



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE
MÉXICO**

FACULTAD DE INGENIERÍA

**DISEÑO Y CARACTERÍSTICAS DE UNA RED
PARA UN LABORATORIO DE COMPUTO PARA
APOYO A LAS CARRERAS DE INGENIERÍA.**

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TÍTULO DE:
**INGENIERO MECÁNICO ELECTRICISTA
(ÁREA ELÉCTRICA Y ELECTRÓNICA)
MODULO DE SISTEMAS DIGITALES**

P R E S E N T A N

**BENITO BECERRIL ESCAMILLA
MARCO ANTONIO MUÑOZ ROJAS**



DIRECTOR DE TESIS: ING. JUAN FERNANDO SOLORZANO PALOMARES

CIUDAD UNIVERSITARIA MÉXICO D.F.

ENERO 2000

279416



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

TEMA:

DISEÑO Y CARACTERÍSTICAS DE UNA RED PARA UN LABORATORIO DE COMPUTO PARA APOYO A LAS CARRERAS DE INGENIERÍA.

OBJETIVO:

PROPONER Y REDISEÑAR LA RED DEL LABORATORIO DE COMPUTADORAS Y PROGRAMACIÓN.

JURADO

PRESIDENTE: Ing. Mario Alfredo Ibarra Pereyra
VOCAL: Ing. Juan Fernando Solorzano Palomares
SECRETARIO: Ing. Rodolfo Peters Lammel
1ER. SPTE: Ing. Jesús Reyes García
2DO. SPTE: Dr. Bohumil Psenicka

FIRMA

Mario
Juan
Rodolfo
Jesús
Bohumil

A mis padres y hermanos:

Como un testimonio de mi infinito agradecimiento por su apoyo incondicional, por sus esfuerzos y sacrificios, por brindarme la confianza y la fuerza que me impulsó a terminar una de mis metas que ya forman parte de mi vida profesional.

A mi esposa e hija por soportar mis desvelos, mis ausencias en reuniones familiares y por el tiempo que no les dediqué; por su amor, apoyo, comprensión y confianza, que de alguna u otra manera me motivaron a realizar este trabajo de tesis, por permitir hacer de mí un hombre ejemplar para mi familia.

A mis profesores de esta Facultad de Ingeniería por haberme transmitido sus conocimientos y experiencias del ambiente profesional que serán la base para actuar con firmeza y decisión para responder a las necesidades del país.

A mis compañeros del Departamento de Sistemas de Computo de la Dirección General de Intercambio Académico por su tolerancia y comprensión que me brindaron.

Deseo que mi triunfo como hombre y profesionista lo sientan como el propio suyo.

Gracias a DIOS.

Con amor, admiración y respeto.

Benito

CONTENIDO

PREFACIO
INTRODUCCIÓN

ÍNDICE

CAPÍTULO I
INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

1.1	HISTORIA DE LAS REDES DE ÁREA LOCAL, (LAN).....	1
1.2	DEFINICIÓN DE RED DE COMPUTADORAS.....	2
1.3	CARACTERÍSTICAS DE UNA RED DE ÁREA LOCAL.....	3
1.4	ESTRUCTURA DE UNA RED DE COMUNICACIONES.....	3
1.5	CLASIFICACIÓN DE REDES.....	5
1.5.1	POR EXTENSIÓN GEOGRÁFICA.....	5
1.5.1.1	Redes de Área Departamental (DAN).....	5
1.5.1.2	Redes de Área Local (LAN).....	5
1.5.1.3	Redes de Área de Campo (CAN).....	5
1.5.1.4	Redes de Área Metropolitanas (MAN).....	5
1.5.1.5	Redes de Área Extensas (WAN).....	5
1.5.1.6	Redes de Área Global (GAN).....	6
1.5.2	POR TOPOLOGÍAS.....	6
1.5.2.1	Topología en estrella.....	7
1.5.2.2	Topología estrella agrupada.....	8
1.5.2.3	Topología en bus.....	9
1.5.2.4	Topología en anillo.....	9
1.5.2.5	Topología en árbol.....	10
1.5.2.6	Topología en malla.....	11
1.5.2.7	Topología anillo en estrella.....	12
1.5.2.8	Topología bus en estrella.....	12
1.5.2.9	Topología estrella jerárquica.....	13
1.5.3	OTRAS CLASIFICACIONES (PÚBLICAS / PRIVADAS).....	13
1.5.3.1	Internet.....	13
1.5.3.2	Intranet.....	14
1.5.3.3	Extranet.....	14
1.5.3.4	Redes virtuales, Virtual Local Area Network (VLAN).....	14
1.5.4	CONECTIVIDAD CON OTRAS REDES.....	14
1.5.4.1	Red telefónica pública.....	14
1.5.4.2	Red de Videoconferencia.....	15

CAPÍTULO II
 MODELO DE REFERENCIA OSI

2	MODELO DE REFERENCIA OSI.....	16
---	-------------------------------	----

CAPÍTULO III
 ESTÁNDARES

3.1	IEEE 802.....	19
3.2	IEEE 802.1 INTERFAZ DE ALTO NIVEL.....	19
3.3	IEEE 802.2 CONTROL DE ENLACE LÓGICO, LLC.....	20
3.4	LOCALES Y DE CAMPUS.....	20
	3.4.1 Ethernet y el IEEE (802.3).....	20
	3.4.2 Token Bus IEEE (802.4).....	31
	3.4.3 Token Ring IEEE (802.5).....	33
	3.4.4 Interfaz de Datos Distribuidos por Fibra Óptica, FDDI.....	40
	3.4.5 Interfaz de Datos Distribuidos por Cables de Par Trenzado, CDDI.....	44
3.5	ÁREA AMPLIA.....	45
	3.5.1 Protocolo Internet de Línea Serie, SLIP.....	45
	3.5.2 Protocolo Punto a Punto, PPP.....	47
3.6	NUEVAS TECNOLOGÍAS.....	48
	3.6.1 Ethernet rápida (Fast Ethernet).....	48
	3.6.2 Ethernet 100VG-AnyLAN grado de voz IEEE (802.12).....	49
	3.6.3 Gigabit Ethernet.....	52
	3.6.4 Frame Relay.....	52
	3.6.5 Modo de Transferencia Asíncrona, (ATM).....	57

CAPÍTULO IV
 PROTOCOLOS

4.1	Control de Enlace de Datos de Alto Nivel, (HDLC).....	63
4.2	Control de acceso al medio, MAC.....	65
4.3	Intercambio de Paquetes Entre Redes, (IPX).....	67
4.4	Intercambio de Paquetes Secuenciados, (SPX).....	74
4.5	Protocolo de Ruta de Información, (RIP).....	75
4.6	Punto de Acceso de Servicio, (SAP).....	78
4.7	Protocolo de Control de Red, (NCP).....	81
4.8	Sistema Básico de Red de Entrada y Salida (NetBIOS)/Interfaz Extendida de Usuario de NetBIOS (NetBEUI).....	82
4.9	X.25.....	86
4.10	Protocolo de Control de Transmisión / Protocolo Internet, (TCP/IP).....	89

CAPÍTULO V
COMPONENTES DE UNA RED

5.1	MEDIOS FÍSICOS Y SISTEMAS DE TRANSMISIÓN.....	93
5.1.1	Cables de Cobre.....	93
5.1.2	Cable de Par trenzado.....	94
5.1.2.1	Cable de par trenzado sin Blindaje (UTP).....	95
5.1.2.1.1	Conector y base RJ-45.....	96
5.1.2.2	Cable de Par Trenzado Blindado (STP).....	96
5.1.3	Cable Coaxial.....	97
5.1.4	Fibra Óptica.....	99
5.1.5	Guías de Onda.....	104
5.1.6	Radio.....	104
5.1.7	Luz.....	104
5.1.8	Microondas.....	104
5.1.9	Módems.....	105
5.2	CABLEADO ESTRUCTURADO.....	107
5.2.1	Historia de los sistemas de cableado.....	107
5.2.2	Componentes básicos de un sistema de cableado estructurado.....	107
5.2.3	Causas comunes de errores en una red.....	112
5.2.4	Diafonía o next.....	113
5.2.5	Pares divididos.....	113
5.2.6	Ancho de banda utilizable.....	113
5.2.7	Aplicaciones del cableado estructurado.....	113
5.2.8	Lineamientos del cableado estructurado.....	113
5.2.9	Costo beneficio de hacer el cableado sólo una vez con un sistema de cableado estructurado.....	114
5.3	HARDWARE.....	115
5.3.1	Estación de trabajo individual en red.....	115
5.3.2	Servidores.....	115
5.3.3	Servidor centralizado.....	116
5.3.4	Servidores de archivos.....	116
5.3.5	Servidores de archivos distribuidos.....	117
5.3.6	Servidor de archivos dedicado.....	118
5.3.7	Servidor de archivos no dedicado.....	118
5.3.8	Servidor de impresión.....	118
5.3.9	Sistemas de respaldo de red.....	119
5.4	EQUIPOS DE INTERCONEXIÓN.....	119
5.4.1	Tarjetas adaptadoras de Red.....	119
5.4.2	Transceptores.....	120
5.4.3	Repetidores.....	120
5.4.4	Concentradores de cableado de redes (hub's).....	121
5.4.5	Puentes ó Bridges.....	122
5.4.6	Encaminadores ó enrutadores.....	122

5.4.7	Servidor de comunicaciones o compuertas (gateways).....	122
5.4.8	Servidor de comunicación asincrónica.....	123
5.4.9	Switch.....	124
5.4.10	Equipos híbridos.....	124
5.5	SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA, (UPS).....	125
5.5.1	Beneficios que aportan los UPS.....	125
5.5.2	Causas y efectos de los problemas de la red eléctrica.....	125
5.5.3	Diferentes tipos de UPS	127
5.5.3.1	Topología ON LINE.....	127
5.5.3.2	Topología ON-LINE doble conversión.....	128
5.5.3.3	Topología ON LINE con BYPASS.....	128
5.5.3.4	Topología STANDBY ú OFF-LINE.....	129
5.5.3.5	Topología IN-LINE.....	131
5.5.3.6	Topología de línea interactiva.....	131
5.5.4	Características eléctricas.....	131
5.5.4.1	Referente al ondulator.....	131
5.5.4.2	Referente al cargador de baterías (ON-LINE) ó al sistema (OFF-LINE).....	131
5.5.4.3	Referente al bypass.....	132
5.5.4.4	Generales.....	132
5.5.5	Recomendaciones para la selección y uso de los UPS's.....	133
5.5.6	Procedimiento para acondicionar UPS's.....	135
5.5.7	Ejemplos de consumo medio.....	135

CAPÍTULO VI
SOFTWARE DE REDES

6.1	ARQUITECTURA CLIENTE/SERVIDOR.....	137
6.2	SISTEMA OPERATIVO.....	137
6.2.1	DOS.....	139
6.3	SISTEMA OPERATIVO DE RED PUNTO A PUNTO.....	139
6.3.1	Lantastic.....	139
6.3.2	Microsoft Windows 95 / NT para Trabajo en Grupo.....	140
6.3.3	Novell Personal Netware.....	140
6.3.4	Macintosh Apple Talk.....	141
6.4	OTROS SISTEMAS OPERATIVOS DE RED.....	141
6.4.1	IBM LAN Server.....	141
6.4.2	VINES de BANYAN.....	141
6.4.3	LINUX.....	141
6.4.4	UNIX.....	143
6.5	SERVICIOS DE RED.....	143
6.5.1	Acceso a archivos.....	143
6.5.2	Respaldo de archivos.....	143

6.5.3	Impresión de archivos.....	143
6.5.4	Detección de virus.....	144
6.5.5	Correo	144
6.5.6	Gopher.....	145
6.5.7	Telnet.....	145
6.5.8	FTP.....	145
6.5.8	WWW.....	145

**CAPÍTULO VII
ANÁLISIS DEL PROBLEMA**

7.1	SELECCIÓN DE LA MEJOR OPCIÓN Y JUSTIFICACIÓN DEL TIPO DE RED A INSTALAR.....	146
7.2	ENCUESTA SOBRE EL TIPO DE SOFTWARE MÁS UTILIZADO EN EL LABORATORIO.....	146
7.3	DISEÑO E INSTALACIÓN Y PRUEBAS.....	148
	7.3.1 Características de los elementos de red.....	151
	7.3.2 Sistemas operativos.....	153
	7.3.3 Servicios de red, software necesario.....	153
7.4	INFRAESTRUCTURA.....	154
	7.4.1 Ductería y cableado estructurado.....	155
	7.4.2 Energía regulada y sistemas de tierras.....	156
7.5	CONCLUSIONES COMENTARIOS Y SUGERENCIAS.....	156
APÉNDICE A. Lista de acrónimos y abreviaturas más usuales en el ambiente de las redes de computadoras y comunicaciones de datos.....		158
APÉNDICE B. Bibliografía utilizada para el desarrollo de este trabajo.....		160

PREFACIO

El presente trabajo tiene como principal objetivo diseñar y caracterizar la red de un laboratorio de computadoras y programación, con el fin de sugerir actualizaciones y escalamiento conforme avanza la tecnología y que de alguna manera sea competente con necesidades actuales y que esté preparada para requerimientos futuros. Para que dicho laboratorio brinde el servicio requerido es necesario implementar las innovaciones tecnológicas de hardware, software, conectividad, fuentes de energía, sistemas de tierra, sistemas operativos, interoperabilidad, e integración con su plataforma actual de computo, en base a la problemática detectada; de tal manera que el laboratorio cumpla con sus funciones académicas.

Este proyecto hace una recopilación de información de redes de computadoras, con el fin de actualizar los sistemas de información de dicho laboratorio. En éste estudio se tendrá la oportunidad de adquirir experiencia en el diseño, diagnóstico, instalación e implementación de redes de área local, redes de área amplia, acceso remoto e instalación de cableado estructurado, fuentes de alimentación y sistemas de tierra.

Este trabajo servirá como una herramienta de apoyo, para que puedan consultarla personas con conocimientos de redes de computadoras, brindando la oportunidad de estar a la vanguardia tecnológica para hacer actualizaciones conforme avanzan las necesidades de las distintas áreas de la ingeniería.

En base a esta necesidad es necesario realizar el siguiente estudio, para que se lleve a cabo este proyecto.

ORGANIZACIÓN DEL PROYECTO:

Los primeros capítulos contienen los antecedentes o bases teóricas de telecomunicaciones. Así como también una introducción a las redes de computadoras y una breve historia sobre las redes de área local, su estructura, sus características de operación, topologías y sus ventajas en cuanto a su desempeño, se describe el modelo OSI, estándares IEEE 802.X, también contiene una breve descripción de las nuevas tecnologías de redes, protocolos de comunicación. Así como también se habla de los componentes físicos que conforman una red de área local de computadoras tanto de hardware, como del cableado estructurado. Fuentes de alimentación ininterrumpibles. También se hace un breve estudio sobre el tipo de software o sistemas operativos que hay para redes. Se presenta un estudio sobre la diversa paquetería que podrá ser instalada en el Servidor de la Red, para que de alguna manera pueda ser utilizada a través de la red; ya sea de uso general o también de aplicaciones específicas de acuerdo a sus requerimientos.

El último capítulo proporciona información acerca del análisis del proyecto para la red del laboratorio. Tomando como base los siguientes puntos:

- Selección de la mejor opción del tipo de red de computo y se da una justificación.
- Tratado del diseño, instalación y pruebas de la red de computo.
- Relación de los elementos de la red:
 - Equipo de computo instalado y a instalar.
 - Sistemas operativos.
 - Servicios que proporcionará y software necesario.
- Relación de la Infraestructura:
 - Ductería y cableado estructurado.
 - Energía regulada y sistemas de tierra.

Finalmente se mencionan las conclusiones.

El apéndice A contiene una lista de acrónimos y abreviaturas más usadas en el medio ambiente de las redes de computadoras y comunicaciones de datos.

El apéndice B contiene la Bibliografía del desarrollo del presente proyecto.

INTRODUCCIÓN

Durante las últimas décadas, las redes de computadoras han estado causando un gran impacto en la sociedad con las grandes innovaciones tecnológicas que han surgido en estos tiempos, los beneficios ya se están viendo al multiplicar la productividad y la eficiencia, tanto en las empresas como en los usuarios.

Mucha gente acude a las redes informáticas para atender a sus necesidades, ya que hoy en día es posible transmitir y recibir voz, datos y vídeo a través de estas redes. Algunas necesidades que se pueden cubrir son por ejemplo: servicio de correo electrónico, visualización de transacciones que se tiene en almacenes, realización de operaciones bancarias, sistemas de punto de venta, interconexión de oficinas situadas en diferentes lugares, servicio de videoconferencias, servicio de fax, etc.

De la misma manera, en la educación se ha visto los beneficios que obtienen los alumnos, al emplear las redes de computadoras como herramientas de trabajo. Debido a esto realizamos una encuesta sobre el tipo de software adecuado que sirva como herramienta útil para las nuevas generaciones que estudiarán en el Laboratorio de Computadoras y Programación de esta Facultad de Ingeniería, así como también, dicho laboratorio se encuentre actualizado y sea compatible con las nuevas tecnologías de tal manera que los alumnos tengan acceso a Internet, para que aprovechen la tecnología de punta y obtengan e intercambien información a nivel mundial. Para brindar esta solución es necesario adaptar la infraestructura tanto de ductería, cableado estructurado, suministro de energía y sistemas de tierra.

Dependiendo de las aplicaciones y componentes que se necesiten en la red LAN / WAN se volverá tan complejo; y el diagnóstico y corrección de fallas podrá convertirse en un verdadero reto para la administración y operación de la red.

Por todo lo anterior es importante conocer el ancho de banda de la red local y de cada uno de sus nodos para tomar decisiones sobre del tipo de red que se requiere.

El buen diseño e instalación de la red, así como su administración y operación del sistema de computo, depende de la solución integral de:

- Hardware.
- Software.
- Conectividad.
- Sistemas operativos.
- Interoperabilidad.
- Integración con su plataforma actual de computo.
- Fuentes de energía regulada y sistemas de tierra.

CAPÍTULO I INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

1.1 HISTORIA DE LAS DE LAS REDES DE AREA LOCAL, (LAN)

La industria de la computación ha evolucionado con gran rapidez en las últimas décadas, aunque fue hasta la llegada de las microcomputadoras cuando se pudo implementar las Redes de Área Local, (Local Area Network, LAN).

Las primeras computadoras de los años cincuenta fueron las Macrocomputadoras (Mainframes), estas no tenían la capacidad para responder en línea a los comandos del usuario, por lo que utilizaban un método de procesamiento por lotes, donde los usuarios presentaban tarjetas codificadas que contenían los comandos del programa y los datos, por lo general no se enviaban luego los resultados impresos al usuario sino hasta el día siguiente.

En ese tiempo había pocas computadoras y eran caras por lo que las empresas no podían comprarse una, la solución a este problema de costo fue el tiempo compartido rentando terminales con su módem y su lectora de tarjetas conectándose a una macrocomputadora a través de una línea telefónica, el usuario podía utilizar una Macrocomputadora sin necesidad de invertir un gran capital.

El mayor problema con el tiempo compartido era la lentitud en el envío de información, este problema se resolvió con la producción de las Minicomputadoras. Cuando se empezaron a distribuir los recursos de la computadora en toda una empresa, mediante la asignación de computadoras a todos los departamentos se le llamó computación distribuida. La figura 1.1.1 muestra el esquema de la computación distribuida.

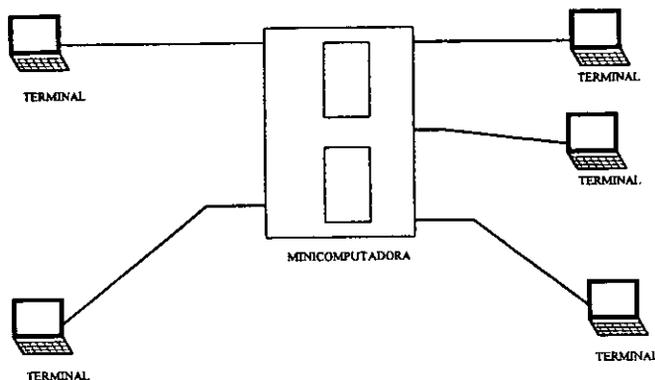


Figura 1.1.1. Computación distribuida con una minicomputadora.

