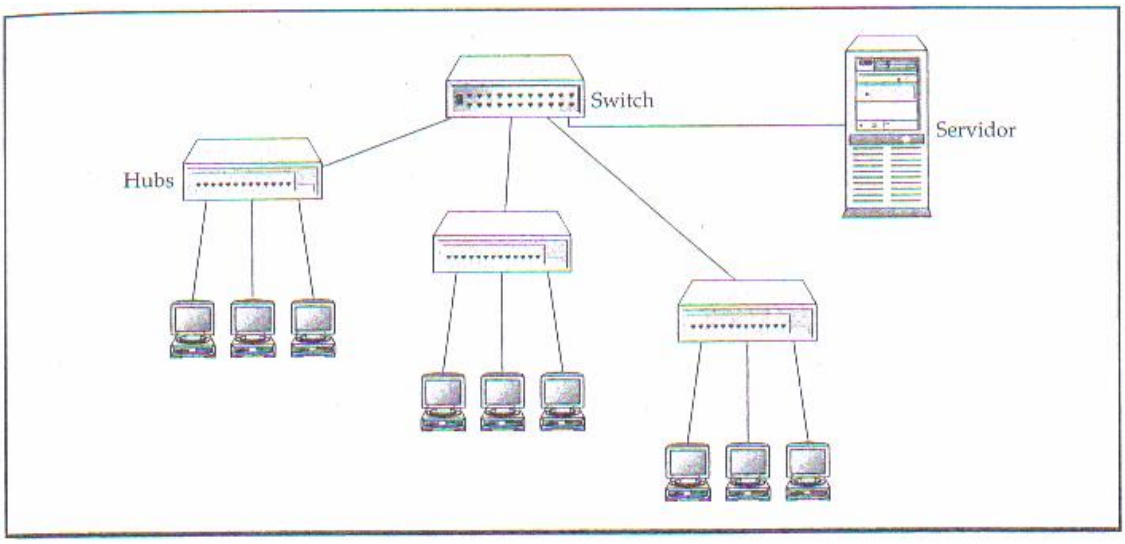

Figura 3.19 Red instalada que utiliza hubs y switches.

3.5.4 PUENTES

Los puentes son, en pocas palabras, versiones de repetidores más inteligentes.

Los puentes pueden conectar dos segmentos de red entre si, pero tienen la inteligencia suficiente para enviar trafico de un segmento a otro solo cuando el trafico esta destinado para ese otro segmento. Por tanto, los puentes se utilizan para segmentar redes en tramos más pequeños. Se encuentran también disponibles algunos puentes que pueden conectar sistemas de conectividad de redes y medios de transmisión diferentes, como cable coaxial Thin Ethernet y par trenzado Token Ring.

Como puede recordar, los repetidores operan a nivel capa física del modelo OSI para la conectividad de redes. Los puentes trabajan una capa mas arriba, en la capa de enlace de datos[35]. Los puentes analizan la dirección de control de acceso al medio de cada paquete que encuentran a fin de determinar si deben de enviar dicho paquete a otra red. Los puentes contienen información acerca de la dirección de todas las partes de su red, a través ya sea de una tabla de enrutamiento estática que usted programa o de un sistema dinámico de aprendizaje tipo árbol que busca automáticamente todos los dispositivos y direcciones en la red.

[35] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

Los puentes se deben utilizar solo en redes pequeñas, o en casos donde usted tenga que utilizar un repetidor, pero que se beneficiaria al evitar que trafico en un segmento se transmitiera en el otro segmento innecesariamente. A menudo los ruteadores o switches ofrecen soluciones que funcionan mejor y crean menos problemas, por lo que examine estas opciones antes de seleccionar un puente.

3.5.5 RUTEADORES

De la misma forma en que los puentes son, básicamente, más inteligentes que los repetidores, los ruteadores son más inteligentes que los puentes. Los ruteadores funcionan en la capa de red del modelo OSI y son más inteligentes que los puentes para enviar los paquetes entrantes a su destino final[36]. Debido a que los ruteadores trabajan en la capa de red, cualquier conexión a través del ruteador requiere solo que las capas superiores utilicen los mismos protocolos.

Los ruteadores pueden traducir cualquiera de los protocolos de las capas uno a tres a cualquier otro protocolo de las capas uno a tres (siempre y cuando el ruteador haya sido configurado y diseñado para hacerlo). Los ruteadores pueden conectar tanto redes similares como diferentes. A menudo se utilizan en los enlaces de las redes de área amplia (WAN).

En realidad, los ruteadores se convierten en un nodo de la red y tienen su propia dirección de red. Otros nodos envían paquetes al ruteador, que analiza el contenido de los paquetes y los transfiere a donde corresponda. (Por esta razón, con frecuencia los ruteadores están construidos con microprocesadores muy veloces, generalmente basados en computadoras basadas en un conjunto de instrucciones reducidas (RISC), y una gran cantidad de memoria en ellos a fin de llevar a cabo esta tarea). Los ruteadores también pueden determinar la ruta mas corta para alcanzar un destino y la usan. Pueden realizar otros trucos

[36] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

a fin de maximizar el ancho de banda de la red y, de forma dinámica, se ajustan a los problemas cambiantes o patrones de trafico de una red.

Los ruteadores forman la espina dorsal del Internet. Cuando usted utiliza el comando TRACERT para rastrear la ruta desde un nodo hacia un destino, la mayoría de las direcciones que aparecen en los saltos son, en realidad, rutas diferentes, cada una de las cuales envía el paquete al nodo siguiente hasta que llega a su destino.

Los ruteadores deben programarse para funcionar de manera correcta.

Necesitan tener las direcciones asignadas a cada uno de sus puertos y deben configurarse diferentes parámetros del protocolo de red[37]. Por otra parte, están generalmente programados en una de dos formas. Primero, la mayoría de ellos tiene un puerto RS-232C. Usted puede conectar una Terminal o una PC con software de emulación de Terminal a este puerto y programar el ruteador en modo texto. Segundo, la mayoría de los ruteadores tiene software basado en red que le permite programar el ruteador, a menudo utilizando herramientas graficas o una interfase web simple. El método que usted utilice depende del ruteador y sus necesidades de seguridad. (Quizás desee deshabilitar la programación de ruteador basado en la red, a fin de que los usuarios no autorizados no puedan modificar la programación del ruteador). La figura 3.17 muestra un ejemplo de una red que utiliza ruteadores.

[37] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

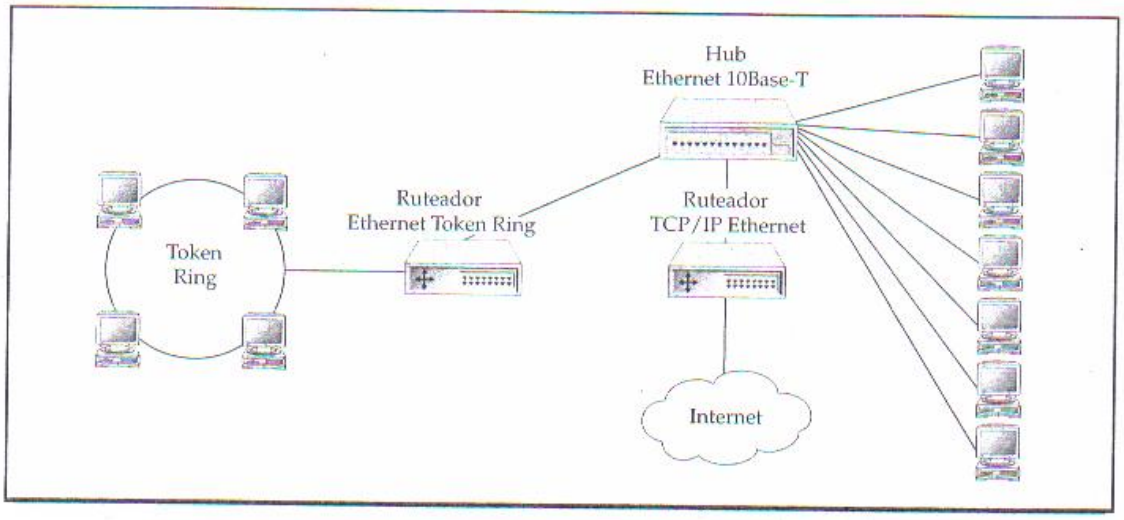

Figura 3.20 Ejemplo de una red que utiliza ruteadores.