Las empresas se dieron cuenta de que necesitaban desarrollar nuevos sistemas más rápidos y flexibles, el costo y el tamaño de las macrocomputadoras y minicomputadoras se convirtió en un problema por lo que se comenzó con el desarrollo de las LAN que ofrecen una solución a esos problemas.

La Computación Distribuida vino a significar el enlace de microcomputadoras de manera que se pudiera compartir información y dispositivos periféricos, esta fue la idea de las primeras redes de área local.

Con el incremento en la demanda de la programación, computación científica, procesamiento de textos y uso personal, la necesidad por enlazar computadoras para compartir información esta creciendo rápidamente. Una buena solución para esto, es la implementación de una (LAN).

1.2 DEFINICIÓN DE RED DE COMPUTADORAS

Red de computadoras: Es un conjunto de equipos de comunicaciones interconectados a través de medios físicos de comunicación, con la finalidad de compartir recursos, intercambiar información, expandir capacidades de un equipo, comunicar usuarios, evitar la duplicidad de trabajo, reducir costos, manejar la información con mejor control y mayor seguridad.

Este sistema de interconexión de equipos informáticos basado en líneas de alta velocidad (decenas o cientos de megabits por segundo), y que son muy usadas en los edificios. Uno de los diseños más difundidos para redes de área local (LAN, Local Area Network) es Ethernet. Este tipo de red es la más usada, y las características que presenta son: topología de bus y usa repetidores para aumentar la longitud de la red.

Una LAN es utilizada generalmente por una sola organización a través de una distancia limitada y que permite a los usuarios compartir información y recursos. Las LAN's utilizan el bloqueo de archivos, lo cual permite que los programas solo sean utilizados por un solo usuario a la vez. Las LAN's actuales utilizan poderosos programas de productividad y negocios, los cuales permiten el uso de varios cientos de usuarios al mismo tiempo.

El uso principal de una LAN es compartir equipo periférico como: impresoras, unidades de disco duro, graficadores etc. En la actualidad algunas redes, como las Novell, son más económicas al aceptar estaciones de trabajo "sin disco" estas no tiene unidad de disco duro ni flexible, estas máquinas emplean un chip ROM arranque remoto especial en las tarjetas de red, que permite que la computadora forme parte de la red.

1.3 CARACTERÍSTICAS DE UNA RED DE ÁREA LOCAL

Una red LAN tiene las siguientes características principales:

- Opera a velocidades de entre 1 y 100 Mbits por segundo.
- Tiene una cobertura pequeña, es decir, entre un servidor de archivos y una estación de trabajo debe haber como máximo 1.5 Km de distancia.
- Una LAN requiere que las estaciones de trabajo individuales (microcomputadoras) estén conectadas físicamente mediante cables (coaxiales o par trenzado) o por medio de conexiones inalámbricas y que el disco duro de la estación de trabajo contenga algún tipo de software de red, esto permite compartir periféricos, datos y programas de aplicación.
- Es Capaz de soportar una gran cantidad de dispositivos.
- Buena rentabilidad.
- Fácil instalación.
- Bajo costo.
- Fácil de mantener y reconfigurar.

Aunque varían de acuerdo a la topología, hardware, medio de transmisión, etc. que se utilice.

1.4 ESTRUCTURA DE UNA RED DE COMUNICACIONES

Una red de comunicaciones básica consta de: Equipo Terminal de Datos (ETD), Equipo de Comunicación de Datos (ECD), y el canal de comunicaciones.

OBJETIVO:

El objetivo de las redes de comunicación es de interconectar distintos ETD para que compartan recursos, intercambien datos. La red proporciona comunicaciones físicas y lógicas entre las computadoras conectadas a ella.

En un Equipo Terminal de Datos (ETD) residen las aplicaciones, un ETD representa al usuario final, puede ser una computadora grande, o una maquina pequeña como una computadora personal (PC, Personal Computer), que pueden utilizarse como cajeros automáticos de los bancos, las terminales punto de venta de un gran almacén, las computadoras o terminales de correo electrónico instaladas en los domicilios particulares o en las oficinas, las computadoras encargadas de automatizar los procesos de fabricación en una planta industrial.

Las aplicaciones son las que maneja el usuario final, como ejemplo de ello son los programas de nóminas, los sistemas de reservación de boletos de aviones, los sistemas de control de inventarios, correo electrónico, etc.

Los Equipos de Comunicación de Datos o simplemente (ECD), tiene como misión conectar los equipos ETD a la línea o canal de comunicaciones y por lo tanto sirve de interfaz entre ETD y la red de comunicaciones un ejemplo de esto es el módem.

El canal de comunicaciones es el medio físico, por el cual se transmite la información. La figura 1.4.1, muestra la estructura de una red de comunicaciones básica.

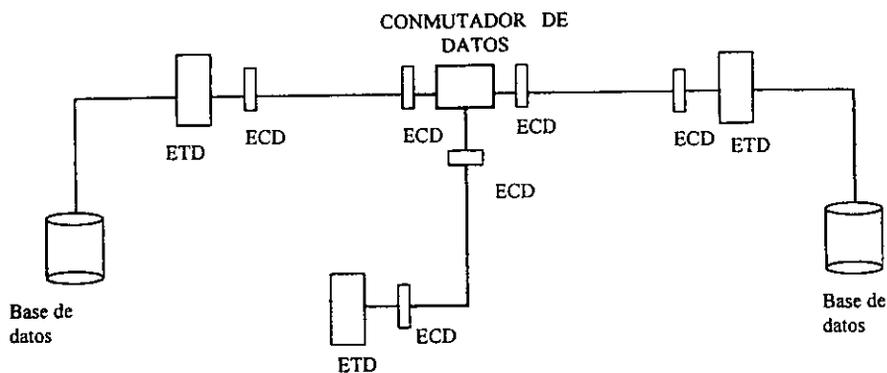


Figura 1.4.1. Estructura de una red de comunicaciones de datos.

1.5 CLASIFICACIÓN DE REDES

1.5.1 POR EXTENSIÓN GEOGRÁFICA

Las redes de computadoras se pueden clasificar de acuerdo a su extensión y distribución geográfica en:

1.5.1.1. REDES DE ÁREA DEPARTAMENTAL (DEPARTMENTAL AREA NETWORK, DAN)

Una red de área departamental es un sistema de interconexión de equipos informáticos, usada principalmente en oficinas.

1.5.1.2 REDES DE ÁREA LOCAL LAN (LOCAL AREA NETWORK, LAN)

Una red de área local es un sistema de interconexión de equipos informáticos basado en líneas de alta velocidad, su rango de velocidad es de 1 Mbps a 100 Mbps, es muy usada en edificios.

1.5.1.3 REDES DE ÁREA DE CAMPO (CAMPUS AREA NETWORK, CAN)

Una red de área de campo es un sistema de interconexión de equipos informáticos, que conecta nodos (o posiblemente LAN's) desde múltiples sitios que pueden estar separados por distancias considerables. A diferencia de una WAN, que no utiliza líneas telefónicas públicas o privadas y que, además, conecta redes a través de cables, fibra óptica o microondas. Su rango de velocidad es 56 kbps a 155 Mbps.

1.5.1.4 REDES DE ÁREA METROPOLITANA (METROPOLITAN AREA NETWORK, MAN)

Una red de área metropolitana es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos.

1.5.1.5 REDES DE ÁREA EXTENSA (WIDE AREA NETWORK, WAN)

Una red de área extensa o amplia, es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.

1.5.1.6 REDES DE ÁREA GLOBAL (GLOBAL AREA NETWORK, GAN)

Una red de área global es un sistema de interconexión de equipos informáticos, basadas en tecnología Internet que abarca a diferentes países.

La figura 1.5.1.1 muestra una ubicación de cada una de las redes por extensión geográfica.

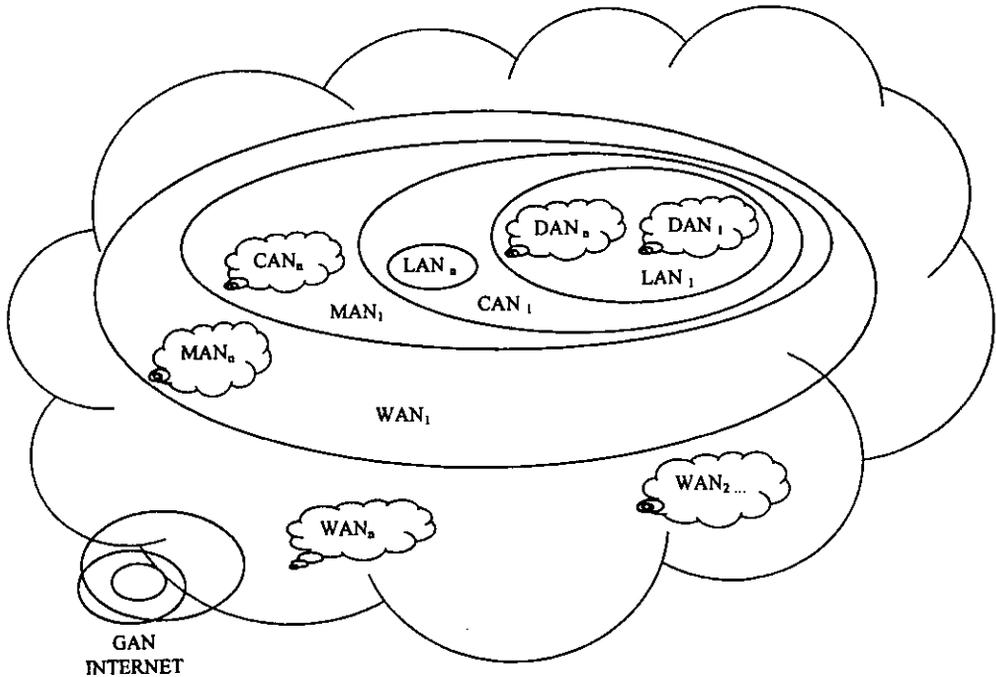


Figura 1.5.1.1. Ejemplo de una clasificación de redes por extensión y distribución geográfica.

1.5.2 POR TOPOLOGÍAS

La topología de una red es la forma geométrica o arquitectura de su conexión física (describe como el cable conecta a los nodos), o lógica (describe como la información es transmitida y controlada por los nodos) de la red. Para establecer la topología de una red, el diseñador ha de plantearse los siguientes objetivos principales:

- Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico de datos.

- Encaminar el tráfico entre el ETD transmisor y el receptor a través del camino más económico (aunque si se consideran otros factores más importantes como la fiabilidad, este camino de coste mínimo, puede no ser el más conveniente); pero de alguna manera u otra se deberá proporcionar el camino más económico para cada actividad concreta; por ejemplo transmitir los datos de baja prioridad a través de un enlace de baja velocidad por línea telefónica normal resultaría más barato que transmitir esos mismos datos a través de un canal vía satélite de alta velocidad.
- Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo.

La fiabilidad de una red se refiere a la capacidad que tiene la misma para transportar datos correctamente (sin errores) de un ETD a otro. Ello incluye también la capacidad de recuperación de errores, ya sea por fallo del canal, del ETD, del ECD, o del equipo de conmutación de datos.

El tiempo de respuesta deberá ser mínimo y un caudal eficaz lo más elevado posible. El caudal eficaz expresa la cantidad máxima de datos de usuario que es posible transmitir en un determinado período de tiempo.

Según la topología de interconexión de computadoras, las redes se pueden clasificar en:

- Estrella.
- Estrella agrupada.
- Bus.
- Anillo.
- Árbol.
- Malla.
- Anillo en estrella.
- Bus en estrella.
- Estrella jerárquica.

1.5.2.1 TOPOLOGÍA EN ESTRELLA

Es una de las tres principales topologías más antiguas y más empleadas en los sistemas de comunicación de datos, en donde la red se une en un único punto, por medio de un concentrador de cableado; utiliza el método de envío y recepción de mensajes, se maneja mediante una estación central de conmutación, esta arquitectura facilita la adición de nuevas estaciones de trabajo a la LAN, todo lo que se requiere es un cable que vaya del punto central de conexión (concentrador) a la tarjeta de interfaz de red de la nueva microcomputadora.

Otra ventaja es que el administrador de la red puede asignar a ciertos nodos un status mayor que a otros, por lo que la computadora central tendera a buscar las señales de estas estaciones de trabajo prioritarias antes de reconocer a otros nodos. Una arquitectura estrella hace posible

contar con diagnósticos centralizados de todas las funciones de la red, como todos los mensajes pasan a través del concentrador central, es fácil analizar todos los mensajes emitidos por las estaciones de trabajo y producir informes que revelen los archivos que utilizan cada nodo, se encarga además de localizar las averías de la red, con esto se puede garantizar la seguridad de la red.

La principal deficiencia de la arquitectura Estrella es que si algo le sucede al concentrador central, falla la LAN completa.

La figura 1.5.2.1.1 muestra la topología de una red en estrella.

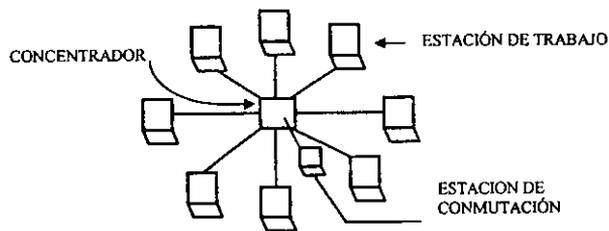


Figura 1.5.2.1.1. Topología de red en estrella.

1.5.2.2 TOPOLOGÍA ESTRELLA AGRUPADA

Existe la topología Estrella agrupada la cual esta compuesta por varias estrellas conectadas entre sí, la falla de cualquier estrella no ocasiona la falla completa de la red, aunque las estaciones de trabajo conectadas a dicha estrella no podrán funcionar en red. La figura 1.5.2.2 muestra una red en topología estrella agrupada.

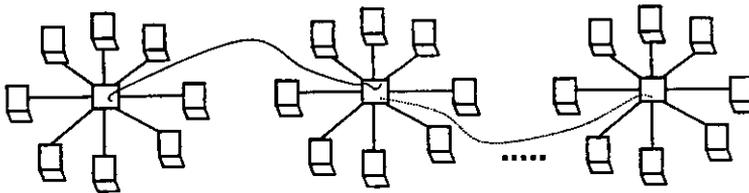


Figura 1.5.2.2.1. Topología de red en estrella agrupada.

1.5.2.3 TOPOLOGÍA EN BUS

En esta topología principal de red todas las estaciones están conectadas por un único segmento de cable como se muestra en la figura 1.5.2.3.1 este tipo de arquitectura conecta a varias estaciones de trabajo de una LAN, por lo general en muchas de estas redes las estaciones de trabajo primero examinan si un mensaje le esta entrando del bus antes de enviar otros mensajes, como todas las estaciones de trabajo comparten este Bus, todos los mensajes pasan por otras estaciones de trabajo hasta llegar a su destino. Cada estación examina la dirección del mensaje para detectar si le corresponde a su propia dirección. Cada estación de trabajo copia los mensajes dirigidos a ella en la memoria RAM de su tarjeta de interfaz de red y luego procesa su información. De esta manera una estación de trabajo puede difundir información a todas las demás.

El cableado de esta topología Bus es muy sencillo, requiere una menor cantidad de cables que cualquier otra topología importante; muchas LAN's de bajo costo usan la arquitectura de Bus. Una ventaja de esta topología es que la falla de una computadora no necesariamente obstruye el funcionamiento de toda la red, es muy fácil añadir nuevas estaciones de trabajo.

Una desventaja es que, debe de haber un mínimo de distancias entre las derivaciones, de manera que las estaciones de trabajo puedan evadir la interferencia de señales, así mismo el administrador de la red del sistema puede realizar un diagnóstico de la red completa. Y por último, una arquitectura de Bus no tiene las características de seguridad de la topología en estrella. Y con una falla en el cableado dejará de funcionar toda la red.

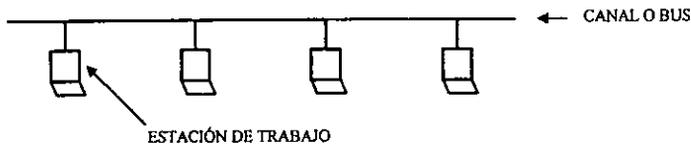


Figura 1.5.2.3.1 Topología de red en Bus.

1.5.2.4 TOPOLOGÍA EN ANILLO

Es una de las principales topologías que consta de varios nodos unidos formando un círculo lógico por medio de un cable. Los mensajes circulan de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional; no obstante solo son capaces de enviar mensajes en una dirección cada vez.

La topología de anillo permite verificar si se ha recibido un mensaje. Cuando un nodo recibe un mensaje que va dirigido a él, éste lo copia y luego lo envía de regreso al emisor con una bandera que indica que ha sido recibido.

Una característica de una topología de anillo es la necesidad de asegurar que todas las estaciones de trabajo tengan el mismo acceso a la red. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como ficha o contraseña de paso. La ficha contiene la dirección del emisor y la dirección del nodo receptor. Cuando la estación receptora ha copiado el mensaje, regresa la ficha a la estación de trabajo generadora, la cual luego envía la ficha a la siguiente estación de trabajo del anillo. Si no tiene algo que enviar, la ficha pasa a la estación de trabajo siguiente.

La topología en anillo combina las ventajas de las topologías de estrella y de Bus. Una estación de trabajo monitorea todas las funciones de la red; y la falla de una estación de trabajo no produce la falla en la red completa.

Para propósitos administrativos del sistema, es necesario designar a una estación de trabajo que actúe como nodo de monitoreo de la red. El nodo de monitoreo maneja todas las funciones de diagnóstico. A esta estación se le llama monitor activo.

Hay muchas ventajas en una topología de anillo. Si el nodo de monitoreo falla, la red sigue funcionando ya que es posible designar a otra estación de trabajo para realizar esta tarea. La red puede resistir la falla de algunas estaciones de trabajo ignorándolas. La mayoría de las redes en anillo ahora incluyen un tipo de conector llamado centros de cableado. Estos permiten que el administrador de la red añada y elimine estaciones de trabajo conectándolas o desconectándolas a los centros de cableado apropiados. Permaneciendo la red intacta y funcionando.

La figura 1.5.2.4.1 muestra la topología de red en anillo.

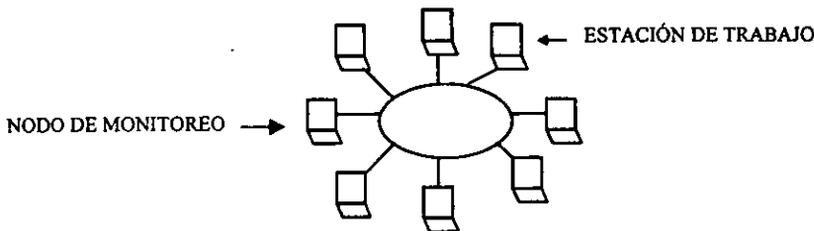


Figura 1.5.2.4.1. Topología de red en anillo.

1.5.2.5 TOPOLOGÍA EN ÁRBOL

La estructura jerárquica es una de las más extendidas en la actualidad. La topología proporciona un punto de concentración de las tareas de control y resolución de errores. En la mayoría de los casos la estación de trabajo situada en el nivel más elevado es la que controla la red. Muchos fabricantes incorporan a esta topología un cierto carácter distribuido dotando a las estaciones subordinadas de un control directo sobre de las estaciones situadas en niveles

inferiores dentro de la jerarquía, lo cual reduce la carga de trabajo del nodo central. La figura 1.5.2.5.1 muestra la topología de red en árbol.