3.5.6 COMPUERTAS

Las compuertas son interfases de aplicación específica que enlazan las siete capas del modelo OSI cuando son diferentes en uno o todos los niveles[38]. Por ejemplo, si usted necesita conectar una red que utilice uno de los modelos OSI para conectividad de redes a otro que utilice el modelo de IBM Systems Network Architecture (SNA), una compuerta podría realizar esta tarea. Las compuertas también pueden traducir, por ejemplo, de Ethernet a Token Ring, aunque existen soluciones más sencillas que utilizar compuertas si usted necesita dicha conversión. Debido a que las compuertas tienen que realizar muchas traducciones, tienden a ser más lentas que otras soluciones, particularmente, cuando trabajan bajo cargas de tráfico considerables.

En estos días, el uso principal de las compuertas es en el manejo del correo electrónico. POP3 y SMTP son dos ejemplos de protocolos para el manejo de correo que son administrados por compuertas. La mayoría de los sistemas de correo electrónico que pueden conectarse en sistemas disímiles, utilizan una computadora configurada como compuerta para llevar a cabo esa tarea o permiten que el servidor de correo electrónico, por si mismo, maneje las tareas de las compuertas.

[38] Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

3.5.7 PROTECCIÓN DE UNA RED CONTRA FIREWALLS

Firewalls, son dispositivos de hardware que refuerzan sus políticas de seguridad de la red. A menudo se instalan al mismo tiempo que los ruteadores.

Por ejemplo, firewalls se instalan a veces con los ruteadores para crear conexiones de interconectividad. En la mayoría de los ruteadores de las oficinas pequeñas u hogareñas, firewalls es parte del ruteador en si mismo. Sin embargo, el equipo de las redes más grandes aun lleva a cabo estas tareas en equipos diferentes.

Firewall es un dispositivo de hardware (que puede ser una computadora configurada para esta tarea en particular, que corra software de firewall o un dispositivo dedicado de firewall que contenga una computadora dedicada) que se instala entre las dos redes y refuerza las políticas de seguridad. En general, firewalls se colocan entre la LAN de una compañía e Internet, pero también puede utilizarse entre LAN y WAN cuando asi convenga.

Existen básicamente dos diferentes tipos de firewalls: basadas en red y basadas en la aplicación. Un firewall basada en red trabaja a nivel paquete y, usualmente, implementa una técnica llamada filtrado de paquetes, que permite que estos entre las redes se comparen con un conjunto de reglas programadas en firewall antes de que se les permita a los paquetes cruzar la frontera entre las dos redes.

Las reglas de filtrado de paquetes pueden admitir o rechazar paquetes que estén basados en la dirección fuente o la dirección destino, o basados en un puerto TCP/IP. Por otro lado, por lo general la aplicación basada en firewalls actúa en un papel proxy entre las dos redes, de forma que no circule trafico directamente entre las dos redes. En lugar de ello, firewall (generalmente llamada firewall proxy) actúa como un proxy para que los usuarios de una red interactúen con los servicios de otra red. Esta interacción proxy, en general, se lleva a cabo mediante una técnica llamada traducción de las direcciones de red (NAT), donde las direcciones de la red en la red interna no están expuestas

directamente a la red externa. En el modelo basado en la aplicación, firewall proxy se encarga de traducir las direcciones a fin de que se puedan llevar a cabo las conexiones.

Firewalls vienen en todas las formas y tamaños y varian en costo desde algunos cientos hasta miles de dolares. En realidad, estos dias uno puede comprar pequeñas firewalls personales para el hogar que cuesten menos de 200 dolares para dispositivos basados en hardware o de 40 dolares para software de firewall que puede instalarse en una computadora personal. Los diferentes dispositivos de firewall tienen distintas caracteristicas y abarcan tanto tecnicas basadas eb red como basadas en la aplicación para proteger la red. Firewalls tambien sirven como punto de auditoria del trafico entre las dos redes, utilizando herramientas de acceso y reporte a fin de que estas ayuden al administrador a detectar y tratar el trafico de red inapropiado.

3.5.8 CONEXIÓN DE DISPOSITIVOS RS-232 CON MÓDEMS DE CORTO ALCANCE

A pesar de que algunas personas consideran que el modem de corto alcance no es, en verdad, un dispositivo de red, es un dispositivo necesario para su red a fin de que pueda ofrecer conectividad punto a punto entre una estación de trabajo o Terminal y otro dispositivo. Los módems de corto alcance (a menudo llamados controladores de línea), le permiten a usted conectar entre si dos dispositivos RS-232 distantes. Los cables estándar RS-232C tienen un límite en cuanto a distancia de 50 a 100 pies. Los módems de corto alcance permiten que la misma conexión recorra una distancia de 5 millas utilizando un cable telefónico de trenzado simple.

A menudo, los módems de corto alcance son soluciones perfectas cuando una computadora necesite acceso por Terminal a un dispositivo remoto. Por ejemplo, un usuario puede necesitar acceder a una Terminal en un sistema telefónico PBX, que utilice un puerto RS-232C. Usted tiene dos opciones para ofrecer este acceso remoto: puede instalar módems convencionales en cada extremo y utilizar una conexión telefónica para conectar la estación de trabajo

al PBX, o emplear dos módems de corto alcance e instalar un cable de par trenzado entre los dos puntos. De acuerdo con que frecuencia se necesite el acceso y que tan lejos se encuentre el dispositivo, cualquier forma es válida.

En general, los módems de corto alcance son mas convenientes cuando los dos dispositivos a veces o siempre necesiten estar conectados e instalar un cable de par trenzado entre los dos puntos no sea demasiado costoso o difícil.

Los módems de corto alcance son muy baratos pues cuestan aproximadamente 100 dólares cada uno.

En la mayoría de los módems de corto alcance, dos pares de alambre conectan cada módem de corto alcance, aunque existen variantes de un solo par. En la variante de dos pares, un par se utiliza para transmitir datos y el otro para recibirlos. La mayoría de lo módems de corto alcance son full duplex, lo cual permite que la transmisión se lleve a cabo en ambas direcciones de manera simultánea.

Para enlazar dos dispositivos mediante módems de corto alcance, debe utilizar un cable estándar RS-232C para conectar cada dispositivo a su módem de corto alcance. Después, usted instala el alambre de par trenzado a un módem de corto alcance utilizando las instrucciones que vienen con el módem. Por ultimo, la mayoría de los módems de corto alcance necesitan alimentación externa, por lo que necesitan un contacto de energía para conectarlos. La figura 3.18 muestra un ejemplo de una conexión por módem de corto alcance.

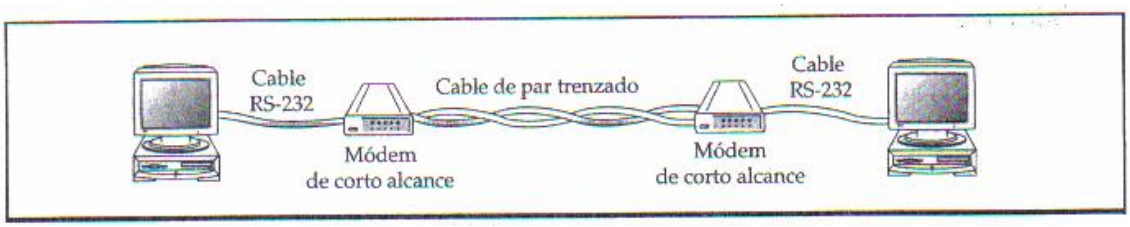

Figura 3.21 Conexión de módem de corto alcance.