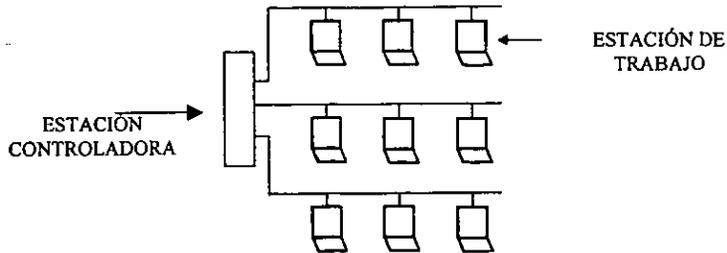


Figura 1.5.2.5.1. Topología de red en árbol.

1.5.2.6 TOPOLOGÍA EN MALLA

En esta topología, cada estación de trabajo de la red es directamente conectada a todas las demás estaciones. Por lo tanto implica que cada estación de trabajo deberá tener $(N-1)$ puertos de entrada/salida donde N es el número de estaciones o nodos en la red, como consecuencia, involucra una gran cantidad de cableado.

Sin embargo, la topología de red en malla tiene una excelente tolerancia a las fallas, y esto significa que cuando un enlace falla, el tráfico de mensajes puede ser enrutado a través de un nodo intermedio.

Esta estructura es típica de las redes de área amplia (Wide, Area, Network, WAN), pero también se puede utilizar en algunas aplicaciones de redes LAN. La figura 1.5.2.6.1 muestra la topología de red en malla.

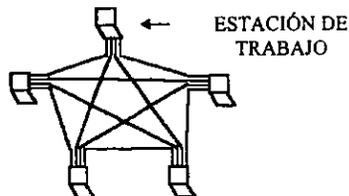


Figura 1.5.2.6.1. Topología de red en malla.

1.5.2.7 TOPOLOGÍA ANILLO EN ESTRELLA

Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente la disposición del cable se parece a una topología regular del cable a una estrella centralizada en un concentrador, mientras que a nivel lógico, la red esta en anillo. La figura 1.5.2.7.1 muestra la topología de red anillo en estrella.

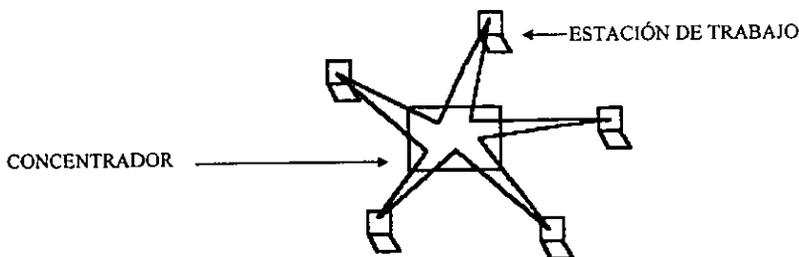


Figura 1.5.2.7.1. Topología de red Anillo en estrella.

1.5.2.8 TOPOLOGÍA BUS EN ESTRELLA

Esta topología tiene el mismo propósito que la topología anterior, lo único que en esta red, es un Bus que se cablea físicamente como una estrella por medio de concentradores. La figura 1.5.2.8.1 muestra la topología de red bus en estrella.

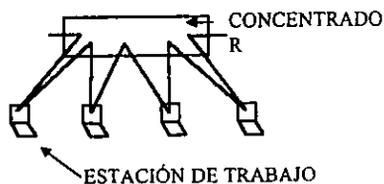


Figura 1.5.2.8.1. Topología de red Bus en estrella.

1.5.2.9 TOPOLOGÍA ESTRELLA JERÁRQUICA

Este tipo de topología se usa en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica. La figura 1.5.2.9.1 muestra la topología de red bus en estrella.

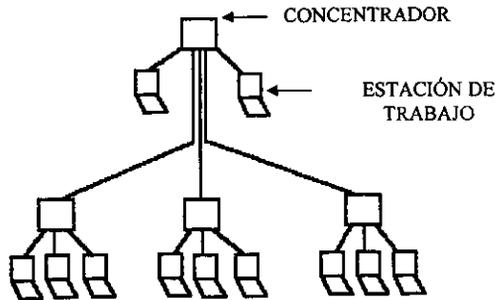


Figura 1.5.2.9.1. Topología de red estrella jerárquica.

En las diferentes topologías es aplicable la palabra segmento de una LAN. Un segmento de una LAN consiste de un solo medio de comunicación y todos los dispositivos de la LAN interconectados. Los segmentos de LAN pueden ser combinados para formar redes de área local más grandes o para interconectar diferentes tipos de segmentos de la LAN en una misma red. La interconexión de segmentos de una LAN se puede lograr a través de puentes, enrutadores, o compuertas. Los segmentos de LAN solamente pueden ser combinados dentro de la misma red usando puentes o enrutadores si comparten una capa de comunicación común (subcapa del control lógico para los puentes, capa de red para los enrutadores). Las compuertas interconectan segmentos de red las cuales pueden usar una arquitectura de comunicación totalmente diferente.

1.5.3 OTRAS CLASIFICACIONES (PÚBLICAS / PRIVADAS)

1.5.3.1 INTERNET

Es un conjunto de redes de computadoras, de alcance internacional, que están enlazadas por diversos medios tecnológicos, y que usan los protocolos TCP/IP como el método principal para la transmisión de datos a través de ellas. Lo cual hace posible que los usuarios de cualesquiera de las redes pueda comunicarse y usar los servicios de alguna otra red.

1.5.3.2 INTRANET

Este tipo de red utiliza tecnología Internet situada detrás de un firewall (bloqueo al acceso de algunas direcciones de archivos), para uso exclusivo de alguna corporación.

1.5.3.3 EXTRANET

Es una Intranet expandida donde la información puede ser accedida solamente por los clientes, mientras que los externos (no clientes) necesitan validación a través de contraseña.

1.5.3.4 REDES VIRTUALES, VIRTUAL LOCAL AREA NETWORK (VLAN)

Son redes de equipos interconectados geográficamente dispersos pero lógicamente unidos que proporcionan la apariencia de trabajo en el mismo segmento físico. Este tipo de configuración de redes es necesario utilizar switches (conmutadores).

1.5.4 CONECTIVIDAD CON OTRAS REDES

1.5.4.1 RED TELEFÓNICA PÚBLICA

Se pueden interconectar las redes utilizando los MODEM's o a través una línea dedicada utilizando el estándar de multiplexación por división de tiempo, Time Division Multiplexing (TDM), el E1 y el T1 son las líneas multiplexadas en el tiempo más comunes. El T1 es el estándar utilizado en el Japón y Estados Unidos; mientras que el E1 es un estándar europeo, el cual es muy utilizado en México.

Multiplexación por división de tiempo: Es una tecnología de multiplexación en banda base en donde cada canal de voz o datos es intercalado en una trama de bits, en donde las señales analógicas son muestreadas o convertidas a señales digitales.

La red telefónica utiliza la conmutación de circuitos para comunicar los distintos equipos terminales de datos.

Los pasos que se siguen en la conmutación de circuitos son:

- Establecer el circuito de conexión (seleccionar un canal).
- Mantener el enlace directo a través de distintos segmentos de la red. Este camino equivale a un par de hilos que une a ambos usuarios y esta trayectoria permanece hasta que el circuito se desconecte.
- Transferencia de datos: Generalmente la conexión es Full Duplex (es decir, que los datos pueden ser transmitidos en ambas direcciones al mismo tiempo).
- Desconexión del circuito: Una vez terminada la transferencia de información entre la fuente y el destino la conexión es terminada. Las señales son propagadas por los nodos de conmutación para desconectar las líneas dedicadas.

1.5.4.2 RED DE VIDEOCONFERENCIA

Las redes de videoconferencia se utilizan para transmitir voz, audio y vídeo en tiempo real en ambas direcciones.

Hay dos tipos de videoconferencia:

- a) Punto a Punto: En este tipo de redes la transmisión es de la fuente a un solo destino.
- b) Punto multipunto: En estas redes, la transmisión es de una sola fuente a varios destinos.

CAPÍTULO II MODELO DE REFERENCIA OSI

2. MODELO DE REFERENCIA OSI (OPEN SYSTEMS INTERCONNECTION) O ISA (INTERCONEXIÓN DE SISTEMAS ABIERTOS)

La Organización Internacional de Estándares, (International Standard Organization, ISO) y el Comité Consultivo Internacional para la Telegrafía y Telefonía (CCITT) han desarrollado el modelo OSI para definir redes y protocolos por capas o niveles.

Los objetivos que persigue el modelo OSI son:

- Proporcionar una serie de normas para la comunicación entre los sistemas.
- Eliminar todas las limitaciones técnicas que pudieran existir para la comunicación entre sistemas.
- Estudiar el funcionamiento interno de los sistemas individuales.
- Definir los puntos de interconexión para el intercambio de información entre sistemas.
- Realizar una fácil comunicación entre sistemas sin necesidad de hacer numerosas conversiones y traducciones entre diferentes productos.

El modelo de referencia OSI consta de siete niveles, cuya estructura se muestra en la figura 2.1.

NIVEL 7 DE APLICACIÓN
NIVEL 6 DE PRESENTACIÓN
NIVEL 5 DE SESIÓN
NIVEL 4 DE TRANSPORTE
NIVEL 3 DE RED
NIVEL 2 DE ENLACE
NIVEL 1 FÍSICO

Figura 2.1. Capas del modelo de referencia OSI.

El modelo de referencia OSI define los protocolos de comunicación en siete niveles. Cada nivel tiene funciones muy bien definidas, que se interrelacionan con las funciones de los niveles contiguos.

La compatibilidad del equipo se puede definir dentro de un nivel o bien se pueden ocultar implantaciones de nivel inferior para lograr compatibilidad en algún nivel superior. El doble fin del modelo OSI es asegurar el flujo de información entre sistemas y al mismo tiempo permitir variación en tecnología de comunicaciones.

En el modelo OSI, el nivel físico define los conectores y componentes que proporcionan comunicaciones de red, es decir es la base del hardware de la red. Las capas 2 a la 7 definen cómo acceden las aplicaciones a los servicios de comunicaciones, es decir se implantan en software.

Nivel de aplicación (nivel 7): Ofrece servicios finales a usuarios de la red, como son transferencias de datos por medio de FTP, correo electrónico, el control de flujo y la recuperación de errores, recursos de emulación de terminales y software de acceso general a la red son ilustrativos del software que opera en este nivel. Y todos los niveles inferiores están diseñados para dar soporte a estas aplicaciones.

Nivel de Presentación (nivel 6): Este nivel ofrece funciones de traducción de formatos y representaciones de datos, tiene los servicios de conversión de protocolo, descompresión de datos, codificación, cambios o conversiones de conjuntos de caracteres, y la expansión de comandos gráficos, este nivel prepara la información que será utilizada por el nivel 7.

Nivel de sesión (nivel 5): Este nivel permite el diálogo entre estaciones en una sesión orientada a la conexión. Facilita el establecimiento y terminación de grandes cantidades de datos de dos o más conexiones de LAN o nodos. Mapea direcciones en conexiones específicas de la red.

Nivel de transporte (nivel 4): Este nivel proporciona un canal de comunicaciones de datos en el cual los sistemas finales pueden acusar el recibo completo de los datos o solicitar la retransmisión.

Aquí en este nivel nos asegura que la información viaja bien del nodo inicial al nodo final y verifica que la información mandada a través de los ruteadores llegue bien.

Dentro de este nivel se confrontan aspectos relacionados con un nivel de confiabilidad en la transferencia de datos, estos aspectos incluyen control de flujo, manejo de errores y problemas que se presentan con la transmisión y recepción de paquetes; un paquete esta compuesto de datos originados por el usuario, además de información que la red necesita para transportar datos del usuario de un nodo de la red a otro.

Nivel de la red (nivel 3): Este nivel define la interfaz entre el Equipo Terminal de Datos (ETD) de usuario y la red de conmutación de paquetes, además de la interfaz de un ETD con otro a través de esta red. También proporciona funciones de encaminamiento de paquetes por la red y la comunicación entre múltiples redes. Establece, supervisa y libera las secciones de comunicación.

En muchas redes de área local no se necesita el nivel de la red (nivel 3), solamente en aquellas que requieran mecanismos de envío entre nodos, pero las LAN en alguna implementación transmiten datos a todos y cada uno de los nodos, y una conexión específica recolecta esos paquetes adecuadamente direccionados a ella.

Nivel enlace de datos (nivel 2): Este nivel sitúa los datos en tramas para la transmitirlos al nivel físico y asegura transmisiones fiables entre estaciones. Así mismo garantiza la identidad de los bits, encargándose de que los datos lleguen sin errores a la estación de trabajo receptora, controla el flujo de datos para impedir que la estación de trabajo se desborde en algún momento. Una de sus funciones más importantes consiste en detectar errores en la transmisión y en recuperar los datos perdidos, duplicados o erróneos.

Este nivel, define la estrategia de acceso para compartir el medio físico mediante el método más común para redes de área local como es el CSMA/CD (Acceso Múltiple con Detección del Portador/Detección de Colisión) y de transmisión de señales codificadas.

Nivel físico (nivel 1): Este nivel define las normas y estructuras del flujo de bits entre los dispositivos, así como también define las características eléctricas y mecánicas de los cables y conectores de la red. Las técnicas de modulación, las frecuencias operación de la red y los voltajes empleados son todas las características de este nivel, como en todas las redes se implantan los niveles 1 y 2, estos son los que reciben la mayor atención de los fabricantes de redes. Por lo que se deben desarrollar componentes compatibles en estos dos niveles, para cumplir con el concepto de estándar.

CAPÍTULO III ESTÁNDARES

3.1 IEEE 802

El instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE) ha producido varios estándares para las redes de área local (Local Area Network, LAN) y redes de área metropolitana (Metropolitan Area Network, MAN), estos estándares son conocidos como IEEE 802, y han sido adoptadas por el Instituto Nacional Americano de Normalización (American National Standard Institute, ANSI) como una norma nacional americana, por la Organización Internacional de Estándares (International Standards Organization, ISO) como una norma Internacional conocida como ISO 8802.

La familia de los 802.x se divide en partes:

- 802.1 Interfaz de Alto Nivel.
- 802.2 Control de Enlace Lógico (Logical Link Control, LLC).
- 802.3 Acceso Múltiple por detección de portadora con detección de colisión (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) muy usado en Ethernet.
- 802.4 Token Bus.
- 802.5 Token Ring.
- 802.6 Redes de Area Metropolitana.
- 802.7 Grupo de consejo técnico de banda ancha.
- 802.8 Grupo de consejo técnico de fibra óptica.
- 802.9 Redes de voz y datos integrados.
- 802.10 Seguridad en redes.
- 802.11 Redes de área local inalámbricas.
- 802.12 Redes 100VG-AnyLAN.

Cuyo objetivo es crear, mantener y promover estándares de la capa 1 y 2 del modelo de referencia OSI.

3.2 IEEE 802.1 INTERFAZ DE ALTO NIVEL

El estándar IEEE 802.1, define la relación entre las normas IEEE y el modelo OSI. Este comité define que las direcciones de los adaptadores de las estaciones de la LAN sean de 48 bits para todas las normas 802. El IEEE registra y asigna los primeros 3 bytes de la dirección a los fabricantes de tarjetas de interfaz de red. Así cada fabricante es responsable de la creación de direcciones únicas para cada una de sus tarjetas adaptadoras de red.

Define la interfaz con funciones básicas a partir de las cuales se puede establecer una interconexión, en la cual se establece una comunicación mediante una petición, indicación, respuesta y confirmación de la solicitud de comunicación de datos.

3.3 IEEE 802.2 CONTROL DE ENLACE LÓGICO, LLC

La norma 802.2 define el protocolo de Control de Enlaces Lógicos (Logical Link Control, LLC) del IEEE.

Tiene las siguientes características:

- Asegura que los datos se transmitan en forma fiable a través del enlace de comunicaciones.
- El nivel de enlace de datos del modelo OSI se divide en dos subniveles: control de acceso al medio (Media Access Control, MAC) y en el LLC.
- Estos dos subniveles permiten conectar una red Ethernet con una red en anillo con testigo.
- Los Puentes (bridges), utilizan estos dos subniveles como un mecanismo de conmutación, en la cual a una trama que llegue de una red Ethernet y se destine a una red en anillo con testigo, se le desmonta su cabecera de trama Ethernet y se empaqueta con una cabecera de anillo con testigo.
- LLC proporciona la interfaz con los niveles superiores del modelo de interconexión de sistemas abiertos (Open Systems Interconnection, OSI).
- LLC proporciona las direcciones de los puntos de acceso al servicio (Service Access Points, SAP's).
- El subnivel MAC ofrece la dirección física de un dispositivo de la red. La dirección física está grabada en una memoria programable de la tarjeta de red y consta de 6 bytes y a esta se le conoce también como dirección MAC.

LLC proporciona los siguientes servicios:

- *Servicio orientado a la conexión.* Se establece una sesión con un destino y se libera cuando se completa la transferencia de datos.
- *Servicios orientados a la conexión con reconocimiento.* Parecido al anterior, en la cual se reconocen las transmisiones de paquetes.
- *Servicio sin reconocimiento no orientado a la conexión.* Los paquetes simplemente se envían al destino.

3.4 LOCALES Y DE CAMPUS

3.4.1 ETHERNET Y EL IEEE (802.3)

El sistema de red Ethernet fue originalmente creado por Xerox, pero desarrollado conjuntamente como una norma en 1980 por Digital Equipment Corporation (DEC), Intel y Xerox. La norma 802.3 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) define una red similar aunque ligeramente diferente por la especificación completa de CSMA/CD.

Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD)

El método de acceso múltiple con detección de portadora y detección de colisiones (Carrier Sense Múltiple Access with Collision Detection, CSMA/CD) se utiliza para compartir el acceso al cable, pero que solamente una estación de trabajo tenga acceso a la red en un momento dado.

Características:

- Reduce el ancho de banda que es desperdiciado por las colisiones de los paquetes. Una colisión se genera cuando una o más estaciones transmiten en forma simultánea.
- El periodo de tiempo crítico durante el cual puede ocurrir una colisión, es igual al retardo de propagación de extremo a extremo del ETHER.
- Cuando se genera una colisión, terminan su transmisión, cada estación envía intencionalmente algunos bytes adicionales para informar a las demás estaciones que ha ocurrido una colisión, esperan un tiempo aleatorio diferente cada una e intentan el proceso nuevamente.
- Cuando una estación desea transmitir, escucha al medio de comunicación para determinar si ya hay una transmisión en la red, si el ETHER esta ocupado, entonces la estación espera hasta que el medio este inactivo.
- A medida que aumenta el tamaño de la red, también debe de aumentar el tamaño mínimo del paquete para alcanzar a toda la red.
- El cableado de la red no debe de introducir ningún camino de regreso circular, si esto sucediera por cada paquete transmitido se detectaría una colisión, ya que el paquete se interferiría consigo mismo.

El sistema prototipo Ethernet se diseñó para operar a 3 Mbps y soportar hasta 256 estaciones y su alcance máximo era de 1Km, operó también en redes de área local del tipo de banda base a 10 Mbps, utilizó un método de acceso sensible a la señal portadora (CSMA/CD) en sus primeras etapas. El medio de comunicación (ETHER) elegido para el sistema prototipo fue un cable coaxial Community Antenna Televisión (CATV) estándar, este tenía características eléctricas apropiadas, además de que era económico.

Ethernet se diseñó como un sistema de comunicaciones apropiado para que se basaran en sistemas distribuidos de computadoras.

El nodo de una red Ethernet esta hecho de varios componentes, la conexión física al Ether se realiza con una derivación, la cual tiene una única restricción: (debe de afectar lo menos posible las características eléctricas del Ether), a la derivación se le conecta un transceptor, este es el componente que realiza la codificación y decodificación de los paquetes Ethernet, la interfaz serializa y deserializa el flujo de bits que intercambia con el transceptor, el controlador el cual es el encargado de la correcta transmisión y recepción de paquetes a través de la red.