CAPITULO IV

COMPARATIVO DE LA UTILIDAD DE LAS DIFERENTES REDES LAN

4.1 ESTUDIO COMPARATIVO ENTRE LAS TRES ARQUITECTURAS (ETHERNET, TOKEN RING Y ARCNET).

Se ha pretendido realizar un estudio comparativo, únicamente a efectos orientados, entre los tres tipos de arquitecturas descritos anteriormente, suponiendo que las tres se instalan con cable coaxial.

En cada una de las filas de la tabla se ha valorado del 1 al 3 en función de las posibilidades de cada una de ellas, obteniéndose los siguientes resultados.

	ETHERNET	TOKEN RING	ARCNET
COSTE	1	3	2
VELOCIDAD	1	2	3
INSTALACION	1	3	2
DISTANCIA	3	1	2
N° DE ESTACIONES	1	3	2

Tabla 4.1 Comparativo entre las tres arquitecturas

4.2 COMPARATIVO DE LOS TIPOS DE TRANSMISION

TIPO DE TRANSMISIÓN	TIEMPOS DE TRANSMISIÓN	EJEMPLOS
TRANSMISIÓN SÍNCRONA	TIEMPOS IGUALES	FRAME RELAY, ISDN, SDH
TRANSMISIÓN ASÍNCRONA	TIEMPOS DIFERENTES	ETHERNET, ATM, X,25
TRANSMISIÓN PLESINCRONA	TIEMPOS CASI IGUALES	PDH

Tabla 4.2 Comparativo entre los tipos de transmisión.

4.3 COMPARATIVA DE LOS DIFERENTES MEDIOS DE TRANSMISIÓN

Las tablas comparativas de todos los medios de transmisión mas importantes son en cuanto a velocidad máxima de transmisión, (un valor aproximado que no tiene en cuenta la longitud del cable), ancho de banda, distancia sin repetidores y otros aspectos de costo e instalación.

Las características de transmisión expuestas en la tabla 4.3 están directamente relacionadas con los medios especificados y no tienen que ver con los estándares utilizados. Hay que tener en cuenta que las limitaciones de transmisión no solo tienen que ver con los medios en cuestión, sino también con los dispositivos conectados a estos que se utilizan para adaptar convenientemente las señales y los protocolos de comunicación en los que se basen. Por lo tanto, la tabla 4.4 compara las características teóricas de los distintos medios, que en la práctica suelen tener valores algo inferiores.

Medio	Velocidad máxima de transmisión	Ancho de banda	Distancia entre repetidores
Par trenzado	1 Gbps	600 Mhz	2-10 Km
Coaxial	2Gbps	800 Mhz	10-100 Km
Fibra óptica	más de 10 Gbps	2 Ghz	más de 100 Km
Ondas de radio	1 Gbps		100-1000 Km
Microondas	10 Gbps	18-19 Ghz	80 Km
Infrarrojo	10 Gbps		200 m
Ondas de luz	1 Gbps		1 Km

Tabla 4.3 Resumen de las características de los medios de transmisión.

Característica	Cable coaxial Grueso	Delgado	Cable de pares trenzados UTP	STP/FTP
Velocidad de Transmisión	1 Gbps	10 Mbps	100 Mbps	1 Gbps
Longitud Máxima Segmento	500 m	200 m	100 m	100 m
Inmunidad Frente a Interferencias	Máxima	Buena	Mínima	Buena
Conectores Usados	Transceptor	BNC	RJ-45	RJ-45
Flexibilidad Física	Ninguna	Media	Máxima	Media
Dificultad de Instalación	Alta	Baja	Media	Alta
Costo	Alto	Bajo	Muy bajo	Bajo

Tabla 4.4 Comparación entre los distintos medios de cobre

4.4 DESCRIPCIÓN Y COMPARACIÓN DE REDES LAN RÁPIDAS.

En una red de área local (LAN), para cualquier usuario típico, una velocidad de conexión a la red de 10 Mbps era y es suficiente. Por ello, a este nivel redes Ethernet y Token Ring son alternativas válidas. Pero con la aparición de nuevas aplicaciones (CAD/CAM, transferencia de imágenes, etc.), de Intranets con servidores Web, o de servidores de bases de datos, esta velocidad ya no es suficiente para proveer la conectividad a grupos de servidores o la interconexión de grupos de trabajo a través de un backbone. Estos factores han generado la necesidad de incorporar en cualquier red institucional redes de alta velocidad, esto es con velocidades iguales o mayores a 100 Mbps.

En la actualidad, en aplicaciones para sistemas administrativos o comerciales, existen básicamente cinco ofertas tecnológicas en el campo de LAN con velocidades del orden de 100 Mbps. Entre estas tecnologías, Ethernet tiene la

preeminencia del mercado. En 1996, más del 83% de las conexiones de redes LAN eran Ethernet o Fast Ethernet. Esto representa sobre 120 millones de PCs, estaciones de trabajo y servidores interconectados. El resto de las conexiones de redes rápidas son alguna combinación de Token Ring, 100-VG-Anylan, Fiber Distributed Data Interface (FDDI) o Asynchronous Transfer Mode (ATM).

Como muestra la Tabla 4.5, la razón entre despachos Ethernet y ATM era de 255 a 1. Se prevé que esta diferencia no se reducirá significativamente en los próximos 5 años.

	Hubs+Switches ports (miles)	Network Interf. (miles)	% del total
Ethernet (10 y 100 Mbps)	62,151	33,507	89,71
Token Ring	5,823	3,996	9,21
FDDI	580	149	0,68
ATM (all speeds)	316	110	0,4

Tabla 4.5. Entregas mundiales de redes LAN en 1996 (ref. Gigabit Ethernet Applications, www.packetengines.com/wp/html/path.html)

De estas tecnologías, Token Ring actualmente provee sólo 4 y 16 Mbps y la versión HSTR (High Speed Token Ring) a 100 Mbps ha sido sólo recientemente propuesta por IBM a los organismos de estandarización, esperándose los primeros productos a mediados del 98. Por estas razones no será considerada en este análisis.

Las redes 100VG-AnyLAN tampoco serán consideradas por la baja aceptación que han tenido en el mercado pese a proveer una técnica de acceso al medio ligeramente superior al CSMA/CD de Ethernet.

Para velocidades mayores a 100 Mbps hay actualmente sólo dos tecnologías: ATM y Gigabit Ethernet.

Luego, las 4 arquitecturas de redes LAN rápidas que serán descritas y luego evaluadas son:

- Fast Ethernet
- FDDI
- ATM
- Gigabit Ethernet

4.5 Descripción de Tecnologías LAN rápidas.

4.5.1 FDDI

- FDDI transmite a velocidades de 100 Mbps sobre cable UTP categoria 5 (100 m entre repetidores), fibra óptica multimodo (2 km entre repetidores) y nimodo.

- Como método de acceso al medio utiliza token passing. Esta característica permite una baja degradación de performance con aumentos del tráfico (esto es, utiliza hasta 90% del ancho de banda).

- Utiliza una topología tipo anillo, ya sea anillo simple o doble. En la arquitectura de anillo doble, normalmente un anillo está activo, y cuando el anillo primario falla, el segundo entra en servicio gracias al protocolo SMT. La implementación de un anillo doble la hace altamente tolerante a fallas.

- FDDI permite transmitir frames de hasta 4500 bytes, permitiendo un throughput más alto que otras tecnologías que operan a la misma velocidad.

- Todas estas ventajas son contrapesados por un más alto costo (600 a 800% mayor que Fast Ethernet), lo cual la justifica sólo cuando se requieren conexiones a 100 Mbps con un alto grado de confiabilidad intrínseca respecto a daños del medio físico.