Para extender una red Ethernet mediante múltiples segmentos se usan repetidores y filtros de paquetes. Un repetidor de paquetes es transmisor receptor bidireccional que opera en el nivel de bits, cuando el tamaño de la red se hace demasiado grande para los componentes del transceptor Ethernet, el Ether se puede dividir en dos secciones, con un repetidor de paquetes entre ellas; la figura 3.4.1.1 muestra el esquema de una red Ethernet de múltiples segmentos. El filtro de paquetes se usa cuando la cantidad de estaciones conectadas a la red causa una demanda de tráfico muy alta, la utilización de la línea puede caer a medida que aumenta el número de transmisores potenciales de una Ethernet debido a la gran cantidad de colisiones que ocurren, por lo que el retardo de acceso aumenta considerablemente.

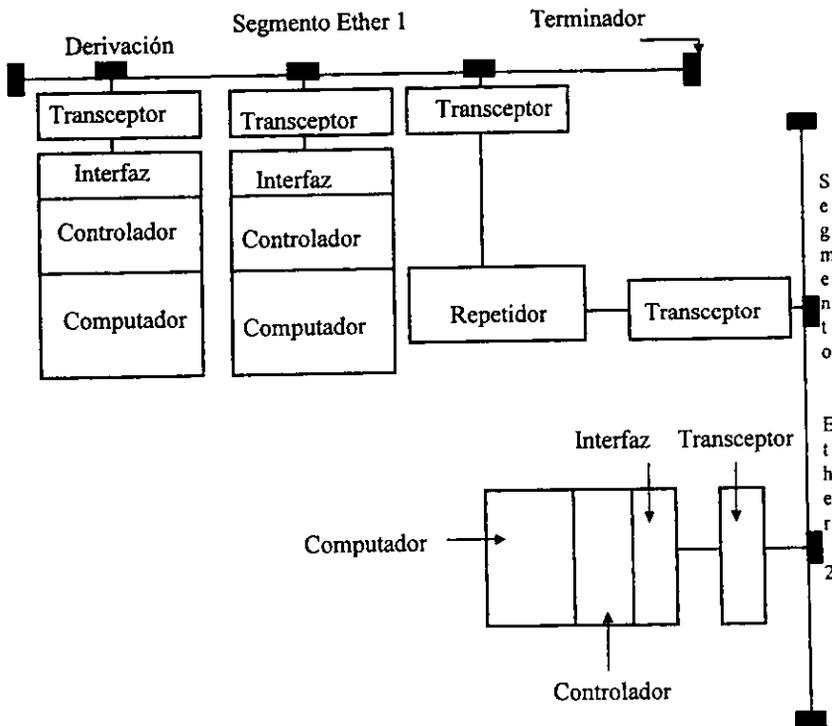


Figura 3.4.1.1. Red Ethernet de múltiples segmentos.

El estándar 802.3 especifica un bus utilizando a CSMA/CD como método de acceso. La primera edición del estándar 802.3 (Estándar 802.3-1985 del IEEE) definió una implantación de banda base de 1 a 10 Mbits/seg operando sobre varios medios físicos de la capa física del modelo de referencia OSI; lo cual hace diferir de Ethernet.

Existen dos especificaciones de Ethernet I y II antes de la adopción del 802.3. Ethernet I fue la original; Ethernet II fue la definición que se convirtió en 802.3, aunque se produce equipo diseñado para que funcione con ambos sistemas.

El nombre de Ethernet se refiere al cable (Ether) que se usa como medio para transmitir la señal. Hay dos tipos de cable coaxial que comúnmente se usan y son el cable delgado y el cable grueso.

En las realizaciones sobre cable coaxial, las estaciones de trabajo se conectan en serie conectando los segmentos de cable entre cada estación. Los segmentos forman un único y extenso sistema de cableado denominado *línea troncal*. La versión de cable trenzado de Ethernet adopta una topología en estrella, en la que el cable trenzado hacia cada estación es una rama que parte de un concentrador central de cableado según como se muestra en la figura 3.4.1.2.

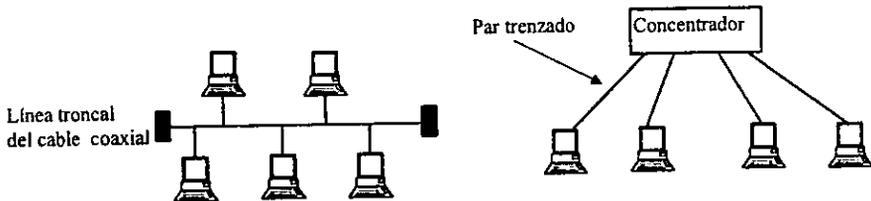


Figura 3.4.1.2. Configuraciones Ethernet de cable coaxial y par trenzado.

En general, la familia de los estándares 802 tiene que ver con la capa física y de enlace de datos definidos por el modelo de referencia OSI. La relación entre el modelo OSI con los estándares 802 se puede ver en la figura 3.4.1.3, en donde solamente las tres primeras capas del modelo OSI tienen relación con los estándares 802.

Segmentación

La segmentación es un proceso de división de un segmento Ethernet en dos o más segmentos, reduciéndose de esta manera el número de estaciones de trabajo conectadas a cada uno de los segmentos. Generalmente, se realiza la división de un segmento y se utiliza un puente o encaminador para conectar los dos segmentos, gestionando así el tráfico entre las redes.

Los sistemas operativos de red disponen de utilidades de encaminamiento incorporadas. Cada adaptador de red situado en un servidor de red forma un segmento separado de red. El sistema operativo gestiona el tráfico entre los segmentos. La figura 3.4.1.4 muestra un servidor con dos tarjetas de interfaz de red instalada, que trabaja con topologías Ethernet tipo bus y estrella. La elección de una u otra topología depende del diseño del entorno de oficina y tipo de cable a utilizar.

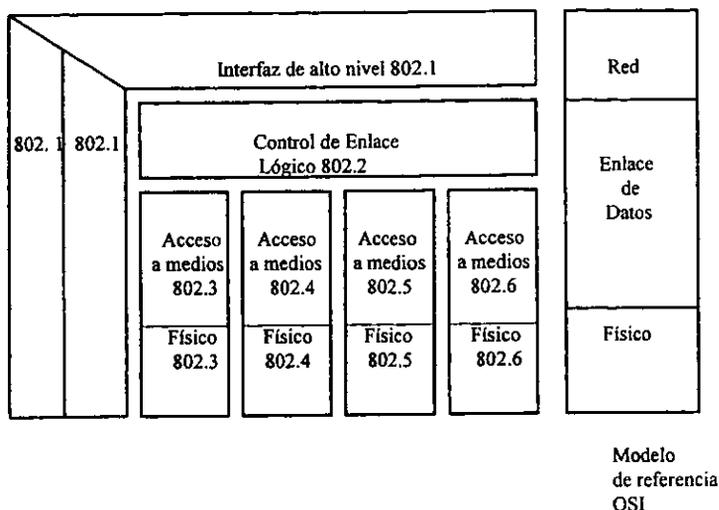


Figura 3.4.1.3. Relación de Estándares de IEEE y el Modelo de referencia OSI.

Una vez dividida una red con el objeto de reducir el tráfico y mejorar las prestaciones, se filtran los paquetes para reducir el tráfico en las redes no compatibles con esos paquetes. Una desventaja en este esquema de interconexión de redes es que los puentes y encaminadores introducen cierto retardo en la transferencia de paquetes entre redes. Los concentradores de conmutación pueden eliminar este problema de retardo.

Formatos de trama

Una trama Ethernet representa la estructura de un paquete de datos enviado a través de una red Ethernet. Describe la posición de las cabeceras, bits de datos y la carga útil de información del paquete. Por medio de un analizador de protocolos conectado a la red, se puede realizar una supervisión del tráfico de la red. Es posible descubrir ciertos problemas en una red observando el contenido de los paquetes y reuniendo estadísticas al respecto.

Existen cuatro tipos de trama en Ethernet:

- Ethernet II. Es el tipo de trama original de Ethernet. Asigna un única cabecera al paquete, el utilizado en las redes Apple Talk Phase y las redes conectadas a sistemas DEC o a computadoras que utilizan el protocolo TCP/IP (Transmission Control Protocol /Internet Protocol).
- Ethernet_802.3. Es tipo de trama utilizado genéricamente en redes NetWare de Novell.
- Ethernet_802.2. Es tipo de trama utilizado por defecto en redes NetWare 4.x de Novell.
- Ethernet_SNAP. Es tipo de trama utilizado en redes Apple Talk Phase II.

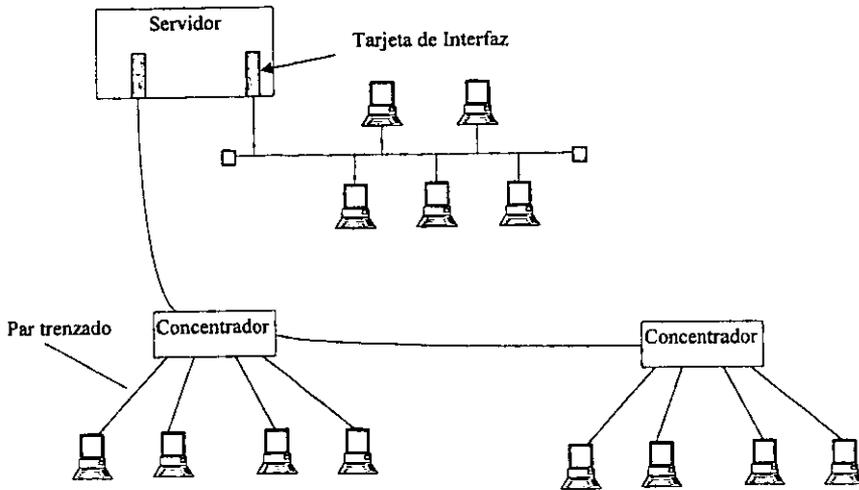


Figura 3.4.1.4. Un servidor de trabajo como puente encaminador hacia diferentes topologías.

Los campos más importantes de las tramas se describen a continuación:

- *Preámbulo*. Este campo señala el comienzo de la trama.
- *Delimitador de inicio de la trama (SFD, start frame delimiter)*. Este campo proporciona un campo adicional que indica el comienzo de la trama Ethernet IEEE 802.3.
- *Destino y origen*. Estos campos contienen la dirección de origen y destino.
- *Longitud (LEN) del campo de datos*. Este campo indica la longitud de la porción de datos de la trama.
- *Control de redundancia cíclica (CRC, Cyclical redundancy Checksum)*. Este campo mantiene un valor calculado por el emisor. El receptor realiza el mismo cálculo para ver si coincide con el valor de campo CRC. Si no es así, se considera que la trama se ha corrompido y se retransmite de nuevo.
- *Tipo*. Es la longitud de campo de datos.
- *PAD*. Son los bytes de relleno.

La figura 3.4.1.5 muestra los tipos de trama en Ethernet.

En las diferentes topologías de Ethernet hay que tomar en cuenta que el primer número del nombre se refiere a la velocidad en Mb/s, y el último a los metros que admite un segmento (multiplicado por 100). *Base* hace referencia a banda base y *Broad* a banda ancha.

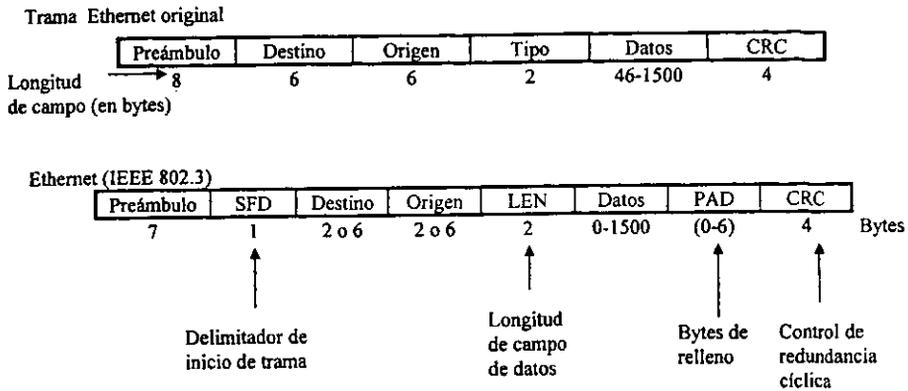


Figura 3.4.1.5. Tipos de trama en Ethernet.

La siguiente tabla 3.4.1.1 muestra las características de operación de cada una de las redes Ethernet y el IEEE 802.3.

Carac. de Operación	Ethernet	10BASE-2	10BASE-5	1BASE-5	10BASE-T	10BROAD-36
Vel. de Transmisión (Mbps)	10	10	10	1	10	10
Método de acceso al medio	CSMA/CD	CSMA/CD	CSMA/CD	CSMA/CD	CSMA/CD	CSMA/CD
Señalización	BANDA BASE	BANDA BASE	BANDA BASE	BANDA BASE	BANDA BASE	BANDA ANCHA
Máxima longitud (m) de segmentos	500	185~200	500	500	100	3600
Estaciones / segmento	100	30	100	12	12	100
Medio	50 ohms coaxial (grueso)	50 ohms coaxial (delgado)	50 ohms coaxial (grueso)	Cable Trenzado	Cable Trenzado	75 ohms coaxial
Topología	Bus	Bus	Bus	Estrella	Estrella	Bus

Tabla 3.4.1.1. Características de las redes Ethernet y el IEEE 802.3.

Ethernet 10Base-2 (DELGADO)

También llamada Cheapernet o Thinnet 10Base-2 utiliza cable delgado coaxial (RG-58 A/U o C/U) de 50 ohms y 4.8 mm de diámetro. Este cable permite una mejor manipulación que el cable grueso y requiere de transceptores en las estaciones. Alcanza una longitud máxima de segmento de 185 metros aunque en realidad se aproxima a 200 metros, utiliza métodos de transmisión en banda base. Utiliza la topología bus.

La figura 3.4.1.6 ilustra una red Ethernet de cable delgado y la figura 3.4.1.7 ilustra los componentes que presenta este sistema de cableado.

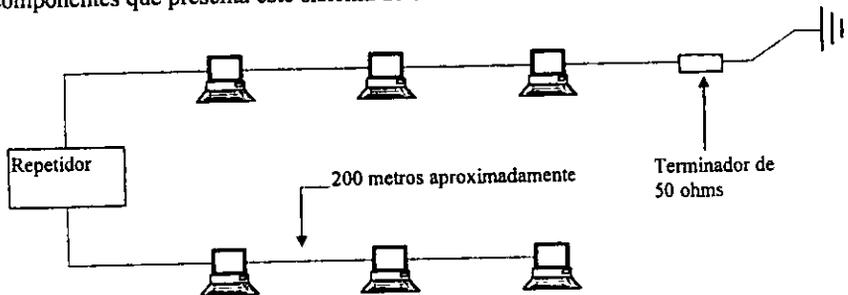


Figura 3.4.1.6. Red Ethernet de cable delgado (coaxial Ethernet 10Base-2).

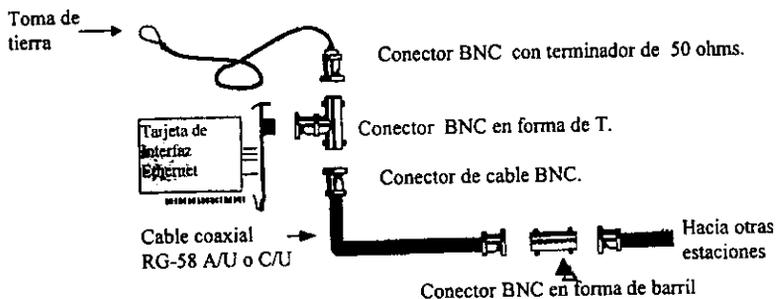


Figura 3.4.1.7. Componentes de un sistema de cableado Ethernet 10Base-2.

Componentes de una red 10Base-2: Tarjetas de interfaz de red, repetidores, cable Ethernet delgado, conectores de cable BNC, conectores en forma de T y terminadores BNC.

10Base-2 utiliza: Tarjeta de interfaz de red Ethernet para cable grueso o delgado. Conectores tipo BNC para formar uniones en T. Repetidores, cuando se necesita unir dos líneas troncales Ethernet y para reforzar las señales entre estas, un mensaje transmitido sobre de una red de área local (LAN) debe pasar a través de dos repetidores como máximo antes de alcanzar su destino o pasar a través de un puente de LAN. Cable delgado en forma de plenum a prueba de incendios. Conectores BNC en forma de barril y en forma de T. Terminadores BNC de 50 ohms para cada final del segmento de cable, cada segmento de cable necesita un terminador con toma de tierra y uno sin ella.

Pueden unirse hasta cinco segmentos troncales mediante cuatro repetidores. Las estaciones de trabajo sólo pueden conectarse en tres de los segmentos. Los otros segmentos se utilizan para distanciar. La longitud máxima de la línea troncal es de 910 metros. En una línea troncal puede haber hasta un máximo de 30 nodos. Los repetidores, puentes, encaminadores, servidores y estaciones de trabajo se consideran nodos. El número total de nodos en todos los segmentos no puede exceder de 1024.

Es posible combinar sistemas de cableado grueso y delgado Ethernet mediante un adaptador especial BNC/serie N macho o hembra en un extremo. Por ejemplo, puede utilizarse cable Ethernet grueso para conectar dos segmentos de cable delgado que están fuera del alcance permitido a un cable delgado. Hay que tener en cuenta que también puede utilizarse un repetidor para extender una red Ethernet.

Ethernet 10Base-5 (grueso)

Ethernet 10Base-5 soporta una longitud máxima de un segmento troncal de 500 metros cada estación se conecta a una línea troncal Ethernet gruesa mediante un transceptor a una distancia mínima al siguiente transceptor de 2.5 metros. La figura 3.4.1.8 muestra un esquema de cableado coaxial para una red Ethernet grueso. En algunos casos utiliza cable de par trenzado con longitud máxima de segmento de 500 metros y velocidad de transmisión de hasta un megabits/seg, y adopta una topología bus y se denomina 1BASE-5.

Componentes de una red 10Base-5: Interfaz de red, transceptores, cables para los transceptores, conectores macho serie N, conectores en forma de barril serie N y terminadores serie N.

Ethernet 10Base-5 utiliza: Interfaz de red, dispone de un conector tipo DIX (DB-15) para realizar la conexión del cable coaxial grueso (de 50 ohms y 9.25 mm de diámetro) procedente del transceptor. La tarjeta que se instale en el servidor tendrá que ser la mejor posible; mientras que la tarjeta que se instale en las estaciones de trabajo podrá ser una más económica. Los transceptores, se conectan al segmento troncal para unir estaciones de trabajo y el cable Ethernet grueso; la distancia máxima entre una estación de trabajo y el transceptor es de 50 metros; dispone de tres conectores, dos de ellos son la entrada y salida del cable grueso y la tercera se utiliza para conectar la estación de trabajo al transceptor mediante un cable especial para transceptor; los transceptores se conectan a la línea troncal de la red de dos formas

posibles, por medio de un sistema de abrazaderas que atraviesa el cable, eliminando la necesidad de cortarlo y montar los conectores; de forma alternativa una versión BNC del transceptor dispone de un conector T al que se conectan los extremos del cable; en el transceptor se realiza un examen a través de pulsos eléctricos, para determinar si la estación se encuentra conectada correctamente. Cable especial para transceptor, este cable se suministra normalmente con cada unidad de transceptor; en cada extremo del cable especial se monta un conector tipo DIX (en un extremo macho y en el otro hembra), junto con cierres deslizantes que sirven para bloquear el cable con la placa de red; este cable para transceptor normalmente es más flexible que el cable troncal. Conectores macho serie N, estos conectores se instalan en ambos extremos del cable, cuando se utilizan transceptores en forma de T; los cables ya ensamblados tienen montados los conectores. Conectores en forma de barril serie N, unen dos segmentos de cable. Terminadores serie N, cada segmento de cable debe de finalizar en ambos extremos de un segmento principal, con un terminador serie N de 50 ohms, con uno de sus extremos conectado a tierra.

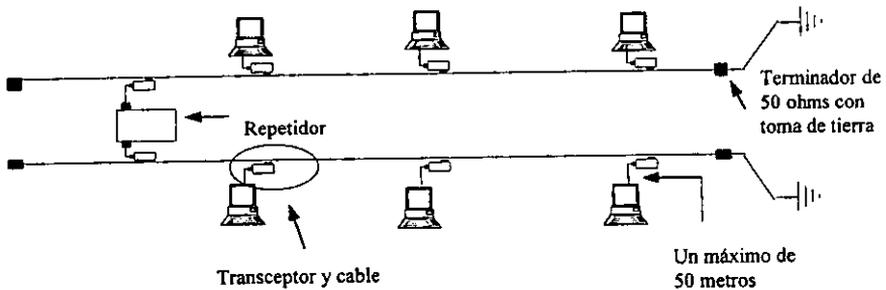


Figura 3.4.1.8. Ejemplo de cableado Ethernet 10Base-5 "cable grueso".

Pueden unirse hasta cinco segmentos troncales mediante cuatro repetidores. Las estaciones de trabajo pueden conectarse únicamente a tres de los segmentos. La longitud máxima principal resultante de la unión de los segmentos es de 2460 metros. En una línea troncal puede existir un máximo de 100 estaciones de trabajo.

Ethernet 10base-T (par trenzado)

Ethernet 10Base-T soporta el cable de par trenzado longitud máxima de segmento de 100 metros, adopta una topología en estrella o distribuida, es más barato que el cable coaxial. Utilizan cable de Categoría 3 o 4, aunque categorías superiores de cable (como la Categoría 5) permiten un crecimiento futuro que acepta tecnologías de transmisión más rápidas, como 100 Mbts/seg. La mayoría de las tarjetas 10Base-T tienen actualmente incorporado el transceptor, para conectar directamente al cable RJ-45.

En la figura 3.4.1.9 se muestra una red básica de Ethernet 10Base-T las estaciones de trabajo se conectan a un concentrador central que actúa como repetidor. Cuando llega la señal procedente de una estación de trabajo, el concentrador la difunde hacia todas las líneas de salida. Es posible realizar conexiones entre distintos concentradores para obtener una configuración jerárquica. Los cables se conectan a un transceptor en un punto próximo a la estación de trabajo, que a su vez se conecta a ésta con un cable de 15 hilos de longitud no superior a 50 metros.

Componentes de Ethernet 10Base-T: Tarjetas de interfaz de red, concentradores (Hub), cable de par trenzado, transceptores, enchufes de pared y conectores RJ-45.

Ethernet 10 Base-T utiliza: Tarjetas de interfaz de red con conector tipo DIX de 15 patillas o RJ-45 10Base-T. Concentradores, hasta con 12 puertos, normalmente dispone de un puerto de conexión a redes con soporte de cable coaxial o de fibra óptica, pueden conectarse hasta 12 concentradores en un concentrador central para aumentar el número de estaciones de trabajo en la red. Cable de par trenzado, con conectores RJ-45 en ambos extremos del segmento, utiliza cuatro pares trenzados de acuerdo con la norma EIA/TIA 568. Transceptores, con bases RJ-45 en un lado y DB-15 en el otro, si es que las tarjetas no presentan un transceptor ya incorporado. Enchufe de pared, con bases RJ-45. Conectores RJ-45, Las patillas 1 y 2 son transmisoras y la 3 y 6 son receptoras; cada par está cruzado de modo que el transmisor en un extremo se conecta con el receptor en el otro.

Pueden existir hasta 1024 estaciones en una red sin necesidad de utilizar puentes. Algunas de estas especificaciones son flexibles, dependiendo del fabricante.

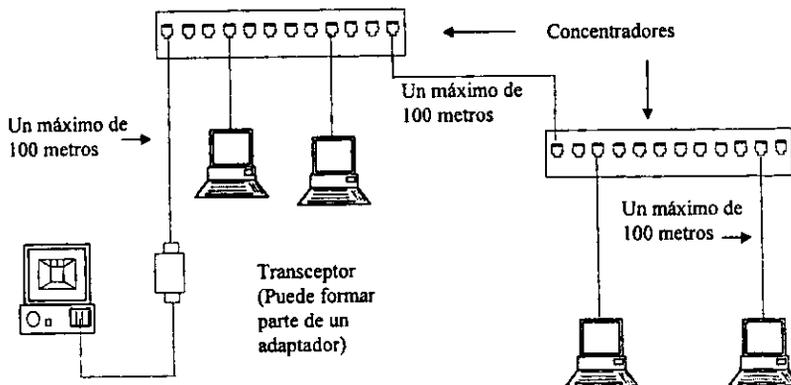


Figura 3.4.1.9. Ejemplo básico de cableado Ethernet 10Base-T.

10Broad-36

Utiliza cable coaxial (RG-59 A/U CATV) con una impedancia de 75 ohms en diversos tamaños, la longitud máxima del segmento es de 3600 metros, está basada en el estándar 802.3 que utiliza métodos de transmisión en banda ancha, adopta una topología tipo bus.

10Base-F

Sirve de soporte a redes de fibra óptica de hasta 4 Km con una velocidad de transmisión a 10 Mbits/seg. La EIA/TIA (Electronic Industries Association/ Telecommunication Industries Association) ha adoptado este cable para establecer conexiones cruzadas entre los edificios.

Si la tarjeta de interfaz de red se instala en una estación sin disco debe utilizarse una memoria programable de solo lectura PROM (programmable read-only memory) de arranque remoto.

3.4.2 TOKEN BUS IEEE (802.4)

Una red Token Bus (bus con testigos) o (bien red de paso de estafeta en canal), es similar a una red en anillo con testigo, en la que una estación debe de tomar la posesión de un testigo antes de que pueda transmitir en la red. Sin embargo la topología y el método de paso de testigo son diferentes.

El comité 802.4 IEEE ha definido las normas de bus con testigo como redes de banda ancha en oposición a la técnica de transmisión de banda base de Ethernet.

Las redes Token bus se construyen con cable coaxial CATV de 75 ohms con el uso de una topología en bus. Las características de la banda ancha de la norma 802.4 IEEE nos dice que soporta transmisión simultánea en ambos canales. El cable de banda ancha tiene capacidades de distancia más grandes y velocidades de transmisión de hasta 10 Mbits/seg.

La norma IEEE 802.4 Token Bus, físicamente, es un cable lineal, en forma de árbol, al cual se le conectan las estaciones. Está lógicamente organizado en un anillo, en el que cada una de las estaciones conoce la dirección de la estación que le precede y de la estación que le sigue, de acuerdo con la secuencia numérica de las direcciones de las estaciones. Cuando el anillo lógico se inicia, la estación que tiene el número mayor es la que puede enviar la primera trama. Después de que esta lo hizo, pasa la autorización a su consecutiva inmediata, mediante la trama de control especial (estafeta) para que esta a su vez pueda transmitir información, la estafeta se propaga alrededor del anillo lógico, de tal forma que solo su poseedor este autorizado para transmitir tramas. La última estación en orden numérico pasa de nuevo el testigo a la primera. El testigo no sigue el orden físico en que las estaciones de trabajo se unen al cable. La estación 1 podría estar en un extremo del cable, la estación 2 podría estar en el

otro extremo, y la estación 3 podría estar en medio. Como solamente una estación puede tener la estafeta, no hay posibilidad de colisiones. La figura 3.4.2.1 muestra una red Token Bus.

El orden físico en el que se encuentren conectadas las estaciones no es importante. Como el cable es de manera inherente a un medio físico de difusión, cada estación recibe cada trama, descartando las que no le están dirigidas. Cuando una estación pasa la estafeta, envía una trama de estafeta dirigida específicamente a su vecino lógico en el anillo independientemente del lugar físico en donde se encuentre la estación en el cable. También es importante hacer notar que, cuando las estaciones se activan por primera vez estas no están dentro del anillo, así que el protocolo tiene la capacidad para agregar y retirar las estaciones del anillo.

La topología en bus con testigo es muy adecuada para grupos de usuarios que se encuentran separados por ciertas distancias.

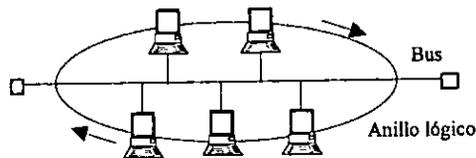
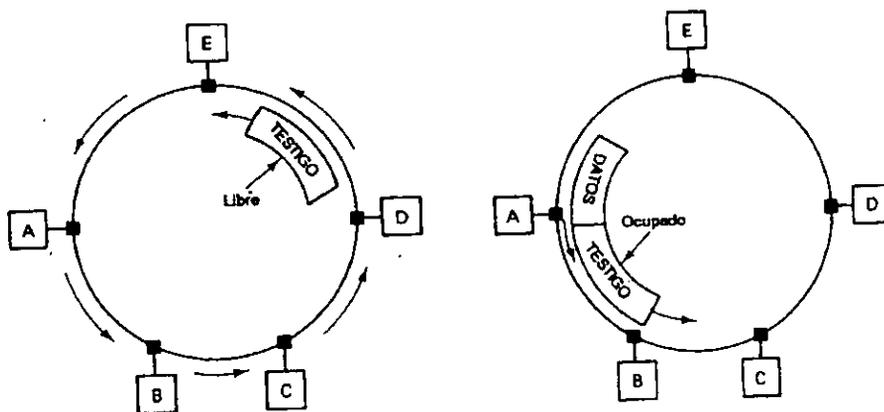


Figura 3.4.2.1. Red Token Bus.

3.4.3 TOKEN RING IEEE(802.5)

Las redes Token Ring son usadas principalmente en las oficinas. Su funcionamiento es de la siguiente manera; cada vez que una estación de trabajo quiere enviar una trama, primero espera el Token (testigo o estafeta), el testigo es el que controla el uso del anillo, e indica si esta ocupado o no. Un testigo ocupado indica que alguna estación está haciendo uso del control del canal y está transmitiendo datos. Por el contrario un testigo libre señala que el anillo esta desocupado y cualquier estación queda autorizada a transmitir en el momento que lo reciba.

Durante el período que una estación posee el testigo, adquiere el control absoluto del anillo y entonces la estación transmisora u origen inserta su trama de datos detrás del testigo y envía esta corriente de datos por el anillo, la cual incluye el encabezado de la trama y la dirección de la estación destino. La trama es retransmitida (es decir que cada bit que se recibe es retransmitido) por todas las estaciones en el anillo hasta que regresa a la estación origen, donde es retirada de la circulación del anillo, en ese momento, esta estación deberá transformar el testigo ocupado en uno libre, y lo entregará a la siguiente estación. En la retransmisión de la trama, la estación destino retiene una copia de la trama (datos) e indica una respuesta a la estación origen. De esta manera se evita que una estación monopolice el uso del anillo. Si el testigo vuelve a recorrer todo el anillo sin que nadie la aproveche, la estación podrá capturarla de nuevo y seguir transmitiendo datos. La figura 3.4.3.1 muestra el paso de testigo o estafeta en anillo.



El testigo o estafeta (libre) circula por el anillo.

La estación A obtiene el control del anillo.

Figura 3.4.3.1. Red de paso de estafeta o testigo en anillo (Token Ring).

Una estación de trabajo libera el testigo de dos formas diferentes dependiendo de la razón de la velocidad de los datos del anillo. Con un anillo de menor velocidad (4 Mbps), el testigo es liberado hasta después de que los bits de respuesta han sido recibidos en la estación emisora. Con los anillos de alta velocidad (16 Mbps), esta es liberada después de la transmisión del último bit de la trama. Esto se le llama liberación temprana del testigo.

Las redes Token Ring IBM usan transmisión en banda base en cualquiera de sus implementaciones de 4 ó 16 Mbps.

La red Token Ring IBM usa un cableado en estrella con topología en anillo lógico. Los dispositivos sobre la red son físicamente conectados a concentradores de cableado. El concentrador de cableado puede ser pasivo como las unidades de acceso multiestación (MAU, Multistation Access Unit); o dispositivo activo como la unidad de acceso controlada (CAU, Controlled Access Unit). Las unidades de acceso son usadas como un punto de control del acceso físico al anillo y para proporcionar la desviación de la conexión (bypass) de una estación para dispositivos defectuosos o inactivos. El uso de unidades de acceso evitan que al agregar o retirar una estación del anillo se interrumpa la señal en éste, afectando a los demás dispositivos del mismo.

Las estaciones de trabajo se conectan a los concentradores centrales (MAU's). Para crear redes grandes multiestación se conectan múltiples concentradores conjuntos, el concentrador contiene un anillo colapsado, como se muestra en la figura 3.4.3.2, si una estación de trabajo falla, la MAU inmediatamente evita la estación para mantener el anillo de la red.

La instalación de las MAU's adicionales aparece en la figura 3.4.3.3. Se proporciona un receptáculo de entrada y salida al anillo en cada MAU's para conexión con otras MAU's. Cuando se conectan de esta manera mantiene la formación en anillo, debido a que el cable contiene múltiples pares de hilos, un corte en un cable causa que el anillo se vuelva sobre sí mismo como se muestra en la figura 3.4.3.4. Simplemente se encaminan las señales en la dirección opuesta, mediante la creación de un bucle de vuelta en la configuración del cable.

También se podrían utilizar repetidores para extender la distancia de la red Token Ring la figura 3.4.3.5 muestra como se puede configurar una red Token Ring en una oficina grande o en un edificio con varias plantas. El anillo principal conecta todas las MAU's en una formación circular.

Las tarjetas Token Ring de IBM están disponibles para una velocidad de 4 Mbits/seg y 16 Mbits/seg. La versión más rápida tiene una longitud de trama incrementada, que requiere menos transmisiones, para la misma cantidad de datos. Son comunes el cable de par trenzado no apantallado y las MAU's con 16 puertos. Además, hay concentradores de dos a cuatro puertos disponibles por algunos vendedores. Esos concentradores se ramifican de una MAU de ocho puertos y permiten la conexión de dos a mas estaciones de trabajo en grupo.

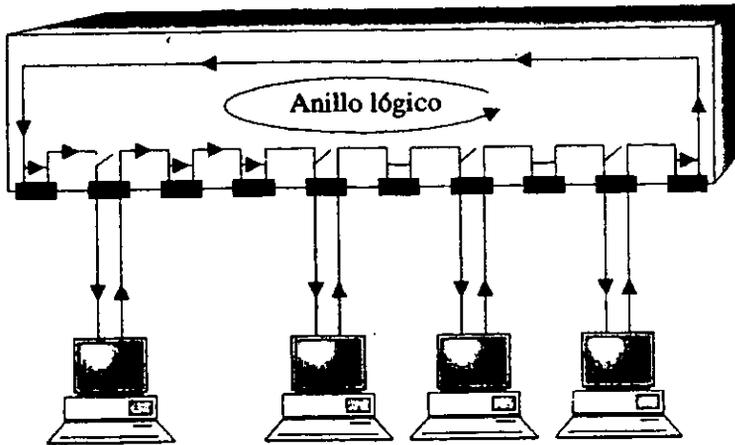


Figura 3.4.3.2. La unidad de acceso multiestación contiene un anillo colapsado con una conmutación que las rodea.

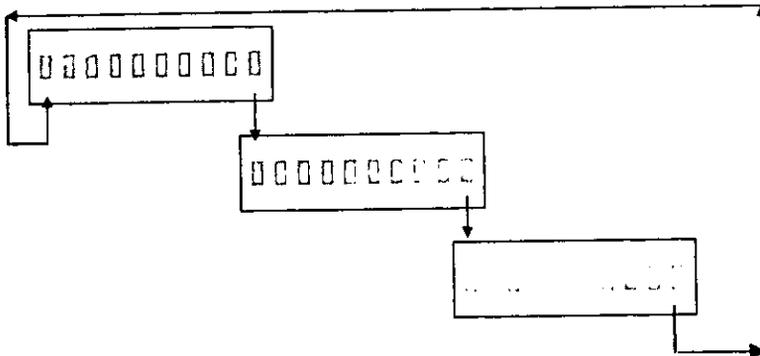


Figura 3.4.3.3. Interconexión de las MAU's de forma que se mantenga la configuración en anillo.

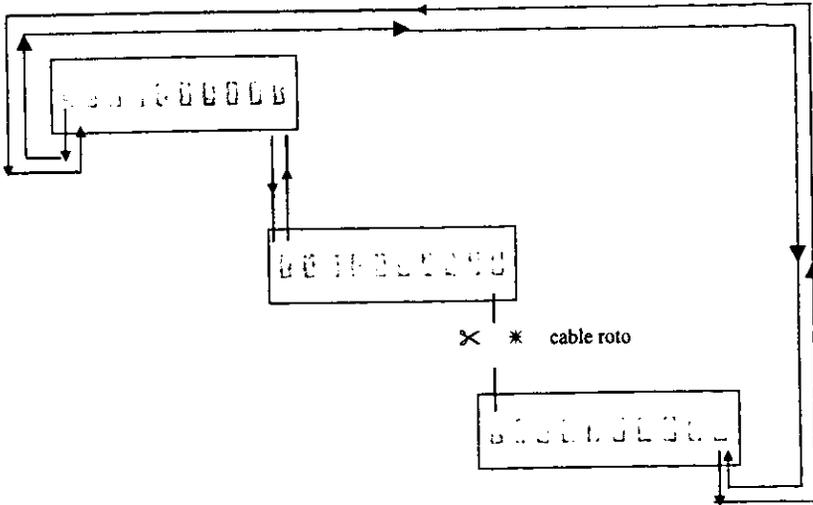


Figura 3.4.3.4. Si se corta un cable entre una MAU, la red se mantiene viva mediante la formación de un bucle de vuelta que utiliza un conjunto de hilos redundantes en el cable.

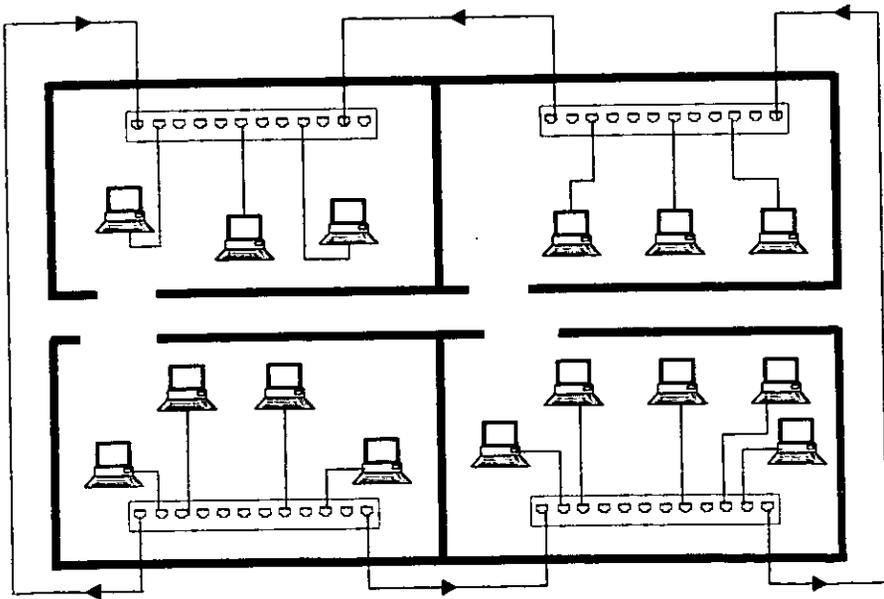


Figura 3.4.3.5. Una red con paso de testigo en anillo grande consta de un anillo que se expande por toda la organización.

Las especificaciones Token Ring de IBM, permiten los tipos de cable de acuerdo a la Tabla 3.4.3.1.