- Los datos pueden ser conmutados y ruteados hacia o desde una red Ethernet o Fast Ethernet sólo una vez que el formato y largo del frame son traducidos.

4.5.2 Fast Ethernet

- Fast Ethernet o 100BasetT (IEEE 802.3u) permite transmisiones a 100 Mbps sobre cable UTP categoría 5 y fibra óptica unimodo y multimodo.

- Al igual que la arquitectura Ethernet de 10 Mbps, Fast Ethernet (FE) utiliza la técnica de acceso a medios compartidos llamada CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Por ello, en medios compartidos, las colisiones resultantes hacen que FE pueda proveer tasas de transferencia de información sólo de 30 a 40%, con burst limitados de 90%, del ancho de banda del canal.

- FE utiliza el mismo formato y largo de frame que Ethernet (1518 bytes), por lo cual no requiere cambios en los protocolos de capas superiores, aplicaciones y software de redes para que sean ejecutados en computadores pertenecientes a una red de área local (LAN) que evoluciona desde esta popular tecnología.
- En el caso de FE conmutado (switched Fast Ethernet), una nueva característica es la opción de utilizar la capacidad fullduplex del medio, eliminando las colisiones y limitaciones topológicas (e.g. el largo del

dominio de colisiones). La operación fullduplex puede ser configurada manualmente o mediante auto configuración. De esta forma, FE provee el doble de ancho de banda que FDDI (i.e. 200 Mbps), con comunicación bidireccional simultánea a una distancia máxima de 2 Km utilizando fibra óptica multimodo. Utilizando FE conmutado se tiene el perfil de performance (sin colisiones ni degradación) y características de redundancia necesarias para ser aplicada en backbones.

- Las dos mayores ventajas de FE respecto a FDDI es su costo más bajo y su fácil integración a la arquitectura Ethernet tradicional. Sus características de autonegociación y autosensing de la velocidad de comunicación facilitan esta tarea. Por ello su aplicación está aumentado rápidamente en conectividad de sistemas cliente servidor.

4.5.3 Asynchronous Transfer Mode (ATM) y ATM LAN Emulation

- ATM es una tecnología de multiplexing y conmutación orientada a la conexión, que utiliza celdas de 53 bytes (5 bytes de header, 48 bytes de data). El tamaño de las celdas utilizadas la adecua a la transmisión simultánea de voz, video y datos.

- Existen a lo menos cuatro alternativas para la aplicación de Raw ATM a redes de datos: LAN encapsulation in ATM (RFC 1483), Classical IP over ATM (RFC 1577, Jan. 1994), ATM LAN emulation (LANE) versión 1.0 y 2.0 (1995 y 1996), y Multi Protocol over ATM (MPOA).

- El uso de Classical IP over ATM exige que ambos dispositivos soporten el estándar ATM tanto a nivel físico como del protocolo en los niveles superiores. Classical IP se utiliza fundamentalmente en la interconexión de redes locales para formar una WAN o en el backbone de redes LAN, donde el tráfico es solamente IP. Esta característica permite ejecutar los protocolos del nivel de transporte TCP y UDP y aplicaciones tales como WWW, FTP, NFS, directamente sobre ATM.

- Al utilizar Classical IP con circuitos virtuales ATM permanentes (PVC), las direcciones IP deben asociarse manualmente a las direcciones ATM. Si los circuitos virtuales son conmutados, debe incluirse un servidor ATMARP (ATM Address Resolution Protocol).

- ATM LAN emulation consiste en un servicio Raw ATM mas una capa de adaptación a los estándares de capa MAC (Media Access Control) ya establecidos en redes locales (Ethernet o Token Ring). De esta forma se puede utilizar todos los drivers y adaptadores de estos estándares establecidos, generándose la interoperabilidad entre backbones ATM y grupos de trabajo operando con tecnologías de menor velocidad.

- La configuración típica donde es aplicable LANE es una LAN con Ethernet (o Fast Ethernet) operando con un backbone ATM. En este caso el protocolo sobre Ethernet probablemente será TCP/IP. Cuando no se defina una red desde cero sino que ya existen redes no ATM operando, la mejor alternativa para incorporar ATM será LANE o MPOA.

- Las dos velocidades actualmente más utilizadas son 155.52 Mbps (OC-3) y 622.08 Mbps (OC-12), y el nivel físico está determinado por el estándar SONET/SDH.

- Una de las grandes ventajas de ATM es que provee servicios de asignación dinámica del ancho de banda total para cada uno de los usuarios que comparten el canal físico, creando canales y pasos virtuales.

- Raw ATM ofrece varias clases de servicio. Servicio Clase C (variable bit rate, asynchronous) es el que se adecua al tráfico típico de una LAN. Por ello el protocolo de la ATM Adaptation Layer (AAL) es el tipo ¾ (bit rate variable).

- ATM ofrece tres tipos de transmisión:

- Full duplex a 155.54 Mbps en cada dirección
- Subscriptor a red a 155.54 Mbps y red a subscriptor a 622.08 Mbps
- Full duplex a 622.08 Mbps

	Medio	Dist. Max.	Estándar	Código
Full duplex 155.54 Mbps	Coaxial (dos)	100 a 200 m	G.703	CMI
	Fibra Optica single mode	800 a 2000 m	G.652	NRZ
Half o Full duplex 622 Mbps	Fibra Optica single mode	800 a 2000 m	G.652	NRZ

Tabla 4.6 Características redes ATM

4.5.4 Gigabit Ethernet (IEEE 802.3z)

- Basada en la casi aceptación universal de la tecnología Ethernet 10Base-T operando a 10 Mbps, la tecnología Fast Ethernet ha provisto una evolución suave y no disruptiva hacia el performance de 100 Mbps. Análogamente, Gigabit Ethernet provee un ancho de banda de 1 Gbps para redes de campus con la simplicidad de Ethernet a un costo más bajo que otras tecnologías de velocidades similares.

- Gigabit Ethernet usa el mismo protocolo (CSMA/CD), el mismo formato y tamaño de frame que sus predecesores operando a 10 y 100 Mbps. Además, también soporta operación half-duplex (en segmentos compartidos o shared) y full-duplex, permitiendo en esta segunda modalidad la implementación debackbones conmutados operando a 2 Gbps.

- Dos nuevas características han sido agregadas a CSMA/CD para permitir una operación eficiente halfduplex en el diámetro práctico del

dominio de colisiones resultante de la velocidad de 1000 Mbps. Estas dos características que solo afectan al modo de operación half-duplex son: carrier extension y packet bursting. Carrier extension permite adaptar paquetes de menos de 512 bytes, a dicho largo mínimo tal que las colisiones sean detectables en la extensión total del segmento. Packet bursting permite a los dispositivos enviar grupos de paquetes pequeños de forrma tal de maximizar la utilización del ancho de banda.

- En el modo full-duplex, la operación es idéntica a Fast Ethernet, sólo más rápida. Esto es, los dispositivos continúan utilizando el interframe gap de 96 bits y largo mínimo de paquete de 64 bytes. La operación full-duplex es posible sobre la longitud máxima del enlace especificada para cada medio físico de transmisión.

- Un nuevo dispositivo es introducido, llamado buffered distributor o fullduplex repeater. Este es un dispositivo fullduplex, multipuerta, similar a un hub el cual interconecta 2 o más enlaces 802.3 operando a 1 Gbps o más rápido. Al igual que el repetidor 802.3, es un dispositivo que no filtra direcciones, sino que envía todos los paquetes que arriban a todos los enlaces conectados excepto el enlace de origen, proveyendo de esta forma un dominio de ancho de banda compartido comparable al dominio de colisiones de 802.3. A diferencia del repetidor 802.3, el distribuidor con buffer puede acumular uno o más frames arribados por cada enlace antes de reenviarlos. Además incorpora control de flujo implementando el estándar IEEE802.3x, lo cual elimina la posibilidad de pérdida de frames por rebalse del buffer.

- De este modo, Gigabit Ethernet ofrece el modo de operación fullduplex no sólo en switches sino que también en Hubs. Así un hub Gigabit Ethernet operando en el modo de repetidor fullduplex (i.e. sin colisiones) puede alcanzar un tasa de transferencia de hasta 95% del ancho de banda disponible (1 Gbps aproximadamente en cada dirección), aun operando con paquetes pequeños. Por lo tanto, el repetidor fullduplex es particularmente adecuado a redes many-to-one. En aplicaciones many-

to-many debiera utilizarse un switch, el cual puede proveer un ancho de banda mayor a 1 Gbps.

- Al igual que los dispositivos switch/router Fast Ethernet, los switches Gigabit Ethernet utilizando el estado del arte de la tecnología ASIC, implementarán la capacidad de ruteo a las velocidades máximas del estándar (wirespeed routing) para comunicaciones IP. Los equipos más sofisticados tendrán la capacidad multiprotocolo (IP/IPX). Esta característica es cada vez más importante considerando que el pattern de tráfico 80/20 que representaba la razón de tráfico típica entre tráfico local e intersubred, tiende a igualarse e incluso invertirse.

- Gigabit IEEE 802.3z provee dos estándar para la capa física utilizando fibra óptica (FO) y dos estándar para cable de cobre. Los estándares de FO corresponden a una mejora de la tecnología actual de la especificación ANSI para la capa física de Fibre Channel la cual opera a 1.063 Mbps, tal que pueda operar a 1.250 Mbps y de esta forma proveer el data rate de 1000 Mbps de Gigabit Ethernet. Por ende, Gigabit Ethernet utiliza el mismo esquema de codificación/decodificación para los datos digitales que Fibre Channel, esto es 8B/10B.

4.5.5 Características de los enlaces Gigabit Ethernet.

1000Base-SX

- Pensada para backbones horizontales de hasta 300 m de longitud.

- Utiliza fibra óptica multimodo de 50 um de diámetro y LED de radiación de corta longitud de onda (850 nm).

1000Base-LX

- Para backbones verticales de hasta 550 m de longitud utilizando FO multimodo de 62.5 um de diámetro y LED se larga longitud de onda (1300 nm).

- Para backbones de campus de hasta 5 Km utilizando FO monomodo con diodos láser operando en 1300 nm.

1000Base-CX

- Pensada para los closets de conmutación y salas de computación con un largo máximo de 25 m.

- Utiliza cable twinax, blindado, balanceado, de 150 Ohm.

- Utiliza codificación Fibre-Channel-based 8B-10B.

1000BaseTX

- Utilizará 4 pares de cable UTP categoría 5 con una distancia máxima de 100 m permitiendo redes de hasta 200 m de diámetro.

- NO está aun disponible.

Notas:

- La fibra óptica más utilizada es la graded index MMF 62.5/125 mm (esto es, 62.5 mm fiber optic core y 125 mm outer cladding).

- Para distancias pequeñas se utiliza radiación de 850 nm (shortwave) y el emisor de radiación es normalmente un LED. Para

distancias mayores se utiliza radiación de 1300 nm (longwave), normalmente manteniendo el LED como fuente de radiación.

- Para fibras monomodo deben utilizarse diodos láser, y el diámetro del núcleo de la fibra puede reducirse de 50 a 9 mm.

- La atenuación típica de FO operando a 850 nm es de 1.5 dB/km y a 1300 nm es de 2 dB/km y de 0.5 a 2 dB por punto de interconexión.

- El ancho de banda y rango de distancias especificado por el estándar, se muestran en la Tabla 4.7:

Estándar	Tipo Fibra	Diámetro (micrones)	Longitud de onda (nm)	Ancho de banda (MHz @1000 m)	Rango Min. (m)
1000Base-SX	MM	62,5	850	160	2 A 220*
1000Base-SX	MM	62,5	850	200	2 A 275 **
1000Base-SX	MM	50	850	400	2 A 500
1000Base-SX	MM	50	850	500	2 A 550***
1000BaseLX	MM	62,5	1300	500	2 A 550
1000BaseLX	MM	50	1300	400	2 A 550
1000BaseLX	MM	50	1300	500	2 A 550
1000BaseLX	SM	9	1300	NA	2 A 5000

Tabla 4.7 Comparativo de los enlaces Gigabit Ethernet.

Notas:

***The TIA 568 building wiring standard specifies 160/500 MHz*km multimode fiber.

**** The international ISO/IEC 11801 building wiring standard specifies 200/500 MHz*km multimode fiber.

***** The ANSI Fibre Channel specification specifies 500/500 MHz*km 50 micron multimode fiber and 500/500 MHz*km fiber has been proposed for addition to ISO/IEC 11801.

4.6 Comparación de Tecnologías LAN rápidas.

Los criterios principales de evaluación de las arquitecturas ya descritas serán:

- Disponibilidad y tolerancia a fallas.
- Capacidad de transferencia de información.
- Escalabilidad que posibilite crecimiento futuro.
- Adaptabilidad a cambios tecnológicos.
- Estandarización de medios de transmisión y protocolos de transferencia de datos.

4.6.1 Fast Ethernet vs. FDDI

En la especificación de backbones de LAN a 100 Mbps, las dos principales tecnologías a considerar son FDDI y Fast Ethernet (FE).

- En un ambiente de backbone conmutado, FE tiene ventajas sobre FDDI ya que provee el doble de velocidad.

- Conexión desde FE o Ethernet a FDDI requiere traducción de los frames con el consecuente mayor retardo y latencia. Esto no sucede al conmutar Ethernet a FE. El performance de una transferencia de datos sostenida, en un ambiente conmutado, está dado por la técnica de arbitración del bus conmutado y la capacidad del backplane del dispositivo. Sin embargo, en conexiones punto-a-punto con FE conmutado CSMA/CD no juega un rol relevante, obteniéndose así su máxima velocidad y estando el performance sólo determinado por la velocidad del dispositivo conmutador (Switch).

- FDDI es capaz de transferir frames más largos por lo que su troughput sería mayor que FE en la transferencia de archivos entre dos servidores en un ambiente compartido. Sin embargo, el tamaño de un frame IP en una red cliente-servidor es, en promedio, entre 200 y 256 bytes. Además, si los clientes son Ethernet, los frames nunca serán más largos que el largo máximo Ethernet. Por ello, en este caso los servidores FE tienen el mismo troughput que FDDI y con una latencia menor.

- Pruebas realizadas por la revista Data Communications muestran que manipulando frames de 64 bytes, los adaptadores 100BaseT utilizan el 58% del ancho de banda. Pero en el caso de frames de 1500 bytes utilizan el 99% del ancho de banda, de tal forma que el usuario, servidor o aplicación obtiene el throuhput máximo de 200 Mbps.

- Por lo tanto, los usuarios obtienen un gran aumento de performance al usar 100BaseT fullduplex en servidores de disco, servidores multimedia, conexiones peer-to-peer, y conexiones backbone.

- En un ambiente compartido, FDDI potencialmente ofrece una mejor tolerancia a fallas al utilizar conexiones con anillos duales (FDDI-DAS). Sin embargo, FE también provee alternativas de tolerancia a fallas, a través del Spanning-Tree Protocol (IEEE802.3d), en el cual se mantiene activo sólo uno de dos enlaces redundantes, generándose el swithover en caso de falla. STP tiene la desventaja de ser lento (20 a 30 seg. de retardo). Para failover instantáneo se pueden utilizar transceivers FE tolerante a fallas, los cuales monitorean por hardware el enlace activo y producen el failover de ser necesario. Esta alternativa tiene sólo 1/2 del costo de la interfaz FDDI-DAS.