Cable	Conductor	Pares / Calibre	Blindaje de metal	Uso en:
Tipo 1	Cobre (alambre)	Dos pares trenzados / 22 AWG	Sí, trenzado o apantallado	Trayectorias principales, pisos falsos, espacios entre el techo y el piso siguiente de un edificio, exteriores, áreas de trabajo y cableado de gabinetes.
Tipo 2	Cobre (alambre)	Dos pares trenzados / 22 AWG (para datos) + Cuatro pares / 22 AWG TTP (para voz)	Sí, trenzado No	Áreas de trabajo y cableado de gabinetes.
Tipo 3	Cobre (alambre)	Cuatro pares / 22 ó 24 AWG TTP	No	Áreas de trabajo y cableado de gabinetes.
Tipo 5	Fibra Óptica	Dos Fibras / 100/140 Núcleo / recubrimiento [micras]	No	Trayectorias principales interiores.
Tipo 5J	Fibra Óptica	Dos Fibras / 50/125	No	Trayectorias principales (500 m máximo)
Tipo 6	Cobre (alambrado)	Dos pares trenzados / 26 AWG	Sí, trenzado	Áreas de trabajo y cableado de gabinetes.
Tipo 8	Cobre (alambre)	Dos pares paralelos / 26 AWG	Sí, trenzado (cada par)	Áreas de trabajo debajo de la alfombra.
Tipo 9	Cobre (alambre)	Dos pares / 26 AWG	Sí, Trenzado	Trayectorias Principales. Espacios entre el techo y el piso siguiente de un edificio.

Tabla 3.4.3.1. Tipos de cable IBM usados en redes Token Ring.
Par trenzado telefónico (TTP, Telephone Twisted Pair).
Calibre americano para conductores eléctricos (AWG, American Wire Gauge).

Componentes de una red normalizada TOKEN RING que utilizan cable tipo 1

Tarjetas de interfaz Token Ring. Las tarjetas paso de testigo en anillo están disponibles en un modelo de 4 Mbits/seg y en otro de 16 Mbits/seg. Si se usa una tarjeta a 16 Mbits/seg en una red a 4 Mbits/seg, se opera a 4 Mbits/seg. Asegurar de usar tarjetas de 16 Mbits/seg en su propia red.

Unidades de acceso multiestación (MAU's, Multistation Access Units). Una MAU conecta a ocho o más estaciones de trabajo con el uso de cables adaptadores de red. Se pueden interconectar hasta doce dispositivos MAU.

Cables adaptadores para red de paso de testigo en anillo. Típicamente los cables para red de paso de testigo en anillo tienen un conector de nueve patillas en un extremo, para fijarse a la tarjeta de interfaz de red, y un conector de datos que se enchufa a la MAU. Generalmente los cables adaptadores únicamente tienen 2.5 metros de longitud, pero hay cables alargadores para extenderlos en incrementos de hasta 46 metros.

Cables alargadores. Los cables alargadores aumentan la distancia de una estación de trabajo a un dispositivo MAU, o cablean dos o más dispositivos MAU juntos. En el sistema IBM, serían cables Tipo 6 de cualquier longitud hasta 46 metros.

Conectores. El cable Tipo 1 usa conectores de datos Tipo 1 del sistema de cableado IBM.

Filtros del medio. Cuando se usa cable telefónico de par trenzado Tipo 3, se necesita un filtro del medio en la estación de trabajo. Este convierte los conectores de cable y reduce el ruido de línea.

Panel alargador: Es útil para la organización de cable entre la MAU y un bloque de conexión telefónico. Se usa un conector telefónico normalizado para conectar el panel alargador al bloque de conexión; otra manera, es cablear la MAU directamente al bloque de conexión.

El número máximo de estaciones en anillo es de 260 para cable apantallado y de 72 para cable telefónico de par trenzado sin apantallar. La distancia máxima desde una estación de trabajo a una MAU, cuando se utiliza cable Tipo 1 es de 101 metros en un segmento continuo. Si se juntan los segmentos de cable mediante el uso de cable alargador, la distancia máxima de la estación de trabajo a la MAU es de 45 metros; debido a que dicho cable alargador reduce por al mitad la distancia de la estación de trabajo a la MAU.

Tramas anillo con testigo

En la figura 3.4.3.6 se dibujan los dos tipos de tramas de paso de anillo con testigo. La parte superior es para el testigo y la inferior se utiliza para la transferencia de información de control.

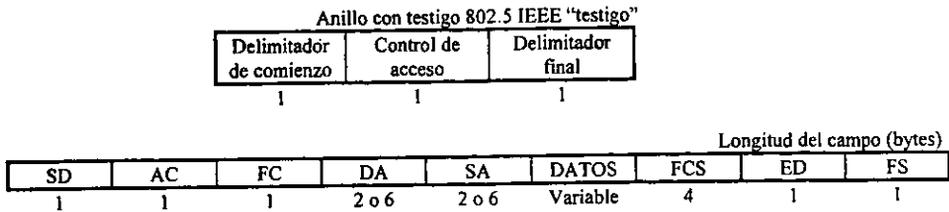


Figura 3.4.3.6. Muestra los dos tipos de tramas de paso de anillo con testigo.

SD = Delimitador de comienzo.
 AC = Control de acceso.
 FC = Control de trama.
 DA = Dirección del destino.
 SA = Dirección de la fuente.
 FCS = Secuencia de verificación de trama.
 ED = Delimitador final de trama.
 FS = Estado de la trama.

- *Delimitador de comienzo.* Indica el comienzo de los datos. Tiene un código único para diferenciarlo de los datos.
- *Control de acceso.* Contiene información sobre la prioridad de la trama y sobre la necesidad de futuras reservas del testigo, para que las demás estaciones le concedan si tienen una prioridad más baja.
- *Control de trama.* Define el tipo de trama, bien sea información para el control de acceso al medio (MAC, Media Access Control) o información para la estación final. Si la trama es una trama MAC, todas las estaciones del anillo leen la información. Si contiene información, únicamente leerá la estación destino.
- *Dirección del destino.* Contiene la dirección de la estación destino que recibe la trama. Se puede direccionar a todas las estaciones del anillo.
- *Dirección de la fuente.* Contiene la dirección de la estación origen que envía la trama.
- *Datos.* Contiene el campo de datos. Si la trama es una trama MAC, este campo puede contener información de control adicional.
- *Secuencia de verificación de la trama.* Contiene información de control de errores para asegurar al receptor la integridad de la trama.
- *Delimitador de final de trama.* Indica el final de la trama.
- *Estado de la trama.* Proporciona indicación de si una o más estaciones en el anillo reconocen la trama, si la trama se copió o si la estación destino no está disponible.

3.4.4 INTERFAZ DE DATOS DISTRIBUIDOS POR FIBRA (FDDI)

Interfaz de Datos Distribuidos por fibra óptica, (Fiber Distributed Data Interface, FDDI). Es una norma de cable de fibra óptica desarrollado por el comité X3T9.5 del Instituto Americano de Normalización (American, National, Standards, Institute, ANSI). Que especifica a las redes de fibra óptica con topología de doble anillo que admite 500 nodos sobre una distancia máxima de 100km, soporta un ancho de banda de 100 Mbps. Los anillos dobles ofrecen redundancia (tolerancia a fallos). Si se produce el fallo de un enlace o se corta el cable, el anillo se reconfigura por si solo como se muestra en la figura 3.4.4.1 de modo que puede continuar la transmisión del tráfico en la red.

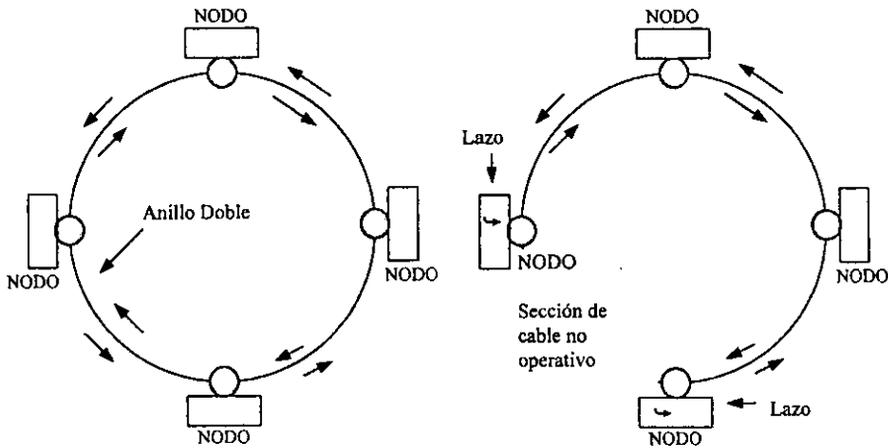


Figura 3.4.4.1. Anillos FDDI.

Las estaciones conectadas directamente a FDDI disponen de una conexión punto a punto con las estaciones adyacentes. En la configuración de doble anillo se utiliza un canal para la transmisión y otro de seguridad. Algunas estaciones de acoplamiento doble (Dual-Attached Stations, DAS) se conectan a los dos anillos. Las estaciones de acoplamiento único (Single-Attached Stations, SAS) se conectan a través de un concentrador que proporciona las conexiones oportunas a muchas SAS's. Una de las ventajas de esta configuración es que una SAS que falle no puede romper el anillo. Además la mayoría de las SAS's son estaciones de trabajo de usuario que se apagan a menudo, lo que podría interrumpir el anillo si su conexión se realizara de una forma directa.

En cuanto a la conexión de un encaminador y de una LAN al anillo FDDI. El sistema óptico proporciona la tecnología que mantiene al anillo intacto si se produce un fallo en el encaminador. Puede utilizarse una conexión redundante para dispositivos de cierta importancia, como los servidores que necesitan mantener una conexión continua. Si una de las

conexiones falla, se establece la otra mediante las dos conexiones DAS de un servidor, según se muestra en la figura 3.4.4.2.

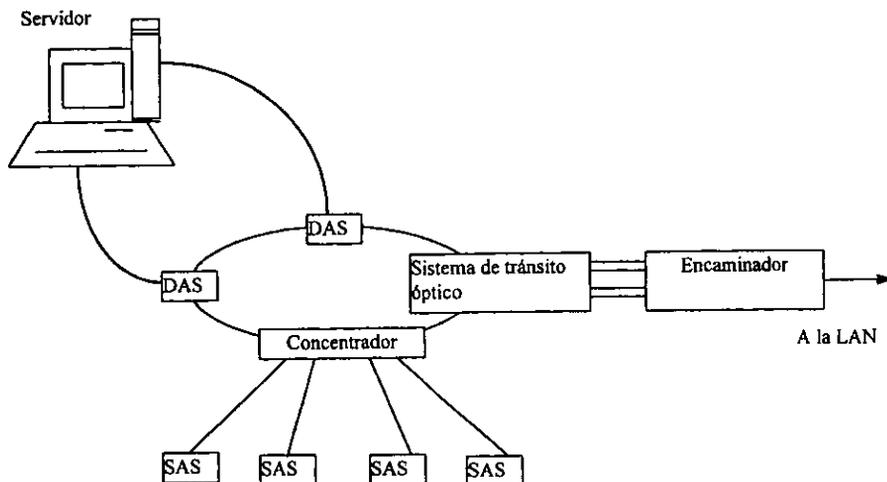


Figura 3.4.4.2. Configuración de una red-soporte FDDI.

Algo que debe de mantenerse presente respecto a cualquier red compartida como FDDI es que su ancho de banda puede llegar a saturarse. Por ejemplo FDDI proporciona un ancho de banda de 100 Mbits/seg, con los que 10 estaciones de trabajo sobre Ethernet que transmite de una forma simultánea puede producir una saturación de ese ancho de banda. Debe evaluarse los requisitos de tráfico de la red. Posiblemente un concentrador de alta velocidad podría proporcionar una solución mejor. Con el crecimiento del uso de vídeo y multimedia, un ancho de banda de 100Mbits/seg, puede convertirse en un cuello de botella; los concentradores de conmutación (Asynchronous Transfer Mode, ATM), podrían ser más adecuados para resolver estos problemas de la red. Alternativamente una red Ethernet rápida puede ofrecer una red más económica a 100 Mbits/seg.

Algunos de los concentradores y dispositivos de conmutación, disponen de puertos Ethernet para estaciones de trabajo y puertos FDDI para servidores. Para estos servidores tiene más sentido uso de adaptadores FDDI. La figura 3.4.4.3 ilustra 10 estaciones Ethernet que encaminan su tráfico hacia un concentrador de conmutación, que reenvía dicho tráfico hacia un servidor con adaptadores FDDI.

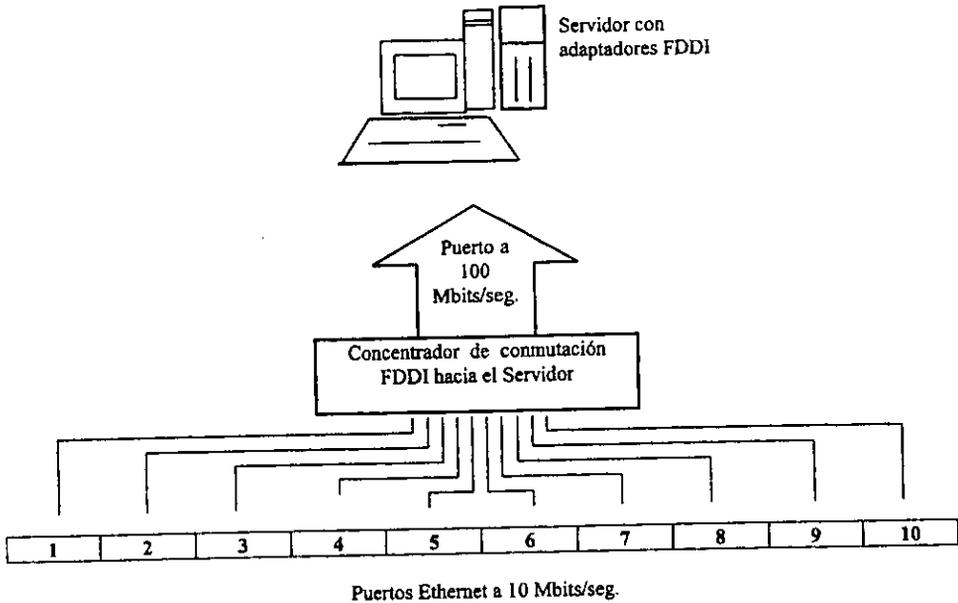


Figura 3.4.4.3. Estaciones de trabajo que se conectan hacia un servidor FDDI.

Método de acceso a FDDI

FDDI utiliza un método de paso de testigo. Se pasa una trama testigo de estación a estación a través de la red; si una estación necesita transmitir, captura la trama. La estación transmite los datos y sitúa el testigo de vuelta en el anillo al finalizar. Se utiliza un mecanismo de regulación para evitar que una estación mantenga el testigo durante demasiado tiempo; las estaciones que generen un alto volumen de tráfico pueden tener mayor prioridad la cual será asignada por el administrador de la red, generalmente concediéndoles un período mayor de tiempo de transmisión antes de liberar el testigo. Ténganse en cuenta las siguientes características:

- Las estaciones directamente conectadas a FDDI trabajan como repetidores. Reciben paquetes de un vecino y los envían al otro, siguiendo el sentido correcto. Cuando un nodo detecta su dirección en un paquete, la copia en su memoria.
- Pueden existir múltiples tramas en la red. Si una estación renuncia al testigo mientras sus tramas todavía se encuentran en tránsito, las otras estaciones pueden comenzar a transmitir.
- Se utiliza un mecanismo de gestión denominado gestión de estación, que capacita a los administradores del sistema a gestionar y a realizar una supervisión de las redes FDDI, los nodos aislados que producen fallos y el tráfico en ruta.

Tipos de FDDI

FDDI dispone de tres modos de transmisión. Los dos primeros, asíncrono y síncrono, descritos por la norma FDDI original. El tercero basado en circuitos, puede proporcionar circuitos dedicados. Este modo se encuentra disponible en la nueva norma FDDI-II, que requiere nuevas tarjetas de adaptación. Estos modos de transmisión resuelven problemas de la naturaleza del paso de testigo de FDDI y la estructura variable de sus tramas las cuales no ofrecen flujo uniforme de datos requeridos aplicaciones de multimedia y video en tiempo real, lo cual puede provocar que una presentación ante un usuario tenga un aspecto discontinuo.

Servicios asíncronos

El modo de anillo asíncrono se basa en el uso de un testigo. Cualquier estación puede acceder a la red mediante la captura del testigo. Este modo implica que no se establece priorización sobre algún tipo de tráfico, lo cual perjudica al tráfico sensible al tiempo, ya que consiste en almacenar los paquetes recibidos hasta completar el conjunto y ordenarlos, y entonces exhibir el vídeo. Sin embargo, esto origina un retraso inaceptable en videoconferencia interactiva, en cual las personas establecen conversaciones.

Servicios síncronos.

El modo de anillo síncrono con testigo permite realizar una priorización de tráfico sensible al tiempo, de modo que los paquetes lleguen dentro de unos márgenes de tiempo. Las tarjetas FDDI que ofrecen capacidad síncrona conceden a los administradores de la red posibilidad de reservar parte del ancho de banda para el tráfico sensible al tiempo; las estaciones asincrónicas luchan por el resto.

Servicios basados en circuitos.

Los servicios basados en circuitos pueden crear una línea de comunicación dedicada entre dos estaciones de trabajo con un ancho de banda garantizado, mediante la asignación de intervalos de tiempo regulares y repetidos durante la transmisión. Este método se denomina comunicación isócrona.

La norma FDDI-II se recomienda aplicar a redes que necesitan transportar vídeo en tiempo real u otro tipo de información que no puede tolerar retrasos. Recomienda que todos los nodos de esta red utilicen FDDI-II; de lo contrario la red se convertiría en una red FDDI. También se recomienda que las estaciones FDDI existentes deberían conectarse a sus propias redes.

FDDI-II utiliza técnicas de multiplexación que dividen el ancho de banda en circuitos dedicados que así mismo pueden garantizar la distribución del tráfico multimedia. Puede crear hasta 16 circuitos separados que trabajan dentro de unos márgenes de velocidad establecidos entre 6.144 Mbits/seg hasta 99.072 Mbits/seg cada uno. La razón de esta variación reside en que el ancho de banda se configura según las necesidades de las estaciones. Cada uno de esos

canales se puede subdividirse posteriormente para producir un total de 96 circuitos separados a 64 kbits/seg.

Estos canales pueden servir de soporte a tráfico asíncrono e isócrono. Los intervalos regulares de tiempo se asignan al anillo para la transmisión de los datos. Las estaciones que gozan de prioridad utilizan el número de intervalos que necesitan para distribuir sus datos dentro de unos márgenes de tiempo. Si estos intervalos no se utilizan por estas estaciones, inmediatamente se asignan a otras.

Esta norma aún no ha sido difundida ampliamente por la incompatibilidad que existe con el diseño FDDI y por otra parte es que ATM es una tecnología de red más interesante para alto tráfico y tráfico dependiente del tiempo.

FDDI/UTP

Una alternativa que sigue la norma de FDDI consiste en el uso del cable de cobre de par trenzado UTP. Se propuso originalmente por IBM Cabletron Systems y otros. La norma (Twisted Pair Physical Medium Dependent, TP-PMD) de ANSI define una red FDDI que trabaja con cable categoría 5 y cable de par trenzado blindado (STP, Shielded Twisted Pair) tipo 1 de IBM. Tiene las características de FDDI, excepto una diferencia en cuanto a la longitud del cable. UTP soporta 100 metros entre los nodos, mientras que la fibra permite soporta 2 Km entre ellos.

Las instalaciones de Ethernet 10Base-T con cable de par trenzado de grado de datos Categoría 5 están preparadas para adaptarse a la norma FDDI/UTP. Pero de alguna u otra manera hay que tener presente que FDDI y 10Base-T presentan distintas configuraciones de cableado. Aunque ambas admiten las conexiones de las estaciones de trabajo a los concentradores, FDDI también acepta conexiones de estaciones de trabajo entre sí, adoptando una configuración que forma un anillo doble. Las estaciones de trabajo se conectan mediante una configuración en forma de estrella desde un concentrador, por medio del cual puede proporcionar una conexión a un anillo de fibra óptica FDDI. Los cables que proceden de los concentradores, van al panel de conexión. El panel de conexión organiza el trayecto del cable que se dirige a las estaciones de trabajo.

3.4.5 INTERFAZ DE DATOS DISTRIBUIDOS POR CABLES DE PAR TRENZADO (CDDI)

Interfaz de Datos Distribuidos por Cables de Par Trenzado, (Copper Distributed Data Interface, CDDI) consiste en una versión de la especificación FDDI diseñado para permitir el uso de cables de par trenzado blindado (Shielded Twisted Pair, STP) y cables de par trenzado sin blindaje (Unshielded Twisted Pair, UTP). Es una norma desarrollada separadamente por Cabletron y Crecendo, que combinado por los resultados de su trabajo, recibieron la aprobación del Instituto Americano de Normalización (American National Standard Institute,

ANSI) en 1993. Una red CDDI típica consiste en concentradores con cierto número de puertos para la conexión de estaciones de trabajo. Debido a que CDDI ha limitado las distancias de cableado, un concentrador CDDI puede conectarse a un anillo FDDI como subred.

3.5 ÁREA AMPLIA

3.5.1 PROTOCOLO INTERNET DE LÍNEA SERIE, (SLIP)

Protocolo Internet de Línea Serie (Serial Line Internet Protocol, SLIP), es un protocolo de comunicación que soporta la transmisión de datagramas del protocolo Internet (Internet Protocol, IP), encapsulados dentro de sus tramas (frames). Opera sobre líneas telefónicas.

Mediante SLIP se puede establecer conexiones entre anfitriones (host), encaminadores y estaciones de trabajo a través de las líneas telefónicas de comunicación que permitan velocidades de hasta 19.2 kbits/seg soporta la transferencia síncrona o asíncrona a través de líneas dedicadas o de enlace telefónico y puede transmitir datagramas IP de hasta 1,006 bytes de longitud. En ambos extremos de la conexión SLIP se utiliza el mismo protocolo, y SLIP no dispone de ningún mecanismo de detección de errores puesto que estos mecanismos suelen estar en los niveles superiores del Protocolo de Control de Transmisión/Protocolo Internet (Transmission Control Protocol/Internet Protocol, TCP/IP). Debido a que SLIP trabaja sobre conexiones Punto a Punto en las que hay un solo sistema conectado en cada extremo, no es necesario utilizar direccionamiento o ninguna otra técnica de identificación. SLIP simplemente se limita a disponer los datos en tramas y transmitirlos.

3.5.2 PROTOCOLO PUNTO A PUNTO, (PPP)

Protocolo Punto a Punto, (Point-to-Point Protocol, PPP), es un protocolo de comunicación serie que opera sobre líneas de enlace telefónico o líneas dedicadas para proporcionar conexiones dentro de redes IP.

Establece y controla sesiones de encaminadores, host, estaciones de trabajo y tramas de datos transmitidos sobre la línea telefónica. PPP puede encapsular protocolos diferentes de nivel de red como IP, IPX, Apple Talk, etc; y el nivel MAC que busca conexiones punto a punto síncronas y asíncronas. PPP puede transformar un puerto serie de computadora en un adaptador de red, lo que significa que puede transmitir datagramas de la misma forma que un adaptador de red por la encapsulación del datagrama a través de transmisiones serie.

PPP proporciona un mecanismo para asignar una dirección IP automáticamente de tal manera que las computadoras remotas se puedan conectar a la red desde cualquier punto. SLIP también es adecuado para sistemas remotos fijos que tan solo transmitan por IP.

PPP también es útil para la conexión de redes de área local remotas para la formación de una Internet. No hay limitaciones de velocidad incorporadas en el protocolo, por lo que el equipo de conexión y las líneas de comunicación determinan las velocidades.

Aunque PPP es usado principalmente en líneas de enlace telefónico o alquiladas, el grupo de trabajo que lo ha definido trabaja en procedimientos para el uso de PPP sobre de redes X.25, Frame Relay y red digital de servicios integrados (Integrated Services Digital Network, ISDN). PPP da soporte a comunicaciones síncronas orientadas a bit o comunicaciones asíncronas orientadas a byte. A continuación se describirán en breve los requisitos de la interfaz física.

La trama PPP, como se representa en la figura 3.5.2.1 contiene información que identifica lo siguiente:

- *Delimitadores.* Marcan el principio y final de la trama.
- *Dirección.* Contiene la dirección destino.
- *Control.* Contiene el número de secuencia para asegurar un manejo apropiado.
- *Protocolo.* Identifica si la trama contiene IP, IPX, Apple Talk u otro.
- *Información.* Contiene los datos que pueden variar en longitud.
- *Secuencia de verificación de trama.* Calcula el código de paridad para la comprobación de errores.

Delimitador 1 byte	Dirección 1 byte	Control 1 byte	Protocolo 2 bytes	Información varios tamaños	Secuencia de verificación de trama 2 bytes	Delimitador 1 byte
-----------------------	---------------------	-------------------	----------------------	----------------------------------	--	-----------------------

Figura 3.5.2.1. Formato de trama del Protocolo Punto a Punto.

La pila de protocolos PPP se dibuja en la figura 3.5.2.2 y se describe a continuación:

Nivel físico. Define la transmisión sobre líneas asíncronas y síncronas mediante el uso de protocolos de comunicación serie como EIA-232-E, EIA-422, EIA-423, Además de V.24 y V.25 del CCITT.

Nivel de enlace de datos. Se basa en la estructura de la trama definida en el control de nivel de enlace de datos de alto nivel (High-Level Data-Link Control, HDLC). El Protocolo de control de enlace (Link Control Protocol, LCP) establece y gobierna los enlaces entre las estaciones conectadas. Especifica métodos de encapsulación de los tamaños de los paquetes y comprueba para asegurarse que los enlaces funcionan adecuadamente. Los paquetes LCP se usan para el establecimiento, el mantenimiento y la finalización de las conexiones.

Nivel de red. El nivel de red contiene un conjunto de protocolos denominados, Protocolos de Control de Red (Network Control Protocol, NCP), cada uno de ellos con su propio procedimiento de control.

Nivel de red	Protocolo de control de red NCP
Nivel de enlace de datos	Protocolo de control de enlace (LCP)
	HDLC
Nivel fisico	EIA-232-E, EIA-422, EIA-423, CCITT (ITU) V.24, CCITT (ITU) V.35

Figura 3.5.2.2. Pila de protocolos Punto a Punto.

3.6 NUEVAS TECNOLOGÍAS

3.6.1 ETHERNET RÁPIDA (FAST ETHERNET)

Ethernet rápida constituye la norma 100Base-X del IEEE, desarrollada originalmente por 3COM, Intel y otros fabricantes. Modifica la norma Ethernet existente en el sentido de admitir una velocidad de transmisión de 100 Mbits/seg, aunque sigue utilizando el método de acceso múltiple con detección de portadora y detección de colisiones (Carrier Sense Multiple Access/Collision Detection, CSMA/CD) sobre configuraciones jerárquicas de cableado de par trenzado de categoría 5, para aceptar una alta velocidad de transmisión de datos. La topología en estrella es similar a la Ethernet 10Base-T con todos los cables controlados por un concentrador. A continuación se mencionan algunos puntos característicos de Ethernet rápida:

- Los fabricantes producen tarjetas 100 Base-X que también trabajan con Ethernet a 10 Mbits/seg, con objeto de ayudar a los clientes a migrar a ésta nueva norma.
- 100 Base-X requiere cable de grado de datos de Categoría 5.
- La alta velocidad de Ethernet limita las distancias a 100 metros.
- 100 Base-X pueden utilizar cable de fibra óptica para trabajar a distancias mayores.

100Base-X se basa en el hecho de que CSMA/CD es escalable. Hay una versión de velocidad inferior a 1 Mbit/seg (IEEE 802.3 1Base-5) que proporciona mayores distancias de cable. 100Base-X aumenta la velocidad disminuyendo la distancia del cable. La red se extiende fácilmente adoptando una configuración jerárquica de cableado que interconecta los concentradores exteriores, según muestra la figura 3.6.1.1. Este tipo de cableado se adapta a las nuevas estrategias de cableado estructurado en base a la "Normativa de cableado para edificios comerciales EIA/TIA 568".

El principal objetivo en el desarrollo de 100Base-X fue preservar el estándar CSMA/CD, con el fin de acomodarse a las instalaciones ya existentes de Ethernet. 100Base-X se sitúa en el subnivel de acceso al medio (Medium Access Control, MAC) de IEEE, que permite establecer un puente entre distintas normas IEEE, como las relativas redes en anillo con testigo, la Interfaz de Datos Distribuidos por fibra óptica, (Fiber Distributed Data Interface, FDDI) y otras normas Ethernet. También permite un puente entre dos redes Ethernet, una a 10 Mbits/seg y otra red 100Base-X, únicamente tendría que realizar una equiparación de velocidades durante el intercambio de paquetes.

El tipo de cableado utilizado para proporcionar una transmisión a 100Mbits/seg es una consideración importante cuando se escoge un diseño Ethernet de alta velocidad. El cable de grado de datos de Categoría 3 instalado en numerosos edificios no es deseable en redes Ethernet a 100Mbits/seg de modo que, hay que realizar una nueva instalación de cableado para 100Base-X en base a la norma del Instituto americano de normalización (American National Standards Institute, ANSI) denominada X3T9.5 (FDDI) TP-PMD, que utiliza dos pares de cables de Categoría 5. Admite fibra óptica y cable de par trenzado blindado (STP) Tipo 1 de IBM.

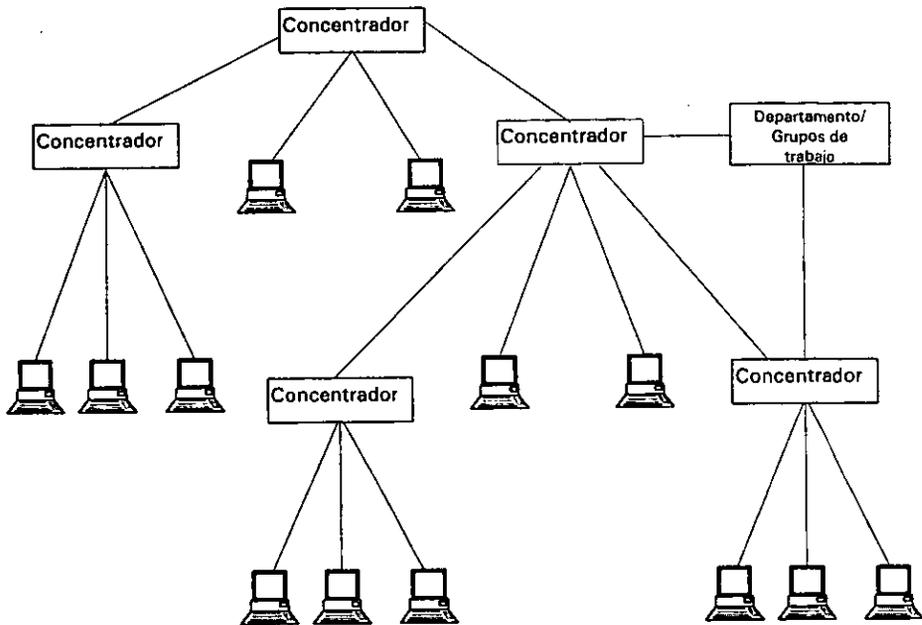


Figura 3.6.1.1. Red Ethernet 100Base-X.

3.6.2 ETHERNET 100VG-ANYLAN GRADO DE VOZ IEEE (802.12)

100VG-AnyLAN es una nueva tecnología IEEE 802.12. El 100 indica que la transmisión de datos se lleva a cabo a 100 Mbps, VG indica que maneja grado de voz (Voice Grade), Any indica que puede transmitir tramas de Ethernet y Token Ring a 100 Mbps en una Red de Área Local (LAN). Esta nueva norma es necesaria en aplicaciones multimedia, de imágenes o vídeo en tiempo real.

La propuesta 100VG-AnyLAN se basa en una tecnología desarrollada por AT&T y Hewlett Packard. Actualmente esta a cargo de la dirección del comité 802.12 del IEEE. La norma utiliza cable de par trenzado de cuatro pares de hilos. Utiliza un nuevo método denominado prioridad bajo demanda, sobre configuraciones jerárquicas de cableado de par trenzado, reemplaza el método de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) utilizado en las redes Ethernet existentes.

Especificaciones 100VG-AnyLAN

100VG-AnyLAN utiliza cuatro pares de grado de voz de Categoría 3 por estación. 100VG-AnyLAN puede aprovechar el cable de Categoría 5 si ya se encuentra instalado. Si es así las distancias de cable pueden aumentar de 100 a 150 metros.

El método de acceso original de Ethernet ha cambiado, pero la trama sigue siendo la misma. El nuevo método se denomina prioridad bajo demanda. Manteniendo el formato de trama original, puede mantenerse la compatibilidad entre normas Ethernet existentes y la norma 100VG-AnyLAN.

Debido a que 100VG-AnyLAN es similar a 10Base-T en cuanto a topología, los adaptadores y otros componentes comparten muchas de las mismas características. Una computadora conectada a 10Base-T ó 100VG-AnyLAN puede conectarse a un concentrador 100VG-AnyLAN y trabajar a la velocidad a que está diseñado. La topología en estrella y el sistema de cableado estructurado se mantienen, al igual que el formato de trama existente de Ethernet. Además se utilizan conectores 10Base-T.

Métodos de señalización

100VG-AnyLAN puede utilizar el mismo tipo de cable que las instalaciones existentes de 10Base-T. Puesto que este cable se clasifica como grado de voz, se requiere de cuatro pares de hilos para la señalización para asegurar una velocidad de 100 Mbits/seg sobre la línea.

Mientras que 10Base-T utiliza dos pares en el cable, uno para transmitir y el otro para recibir, 100VG-AnyLAN utiliza los cuatro pares.

El método de señalización por cuarteto utiliza las mismas frecuencias que 10Base-T, pero transmite señales a 25 MHz en cada uno de los pares del cable. Las frecuencias de señal más pequeñas de 100VG-AnyLAN, divididas a través de los hilos, mantienen las emisiones de radio frecuencia dentro de los requisitos que permiten el uso cable de grado de voz. En contraste, la norma 10Base-T transmite una señal de 20MHz dividida en dos pares.

Prioridad bajo demanda.

Es el nuevo método de acceso en 100VG-AnyLAN, que reemplaza el método CSMA/CD utilizado en otras normas de Ethernet. Con el método de prioridad bajo demanda, las estaciones de trabajo pueden recibir al mismo tiempo que transmiten. Esto es posible gracias al uso de los cuatro pares del cable de par trenzado y al cuarteto de señalización.

La prioridad bajo demanda aprovecha el diseño estructurado del cableado y el esquema centrado en un concentrador, como se representa en la figura 3.6.2.1. Este diseño es similar al esquema de Ethernet 10Base-T, sin embargo el concentrador realiza un mayor control de gestión del acceso a la red, arbitra qué estaciones de trabajo acceden a la red dependiendo de la prioridad del tráfico. Cuando una estación de trabajo necesita transmitir, envía una petición al concentrador, acompañada de un nivel de prioridad. Si la red no está ocupada, la estación de trabajo puede comenzar la transmisión. Todas las transmisiones se realizan a través del concentrador, que ofrece un sistema de conmutación rápida al nodo destino.

El mecanismo de prioridad asegura que ciertos tipos de tráfico, como vídeo, que es sensible al tiempo, obtienen más prioridad que otros tipos de tráfico. Si llegan al concentrador muchas peticiones de transmisión, se atenderá la más prioritaria. Si dos estaciones realizan una petición de transmisión de igual prioridad, se atienden simultáneamente, alternándose al servicio entre ambas, de esta manera se elimina el fenómeno de contención. CSMA/CD es inferior al método de "prioridad bajo demanda" debido a que en CSMA/CD las estaciones de trabajo compiten para obtener acceso al cable por sí solas sin estar dirigidas por un concentrador. El fenómeno de contención sucede cuando dos o más estaciones de trabajo intentan acceder al mismo tiempo. Las estaciones de trabajo realizan un nuevo intento tras un intervalo aleatorio de tiempo. Este sistema reduce las prestaciones y origina de nuevo contención debido a que las estaciones de trabajo tienen que volver a competir para acceder una vez más al cable.

Una ventaja más del método de prioridad por demanda es que las transmisiones enviadas a través del concentrador no alcanzan otras estaciones, como Ethernet estándar, lo que permite reducir la probabilidad de que el contenido de una transmisión pueda ser observado por alguien no autorizado, asegurándose una mayor privacidad.

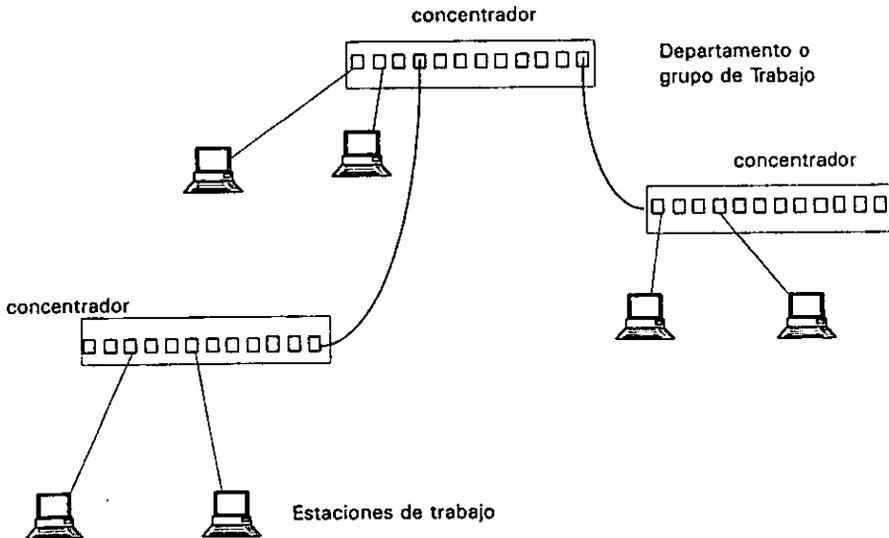


Figura 3.6.2.1. Ejemplo de cableado estructurado Ethernet 100VG-AnyLAN.

3.6.3 GIGABIT ETHERNET (IEEE 802.3z)

En julio de 1996 se creó el grupo 802.3z del IEEE, para establecer una norma que regiría el estándar Gigabit Ethernet. Sus principales objetivos fueron:

- Desarrollar tareas pesadas.
- Ofrecer un ancho de banda de 1000 Mbps.
- Permitir trabajar transmisiones de datos en half y full- duplex a velocidades a 1000 Mbps.
- Usar el formato de trama del estándar IEEE 802.3, para mantener la plena compatibilidad con la gran base de nodos Ethernet ya instalados..
- Usar el método de CSMA/CD.
- Proporcionar compatibilidad de direccionamiento con las tecnologías de 10BASE-T y 100BASE-T.

Las tareas pesadas identifican tres objetivos para hacer enlaces a distancia:

- Enlace con fibra óptica multimodo con una máxima longitud de 550m.
- Enlace con fibra óptica monomodo con una máxima longitud de 3 Km.
- Enlaces con cable coaxial con una máxima longitud menor a los 25m.

Los componentes para una red Gigabit Ethernet son: conmutadores o switches, enrutadores Gigabit Ethernet, concentradores, servidores, estaciones de trabajo, NIC's.

Así que Ethernet, ahora es escalable de 10 a 100 y a 1000 Mbps, puede ser desarrollado en el Backbone para una conexión de alta velocidad a grupos de servidores, grupos de trabajo robustos, o simplemente clientes de estaciones de trabajo.