4.6.2 Raw ATM vs IP sobre ATM y FDDI.

- En una configuración de nodos back-to-back conectados con un enlace OC-3, Classical IP sobre ATM presenta mayores latencias que aquellas obtenidas usando FDDI, particularmente para mensajes pequeños.

- Sin embargo, para un enlace de la misma velocidad (OC-3), IP sobre ATM vía switches ATM puede exhibir un mejor performance que switches o ruteadores FDDI, debido a la optimización de los switch ATM para celdas de tamaño fijo. Esto indica que ATM es una mejor base que FDDI para implementar comunicaciones internetwork.

- Al utilizar Raw ATM, con Fore ATM API y con la capa de adaptación AAL ¾, se obtienen latencias significativamente más bajas que con las configuraciones equivalentes usando IP sobre ATM o FDDI. Esto es lógico, pues en este caso se elimina la capa de emulación y el costo de la emulación asociado.

- Sin embargo el costo de llevar raw ATM hasta el usuario final es mucho más alto que utilizar tecnologías Ethernet, por lo cual actualmente la tendencia es utilizar ATM en el backbone o la interconexión de redes.

4.6.3 Gigabit Ethernet vs ATM

- Las conexiones Gigabit Ethernet se espera que serán de menor costo que las interfaces ATM de 622 Mbps (asumiendo idénticas interfaces físicas) debido a la simplicidad relativa de Ethernet y mayores volúmenes de producción. Por ejemplo los dispositivos repetidores Gigabit Ethernet serán significativamente más baratos que conexiones ATM de 622 Mbps, proveyendo alternativas de mayor relación costo beneficio para backbones de redes de datos y conexiones a servidores (ver Tabla 4.8).

Tecnología	Tipo de Equipo	1996 Precio/Puerta	1998 Precio/Puerta	Cambio %
Shared Fast Ethernet	Hub	$137	$102	-25%
Switched Fast Ethernet	Switch	$785	$500	-38%
Shared FDDI	Concentrator	$835	$680	-19%
Switched FDDI	Switch	$4000	$3200	-20%
ATM 622 Mbps [1]	Switch	$6600	$4200	-36%
Shared Gigabit Ethernet [2]	Hub	NA	$920 a $1400 [3]	
Switched Gigabit Ethernet [2]	Switch	NA	$1850 a $2800 [3]	

Tabla 4.8 Precios de conexiones para backbone de redes

[1] Estimación para fibra multimodo

[2] IEEE goal para fibra multimodo

[3] Estimación Dell'Oro Group e IEEE goals. (2x a 3x Fast Ethernet MM)

- La emergencia de aplicaciones Intranet promueve la migración a nuevos tipos de datos, incluyendo video y voz. En el pasado se pensaba que video requeriría una tecnología de redes diseñada específicamente para multimedia. Esta fue la razón principal que impulsó el desarrollo de ATM, el cual incluye en forma nativa capacidades avanzadas para multimedia, llamadas Quality of Service (QoS). Pero hoy en día es posible mezclar datos y video en redes Ethernet mediante la combinación de los siguientes factores:

- El aumento de ancho de banda provisto por Fast Ethernet y Gigabit Ethernet, el cual es a su vez aumentado por la técnica de LAN conmutadas y comunicación fullduplex. En efecto, mientras mayor es el ancho de banda, menor es el efecto sobre aplicaciones temporalmente críticas (transmisión de voz o video) de variables tales como delay o delay variation (jitter).

- El desarrollo de nuevos protocolos, tal como Resource Reservation Protocol (RSVP), que provee la posibilidad de reservar ancho de banda y por lo tanto de asegurar QoS. Esta posibilidad estaba previamente reservada sólo a Raw ATM.

- El desarrollo de nuevos estándares tales como 802.1Q (priorización) y/o 802.1p (tagging), los cuales proveen facilidades para entregar QoS utilizando información de prioridad explícita para los paquetes en la red.

- Switches sofisticados utilizando las prioridades embebidas en los paquetes por los protocolos antes mencionados, junto con el manejo de colas internas de paquetes, proveerán ruteo con QoS.

- El amplio uso de compresión de video avanzada tal como MPEG-2.

4.6.4 Distancias máximas permitidas

	Ethernet 10 BaseT	Fast Ethernet 100 BaseT	Gigabit Eth. 1000 Base X	FDDI	ATM full duplex
Data Rate	10 Mbps	100 Mbps	1000 Mbps	100 Mbps	155 Mbps
Cat 5 UTP	100 m (min)	100 m	100 m (3)	NA	NA
STP/Coax	500 m	100 m	25 m	NA	100-200 m
Multimode Fiber	2 km	412 m (1) 2 km (2)	200 m (1) 550 m (2)	2 km	
Single-mode Fiber	32 km	20 km	5 km	20 km	800-2000 m

Tabla 4.9 Comparación de las restricciones de distancia de los diferentes estándares

(1) IEEE spec half duplex

(2) IEEE spec full duplex

(3) IEEE 802.3ab bajo estudio

CONCLUCIÓN

Con la evolución que cada día sufre los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, se puede decir que igualmente se ha incrementado el número de usuarios que trabajan con computadoras haciéndolas ya una necesidad, no sin antes destacar él Internet; una vía de comunicación efectiva, eficaz y rapidísima, donde nos une a todo el mundo por medio de una computadora. Y es en todo esto que se ve involucrado el tema de la presente tesis. Ya que a lo largo de la misma se ha visto que la Red de Área Local en una estructura que se necesita conocer y dominar donde no debemos de olvidar que se manejan entre otras cosas los protocolos TCP/IP. Permite a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información.

GLOSARIO

Administración de red: Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

Ancho de banda: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

Aplicación: Programa que ejecuta una función directamente para un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red.

Atenuación: Pérdida de energía de la señal de comunicación

Autenticación: Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Binario: Sistema numérico compuesto por unos y ceros (1 = encendido; 0 = apagado).

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

Broadcast: Paquete de datos enviado a todos los nodos de una red.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit.

Cable coaxial: Cable que consta de un conductor cilíndrico externo hueco, que reviste a un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohms, utilizado para la señalización

digital, y el cable de 75 ohms, utilizado para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

Cableado de categoría 1: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 1 se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos. Ver también UTP.

Cableado de categoría 2: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 2 puede transmitir datos a velocidades de hasta 4 Mbps. Ver también UTP.

Cableado de categoría 3: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps. Ver también UTP.

Cableado de categoría 4: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Ver también UTP.

Cableado de categoría 5: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps. Ver también UTP.

Capa de aplicación: Capa 7 del modelo de referencia OSI. Esta capa brinda servicios de red para aplicaciones del usuario. Por ejemplo, una aplicación de

procesamiento de textos recibe servicios de transferencia de archivos en esta capa. Ver también modelo de referencia OSI.

Capa de enlace de datos: Capa 2 del modelo de referencia OSI. Esta capa proporciona un tránsito de datos confiable a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y control de flujo. IEEE dividió esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. A veces se denomina simplemente capa de enlace.

Capa de presentación: Capa 6 del modelo de referencia OSI. Esta capa suministra representación de datos y formateo de códigos, junto con la negociación de la sintaxis de transferencia de datos. Asegura que los datos que llegan de la red puedan ser utilizados por la aplicación y garantiza que la información enviada por la aplicación pueda transmitirse a través de la red. Ver también modelo de referencia OSI.

Capa de red: Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento. Equivale aproximadamente a la capa de control de ruta del modelo SNA. Ver también modelo de referencia OSI.

Capa de sesión: Capa 5 del modelo de referencia OSI. Esta capa establece, mantiene y administra las sesiones entre las aplicaciones. Ver también modelo de referencia OSI.

Capa de transporte: Capa 4 del modelo de referencia OSI. Esta capa segmenta y reensambla los datos dentro de una corriente de datos. La capa de transporte tiene el potencial de garantizar una conexión y ofrecer transporte confiable. Ver también modelo de referencia OSI.

Capa física: Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para

activar, mantener y desactivar el enlace físico entre sistemas finales. Corresponde a la capa de control físico del modelo SNA. Ver también modelo de referencia OSI.

Carga: Parte de una celda, trama o paquete que contiene información de capa superior (datos).

Carga: Cantidad de actividad de un recurso de la red, como por ejemplo un router o un enlace.

Cifrado, codificado (encryption)**:** Método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza normalmente en Internet para sustraer el correo electrónico.

Circuito: Ruta de comunicaciones entre dos o más puntos.

Circuito asíncrono: Señal que se transmite sin sincronización precisa. Estas señales normalmente tienen diferentes frecuencias y relaciones de fases. Las transmisiones asíncronas habitualmente encapsulan caracteres individuales en bits de control (denominados bits de inicio y detención) que designan el principio y el final de cada carácter. Ver también circuito síncrono.

Circuito síncrono: Señal transmitida con sincronización precisa. Estas señales tienen la misma frecuencia, y los caracteres individuales están encapsulados en bits de control (denominados bits de arranque y bits de parada) que designan el comienzo y el fin de cada carácter.

Codificación: Técnicas eléctricas utilizadas para transmitir señales binarias.

Codificación: Proceso a través del cual los bits son representados por voltajes.

Colisión: En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Comunicación: Es el proceso que involucra a un emisor y a un receptor mediante un mensaje a través de un canal.

Concentrador: Ver hub.

Congestión: Tráfico que supera la capacidad de la red.

Conmutación: Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

Conmutación asimétrica: Tipo de conmutación que brinda conexiones conmutadas entre puertos de ancho de banda diferente, como una combinación de puertos de 10 Mbps y 100 Mbps.

Conmutación de circuito: Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la "llamada". Se usa ampliamente en la red de la compañía telefónica. La conmutación de circuito se puede comparar con la contención y la transmisión de tokens como método de acceso de canal y con la conmutación de mensajes y la conmutación de paquetes como técnica de conmutación.

Conmutación de paquetes: Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes.

Conmutación rápida: Conmutación que ofrece el nivel más bajo de latencia, enviando inmediatamente un paquete después de recibir la dirección destino.

Conmutación sin fragmentos: Técnica de conmutación que filtra, antes de que comience el envío, los fragmentos de colisión que constituyen la mayoría de los paquetes de errores.

Conmutador: Un conmutador (switch) en un dispositivo de conexión que permite la transmisión de datos desde distintos equipos de una red al mismo tiempo.

Control de Acceso al Medio: Ver MAC.

CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones): Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Datagrama IP: Unidad fundamental de información transmitida a través de la Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación del encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

Datos: Datos de protocolo de capa superior.

Dirección: Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular

Dirección IP: Es la dirección de red del ordenador. La dirección IP esta formada por cuatro números comprendidos entre valores de 0 a 255.

DNS: Las direcciones IP son difíciles de recordar por eso se utiliza los DNS. Son un conjunto de palabras más fáciles de recordar.

Dominio (domain): Nombre empleado para referirse a una máquina o a un servidor determinado en Internet. El nombre de dominio comprende varias partes; la última parte, o sufijo, designa el nivel de estructura superior.
Ejemplos de dominios:
.com (organizaciones comerciales)
.edu (organizaciones educativas)
.gob (organizaciones gubernamentales)

Encabezado: Información de control colocada antes de los datos al encapsularlos para la transmisión en red.

Encapsulamiento: Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.

Encapsular: Colocar un encabezado de protocolo en particular a los datos. Por ejemplo, a los datos de Ethernet se les agrega un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red simplemente se coloca en el encabezado utilizado por el protocolo de enlace de datos de la otra red.

Enlace: Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor. Se utiliza con mayor frecuencia para referirse a una conexión de WAN. A veces se denomina línea o enlace de transmisión.

Enrutamiento: Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Estándar: Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet: El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

Ethernet de dúplex completo: Capacidad de transmisión simultánea de datos entre una estación emisora y una estación receptora. Comparar con Ethernet semidúplex.

Ethernet semidúplex: Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con Ethernet de dúplex completo.

Fast Ethernet : Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3. Ver también Ethernet.

Fibra multimodo: Fibra óptica que soporta la propagación de múltiples frecuencias de luz.

Fibra óptica: Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda electromagnética generada por un láser.

Filtrado de tráfico local: Proceso por el cual un puente filtra (descarta) tramas cuyas direcciones MAC origen y destino se ubican en la misma interfaz en el puente, lo que evita que se envíe tráfico innecesario a través del puente. Definido en el estándar IEEE 802.1.

Filtro: En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Flujo: Corriente de datos que viajan de un punto a otro a través de una red (por ejemplo, desde una estación de la LAN a otra). Se pueden transmitir varios flujos en un solo circuito.

Fragmentación: Proceso de dividir un paquete en unidades más pequeñas al transmitir a través de un medio de red que no puede acomodar el tamaño original del paquete.

Fragmento: Parte de un paquete mayor que se ha dividido en unidades más pequeñas. En las redes Ethernet, también se hace referencia a esto como una trama con un límite inferior al límite permitido de 64 bytes.

Frame Relay: Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un

encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FTP (Protocolo de Transferencia de Archivos): Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

Full dúplex: Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora. Comparar con semidúplex y unidireccional.

Gateway: En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con router.

Gateway de último recurso: Router al cual se envían todos los paquetes no enrutables.

Gb (gigabit): Aproximadamente 1.000.000.000 de bits.

Gbps (gigabytes por segundo): Medida de velocidad de transferencia.

Gigabit: Ver Gb

Host: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers. Ver también nodo.

Hub : 1. En general, dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto.
2. Dispositivo de hardware o software que contiene múltiples módulos de red y

equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

IEEE (Instituto de Ingeniería Eléctrica y Electrónica): Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares de mayor importancia para las LAN de la actualidad.

IEEE 802.2: Protocolo de LAN de IEEE que especifica una implementación del la subcapa LLC de la capa de enlace de datos. IEEE 802.2 maneja errores, entramados, control del flujo y la interfaz de servicio de la capa de red (Capa 3). Se utiliza en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT y 10Broad36. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFX.

IEEE 802.5: Protocolo de LAN de IEEE que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4 ó 16 Mbps en cableado STP o UTP y desde el punto de vista funcional y operacional es equivalente a Token Ring de IBM. Ver también Token Ring.

Interfaz: 1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

Internet: La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general internet.

Internet: Abreviatura de internetwork de redes. No debe confundirse con la Internet.

IP (Protocolo Internet): Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo. Ver también IPv6.

IPv6 (IP versión 6): Reemplazo de la versión actual de IP (versión 4). IPv6 brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para identificar flujos. Anteriormente denominado IPng (IP de próxima generación).

ISO (Organización Internacional para la Normalización): Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

kb (kilobit): Aproximadamente 1.000 bits.

kB (kilobyte): Aproximadamente 1.000 bytes.

kbps (kilobits por segundo): Medida de velocidad de transferencia.

kBps (kilobytes por segundo): Medida de velocidad de transferencia.

Kilobit: Ver kb.

kilobits por segundo: Ver kbps.

Kilobyte: Ver kB.

Kilobytes por segundo: Ver kBps.

LAN (red de área local): Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

MAC (Control de Acceso al Medio): Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. Ver también capa de enlace de datos.

Mapa de ruta: Método para controlar la redistribución de rutas entre dominios de enrutamiento.

Máscara: Ver máscara de dirección y máscara de subred.

Máscara de dirección: Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se llama simplemente máscara.

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Máscara wildcard: Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se

compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

Mb (megabit): Aproximadamente 1.000.000 de bits.

megabits por segundo: Ver Mbps.

megabyte: Ver MB.

Modelo de referencia OSI (Modelo de referencia de internetwork de sistemas abiertos): Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes. La capa inferior (la capa física) es la más cercana a la tecnología de los medios. Las dos capas inferiores se implementan en el hardware y en el software, y las cinco capas superiores se implementan sólo en el software. La capa superior (la capa de aplicación) es la más cercana al usuario. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red. Similar en algunos aspectos a SNA. Ver capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

MTU (**unidad máxima de transmisión):** Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

Multiplexión: Esquema que permite que varias señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo. Comparar con demultiplexión.

Nodo: Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales; pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

NOS (sistema operativo de red): Sistema operativo utilizado para hacer funcionar una red, como, por ejemplo, NetWare de Novell y Windows NT.

OSI (**internetwork de sistemas abiertos):** Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados entre sí que operan de forma conjunta y, como grupo, dirigen la comunicación a alguna o a todas las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo, y a menudo un solo protocolo de la pila se refiere a varias capas a la vez. TCP/IP es una pila de protocolo típico.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos.

Protocolo: Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP. Comparar con protocolo enrutado.

Protocolo enrutado: Protocolo que puede ser enrutado por el router. Un router debe ser capaz de interpretar la internetwork de redes lógica según lo que especifique dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados. Comparar con protocolo de enrutamiento.

Protocolo exterior: Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común.

Red: Sistema de interconexión de ordenadores que permite compartir recursos e información.

También se puede definir como estructura formada por un conjunto de elementos tanto físicos como lógicos, con el fin de conseguir la interconexión de varias estaciones y poder así llevar la información de unas a otras.

Una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación.

Red de área local: Ver LAN.

Reensamblaje: Colocación en su formato original de un datagrama IP en el destino después de su fragmentación en el origen o en un nodo intermedio.

Rendimiento: Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

Repetidor: Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

Reserva de ancho de banda: Proceso de asignar ancho de banda a usuarios y aplicaciones que reciben servicios de una red. Involucra asignar una prioridad a diferentes flujos de tráfico según su importancia y grado de sensibilidad al retardo. Utiliza de la mejor manera posible el ancho de banda disponible y, si la red se congestiona, el tráfico de baja prioridad se descarta. A veces se denomina asignación de ancho de banda.

Resolución de direcciones: En general, un método para resolver diferencias entre esquemas de direccionamiento del computador. La resolución de direcciones habitualmente especifica un método para asignar las direcciones de capa de red (Capa 3) a las direcciones de capa de enlace de datos (Capa 2).

Router: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Router de generación: Router de una red AppleTalk que tiene el número de red o rango de cable incorporado en el descriptor de puerto. El router de generación define el número de red o el alcance de cable para otros routers de ese segmento de la red y responde a las consultas de configuración de los routers no generadores en la red AppleTalk conectada, permitiendo que esos routers confirmen o modifiquen sus configuraciones en consecuencia. Cada red AppleTalk debe tener al menos un router de generación.

Router designado: Router OSPF que genera LSA para una red multiacceso y tiene otras responsabilidades especiales al ejecutar OSPF. Cada OSPF multiacceso que tiene por lo menos dos routers conectados tiene un router designado elegido por el protocolo Hello OSPF. El router designado permite una reducción en la cantidad de adyacencias requeridas en una red multiacceso, que a su vez reduce la cantidad de tráfico de protocolo de enrutamiento y el tamaño de la base de datos topológica.

Router fronterizo: Router ubicado en los bordes, o al final, de la frontera de la red, que brinda protección básica contra las redes externas, o contra un área menos controlada de la red para un área más privada de la red.

Router no generador: En AppleTalk, un router que primero debe obtener, y luego verificar, su configuración con un router de generación antes de poder comenzar a operar. Ver también router de generación.

Routers vecinos: En OSPF, dos routers que tienen interfaces a una red común. En redes multiacceso, el protocolo Hello OSPF detecta a los vecinos de forma dinámica.

Ruta por defecto: Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas para las cuales el próximo salto no está explícitamente mencionado en la tabla de enrutamiento.

Salto: Pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).

Segmentación: Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

Segmento: Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continúo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de

capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Semidúplex: Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con full dúplex.

Señalización: En el contexto RDSI, el proceso de configuración de llamada utilizado, como establecimiento de la llamada, terminación de la llamada, información y mensajes varios, incluyendo configuración, conexión, liberación, información del usuario, cancelación, estado y desconexión.

Servidor: Nodo o programa de software que suministra servicios a los clientes.

TCP (Protocolo de Control de Transmisión): Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (Protocolo de Control de Transmisión /Protocolo Internet): Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años ’70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Token: Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

Token Ring: LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

TokenTalk: Producto de enlace de datos de Apple Computer que permite que una red AppleTalk se conecte mediante cables Token Ring.

Topología: Disposición física de los nodos y medios de red en una estructura de networking a nivel empresarial.

Topología de anillo: Topología de red compuesta por una serie de repetidores conectados entre sí por enlaces de transmisión unidireccionales para formar un bucle cerrado único. Cada estación de la red se conecta a la red a través de un repetidor. Aunque son anillos lógicos, las topologías de anillo a menudo se organizan en una estrella de bucle cerrado. Comparar con topología de bus, topología en estrella y topología en árbol.

Topología de bus: Topología de LAN en la que las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las demás estaciones Comparar con topología de anillo, topología en estrella y topología en árbol.

Topología de malla completa: Topología en la que todos los dispositivos Frame Relay tienen un PVC hacia todos los demás dispositivos en una WAN multipunto.

Topología de malla parcial: Topología en la cual no todos los dispositivos en la nube Frame Relay tienen un PVC hacia cada uno de los demás dispositivos.

Topología en árbol: Topología de LAN similar a una topología de bus, salvo que las redes en árbol pueden tener ramas con varios nodos. Las transmisiones desde una estación se propagan a lo largo del medio y todas las demás estaciones las reciben. Comparar con topología de bus, topología de anillo y topología en estrella.

Topología en estrella: Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto. Comparar con topología de bus, topología de anillo y topología en árbol.

Trama: Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

TTL (Tiempo de Existencia): Campo en un encabezado IP que indica el tiempo durante el cual se considera válido un paquete.

UTP (par trenzado no blindado): Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5.

VLAN (LAN virtual): Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VLAN de puerto central: VLAN en la que todos los nodos en la misma VLAN se conectan al mismo puerto de switch.

VLAN dinámica (**VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos.):** VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos. Comparar con VLAN estática. Ver también LAN y VLAN.

VLAN estática: VLAN en la que los puertos de un switch se asignan estáticamente. Comparar con VLAN dinámica. Ver también LAN y VLAN.

VoIP (Voice over IP) (Voz sobre Protocolo de Internet (IP)): La habilidad para transportar voz telefónica normal sobre una red de datos basada en el protocolo de Internet, con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales.

La Voz sobre protocolo Internet le permite a un router llevar tráfico de voz (por ejemplo llamadas telefónicas y faxes) sobre una red IP. En Voz sobre IP, la parte de dominio específica (DSP), segmenta la señal de voz en tramas, las cuales son luego agrupadas en parejas y guardadas en paquetes de voz. Estos paquetes de voz son transportados utilizando IP, de acuerdo con la especificación ITU-T H.323.

WAN (Red de área amplia) : Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN.

BIBLIOGRAFÍA

- Hallberg, Bruce. Fundamentos de redes. 4a. ed. Mc. Graw Hill, Interamericana. 2007.

- Molina Robles, Francisco José. Instalación y Mantenimiento de Servicios de Redes Locales. 2a. ed. Madrid, España: Alfaomega, Ra-Ma. 2005.

- Molina Robles, Francisco José. Redes de Área Local. 2a. ed. México: Alfaomega, Ra-Ma. 2004.

- Raya Cabrera, José Luis y Raya Pérez Cristina. Redes Locales y TCP/IP. Madrid, España: Ra-Ma. 1995.