3.6.4 FRAME RELAY.

Frame Relay (Paso de tramas) constituye un método de comunicación orientado a paquetes para la conexión de sistemas informáticos. Se originó a partir de las interfaces ISDN y se propuso como estándar al Comité Consultivo Internacional para la Telegrafía y Telefonía (Consultive Committee for International Telegraph and Telephone, CCITT) en 1984. Sus principales objetivos son:

Interconecta redes LAN y redes WAN sobre de redes públicas o privadas de conmutación de paquetes, situando la trama procedente las LAN/WAN en una trama Frame Relay y distribuyéndola a través de la capa de la red (la mezcla de conexiones Frame Relay) hacia el destino. Ofrece enlaces de conexiones virtuales. Ofrece una interfaz de usuario dentro de una red de conmutación de paquetes de área extensa que típicamente ofrece un ancho de banda comprendida entre 56 kbits/seg y 1.544 Mbits/seg. Utiliza la conmutación mejorada de paquetes. Las conexiones a ésta red requieren de un encaminador y una línea desde las instalaciones del cliente hasta el puerto de entrada a Frame Relay para tener conexiones punto a punto, esta línea consiste a menudo en una línea digital equilibrada como T1 aunque esto depende del tráfico. Utiliza un parámetro llamado Tasa de Información Asegurada (Committed Information Rate, CIR) la cual se utiliza para facturar las conexiones a redes públicas. Este valor se basa en la naturaleza aleatoria de la transmisión de datos, ya que no todas las estaciones transmiten al mismo tiempo, con lo cual, la suma de la capacidad, en bits/seg, de los

canales de cada una de ellas, puede ser superior a la capacidad de los canales de interconexión. Cada estación va transmitir toda la información que permita el canal, pero, en caso de que la red se congestione, sólo podrá transmitir, en principio, la cantidad permitida por el CIR. Frame Relay no es deseable para tráfico de voz y video debido a que la longitud de sus tramas es variable. La figura 3.6.4.1 ilustra dos posibles métodos de conexión en área extensa, como se describe a continuación:

- *Método de red privada.* En este método, cada instalación necesita tres líneas dedicadas (alquiladas) y encaminadores asociados, para conectarse con cualquiera de los otros lugares, a través de un total de seis líneas dedicadas y 12 encaminadores.
- *Método de red pública (Frame Relay).* En este método de red pública, cada instalación requiere una línea dedicada y un encaminador asociado dentro de la red de Frame Relay. Los paquetes recibidos de múltiples usuarios son multiplexan sobre la línea y se envían a través de la red Frame Relay a sus destinos.

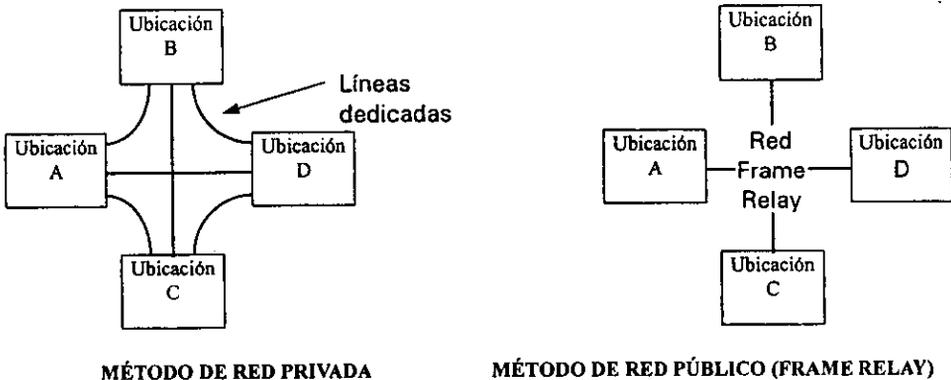


Figura 3.6.4.1. Red Frame Relay comparada con una red con líneas dedicadas.

Conmutación mejorada de paquetes

Durante los últimos años, las compañías de telecomunicaciones han instalado una gran cantidad de cables de fibra óptica en todo el mundo con el fin de aumentar el ancho de banda disponible y enviar información a través de muchos enlaces de red, evitando así el control de flujo y la gestión de errores dentro de la propia red y los originadores de retardos. Gracias a que esta técnica de conmutación solo utiliza el ancho de banda únicamente cuando se transmiten datos. Frame Relay asume que los nodos finales son máquinas programables que puede realizar su propia gestión de errores. Si se produce la corrupción o pérdida de un paquete debido a la congestión en una red Frame Relay, el sistema receptor detectará la pérdida de la trama y solicitará una retransmisión.

Establecimiento de conexiones FRAME RELAY

Hay que seleccionar la velocidad de acceso y el tipo de acceso (dedicado o conmutado), según se describe a continuación:

- Acceso conmutado a 56/64 Kbits/seg, proporcionado por un servicio de la Red digital de servicios integrados ISDN. El avance dedicado lo proporciona Advanced Digital Network (ADN).
- Acceso a 128 Kbits/seg proporcionado por dos líneas ISDN o ADN.
- Conexión desde 384 Kbits/seg hasta 1.544 Mbits/seg. Disponible a través de líneas T1 o línea fraccionales T1.

Fraccional T1 y Fraccional T3

Una línea Fraccional T1 consiste en un subcanal de una línea T1 completa, puesta a la venta por compañías telefónicas; existen 24 líneas fraccionales T1 en una línea completa, y cada una de ellas tiene un ancho de banda de 64 Kbits/seg. Existen 28 canales T1 en una línea T3. Los usuarios pueden adquirir una o más líneas fraccionales sin la necesidad de adquirir la línea completa, con la posibilidad de añadir más líneas fraccionales en cualquier momento.

Un canal de acceso de un cliente a una red de una compañía de telecomunicaciones se encuentra determinado por la velocidad de acceso. Un canal de línea T1 puede denotar a cualquiera de los siguientes:

- T1 canalizado, en el que un canal es cualquiera de los 24 intervalos temporales T1.
- T1 no canalizado, en el que los 24 intervalos temporales T1 se consideran como un canal.
- T1 Fraccional, en el que un canal es un grupo de 1 a 123 intervalos temporales.

Una vez aprobado el servicio, se planea un enlace hasta el proveedor del servicio Frame Relay. Los encaminadores y dispositivos de acceso a Frame Relay se utilizan para establecer una conexión al puerto proveedor de Frame Relay. Como se muestra en la Figura 3.6.4.2.

Algunas utilidades que proporcionan fabricantes de Frame Relay se mencionan a continuación:

Servicios de red. Las siguientes utilidades y servicios de gestión se encuentran disponibles en redes Frame Relay:

- *Mensajes de estado de los circuitos virtuales.* Este servicio proporciona la comunicación entre la red y el cliente. Asegura que el PVC existe e informa sobre los PVC's eliminados.
- *Multidistribución.* Este servicio opcional permite a un usuario enviar tramas a múltiples destinos.
- *Direccionamiento global.* Este servicio opcional concede a una red Frame Relay capacidades semejantes a las de una LAN.

- *Control simple de flujo.* Este servicio opcional proporciona el mecanismo de control de flujo.

Los puertos de Frame Relay se conectan normalmente mediante enlaces lógicos (PVC, Permanent Virtual Circuit) que proporcionan conexiones rápidas entre los puntos finales predefinidos.

Control de congestión. Cuando una red Frame Relay alcanza la congestión, las tramas pueden descartarse arbitrariamente (los nodos finales son los responsables de la retransmisión de las mismas), o bien el rechazo se efectúa según las preferencias del cliente. Por ejemplo, los clientes pueden asignar el tráfico normalmente no crítico en las operaciones de la empresa en el atributo de descarte DE (discard-elegible). Las tramas se marcan con DE mediante un encaminador o conmutador Frame Relay. El uso de DE proporciona una forma de asegurar que la información más importante viaja a través de la red y la menos importante se retransmite cuando la red no se encuentra ocupada.

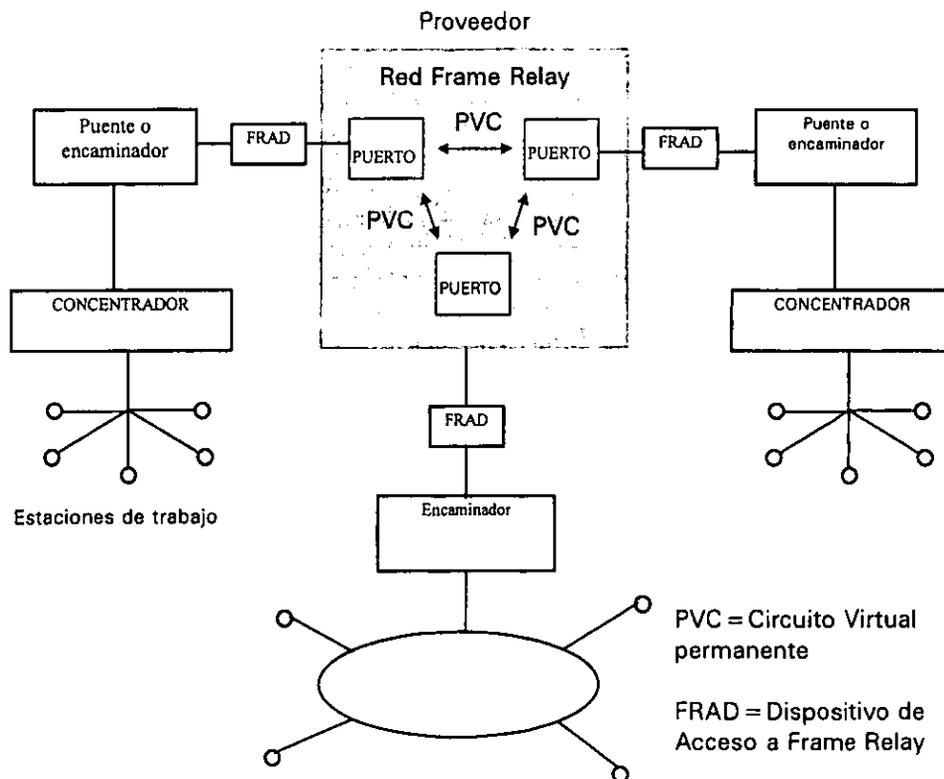


Figura 3.6.4.2. Una típica conexión de Frame Relay.

Seguridad. Existen numerosas opciones de seguridad en Frame Relay:

- Únicamente líneas privadas pueden acceder a la red.
- Se necesitan contraseñas para acceder a la red.
- Una utilidad de exceso de tiempo desconecta estaciones inactivas.

Estructura de trama FRAME RELAY

La estructura de trama de un paquete de Frame Relay se muestra en la figura 3.6.4.3. Los campos indicadores situados a cada extremo delimitan la trama mediante una secuencia de bits, siguiendo al campo inicial se encuentra el encabezamiento Frame Relay, que mantiene la información sobre direcciones y control de congestión. Se sigue por la información y la secuencia de verificación de trama (Frame Check Sequence, FSC). Se realiza un cálculo con cada trama recibida y se compara con el campo FSC, que calculó el emisor. El paquete se elimina si no hay coincidencia y las estaciones finales deben de solucionar su pérdida. Esta verificación de errores se realiza únicamente en los conmutadores. El encabezamiento contiene la siguiente información:

- *Identificador de conexión de enlace de datos (Data Link Connection Identifier, DLCI).* Esta información contiene el número de identificación de la conexión lógica multiplexada dentro del canal.
- *Capacidad de elección de descarte (Discard Eligibility, DE).* Esta información establece las prioridades que indican si una trama puede descartarse al presentarse congestión.
- *Notificación de congestión explícita hacia delante (Forward Explicit Congestion Notification, FECN).* Informa al encaminador que recibe la trama que se ha experimentado congestión en el trayecto que ha atravesado ésta.
- *Notificación de congestión explícita hacia atrás (Backward Explicit Congestion Notification, BECN).* Esta información se añade a las tramas que viajan en sentido contrario a las tramas que encontraron congestión. Esta información se ha diseñado para ayudar a los protocolos de alto nivel ha emprender la acción adecuada respecto al control de flujo.

Indicador	Encabezamiento	Información	FSC	Indicador
-----------	----------------	-------------	-----	-----------

Figura 3.6.4.3. Estructura de la trama Frame Relay.

FRAME RELAY FORUM

Frame Relay Forum es una asociación de usuarios y fabricantes de Frame Relay, con base en Mountain View, California (415/962-2579). Se compone de comités que crean acuerdos de realización con el propósito de desarrollar normas basadas en Frame Relay. Los acuerdos se crean mediante información y sugerencias de los miembros de la comunidad. El FORUM dispone de material técnico e información marketing sobre Frame Relay.

3.6.5 MODO DE TRANSFERENCIA ASÍNCRONA (ATM)

La tecnología llamada Modo de Transferencia Asíncrona (Asynchronous Transfer Mode, ATM), ha sido definida tanto por el Instituto Americano de Normalización (American National Standards Institute, ANSI); como por el Comité Consultivo Internacional para la telefonía y la telegrafía (Consultive Committee for International Telegraph and Telephone, CCITT). Se puede definir como una tecnología de conmutación de celdas (paquetes de información de longitud fija de 53 bytes de alta velocidad). ATM provee un ancho de banda dedicado para la conexión, haciéndola ideal para aquellas aplicaciones en tiempo crítico como voz y vídeo; mantiene la compatibilidad con las redes de datos actuales; garantiza el ancho de banda cuando sea necesario; es una tecnología capaz de integrar en ambientes: local, campus y de área amplia.

ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización. Una vez establecida la conexión, las celdas de ATM incluyen información que permite identificar la conexión a la cual pertenecen. En una red ATM las comunicaciones se establecen a través de un conjunto de dispositivos intermedios llamados switches.

Un switch típico soporta la conexión de entre 16 y 32 nodos. Para permitir la comunicación de datos a alta velocidad, la conexión entre los nodos y el switch se realizan por medio de un par de hilos de fibra óptica.

Aunque un switch ATM tiene una capacidad limitada, múltiples switches pueden interconectarse entre sí para formar una gran red. En particular, para conectar nodos que se encuentran en dos sitios diferentes es necesario contar con un switch en cada uno de ellos y ambos a su vez deben estar conectados entre sí.

El tamaño fijo de celda ofrece diferentes ventajas:

Son menos complejas y más fácil de manejar, lo que permiten que sean procesadas por hardware a mayor velocidad.

Permiten el procesamiento en paralelo, por lo que mejora notablemente su velocidad en comparación con la arquitectura tipo bus.

Los retardos son predecibles, por lo que permite establecer el control de tráfico y de colas para un mejor manejo de congestión.

Las conexiones entre nodos ATM se realizan en base a dos interfaces diferentes. Una es la User to Network Interface o UNI, se emplea para vincular a un nodo final con un switch (SW). Y otra es la Network to Network Interface o NNI, define la comunicación entre dos switches.

UNI es como la interfaz para conectar equipos del cliente a la red del proveedor y NNI es la interfaz para conectar redes de diferentes proveedores.

Tipos de conexiones

ATM provee servicios orientados a la conexión. Para comunicarse con un nodo remoto, un host debe solicitar a su switch local, el establecimiento de una conexión con el nodo destino. Estas conexiones pueden ser de dos naturalezas: Switched Virtual Circuits (SVC) o Permanent Virtual Circuits (PVC).

Switched Virtual Circuits (SVC)

Un SVC opera del mismo modo que una llamada telefónica convencional. Un host se comunica con el switch ATM local y solicita el establecimiento de un SVC. El host especifica la dirección completa del nodo destino y la calidad del servicio requerido. Luego espera que la red ATM establezca el circuito.

El sistema de señalización de ATM se encarga de encontrar el path o trayectoria necesaria desde el host origen al host destino a lo largo de varios switches. El host remoto debe aceptar el establecimiento de la conexión.

Durante el proceso de señalización (toma este nombre por analogía con el usado en sistemas telefónicos de los cuales deriva ATM) cada uno de los switches examina el tipo de servicio solicitado por el host de origen. Si acuerda propagar información de dicho host, registra información acerca del circuito solicitado y propaga el requerimiento al siguiente switch de la red. Cuando el proceso de señalización concluye, el switch local reporta la existencia del SVC al host local y al host remoto.

La interfaz UNI identifica a cada uno de los SVC por medio de un número de 24 bits. Cuando un host acepta un nuevo SVC, el switch ATM local asigna al mismo, un nuevo identificador. Los paquetes transmitidos por la red no llevan información de nodo origen; ni de nodo destino. El host marca a cada paquete enviado con el identificador de circuito virtual necesario para llegar al nodo destino.

Permanent Virtual Circuits (PVC)

La alternativa al mecanismo de SVC descrito anteriormente es el PVC. El administrador de la red puede configurar en forma manual los switches para definir circuitos permanentes. El administrador identifica el nodo origen, el nodo destino, la calidad de servicio y los identificadores de 24 bits para que cada host pueda acceder al circuito.

Paths, Circuitos e Identificadores

ATM asigna un entero único como identificador para cada path abierto por un host. El identificador solo es válido mientras que el circuito permanece abierto; además solamente es válido para un solo sentido del circuito. Esto quiere decir que los identificadores de circuito obtenidos por los dos hosts en los extremos del mismo, usualmente son diferentes.

Los identificadores SVC usados por la interfase UNI están formados por 24 bits, divididos en dos campos, el primero de 8 bits y el segundo de 16 bits. Los primeros 8 bits forman el llamado (Virtual Path Identifier, VPI) y los 16 restantes, el (Virtual Circuit Identifier, VCI). El primer campo identifica la red y el segundo campo identifica el host. Este conjunto de bits suele recibir el nombre de (par VPI/VCI).

Si un conjunto de circuitos virtuales (VC's) sigue el mismo camino (path) el administrador puede asignar a todos ellos un mismo VPI. El hardware de ATM usa entonces, los VPI para funciones de ruteo de tráfico.

Celda de transporte ATM

Cada celda de ATM tiene una longitud de 53 bytes, reservándose los 5 primeros para el encabezado y el resto (48) para datos.

EL encabezado contiene información, que permite establecer conexiones punto a punto, control de congestión, administración de tráfico y además del chequeo de errores.

Dentro del encabezado se coloca el par VPI/VCI que identifica al circuito entre extremos, dentro de esos campos de control, incluyen tanto el enrutamiento de celdas como el tipo de conexión. Además da información de control de flujo y un Control de redundancia cíclica (Cyclical redundancy Checksum, CRC).

La organización de la cabecera (header) variará levemente dependiendo de si la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local; ya que pueden ser cambiados de interfase a interfase.

La conexión final entre dos nodos recibe el nombre de Virtual Channel Connection o VCC. Una VCC se encuentra formada por un conjunto de pares VPI/VCI. La figura 3.6.5.1 muestra un ejemplo de una red ATM, en la cual hay dos PC's conectadas a través UNI, NNI y varios switches; los cuales forman un VCC.

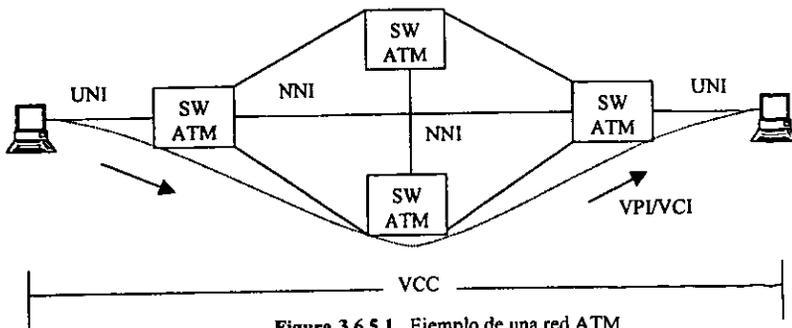


Figura 3.6.5.1. Ejemplo de una red ATM.

Modelo de capas de ATM

Capa Física

Define la forma en que las celdas se transportan por la red.

Es independiente de los medios físicos.

Tiene dos subcapas:

-TC (Transmission Convergence). Se encarga del control de errores y lineamiento de celdas.

-PM (Physical Medium). Depende del medio físico y se encarga de la transmisión de los bits, alineamiento y señalización en línea, así como también de las señales electro-ópticas.

Capa ATM

Provee un solo mecanismo de transporte para múltiples opciones de servicio.

Es independiente del tipo de información que es transmitida (datos, gráficos, voz audio, vídeo) con excepción del tipo de servicio requerido.

Tipos de encabezado (header) ATM

UNI (User-Network Interface).

NNI (Network to Network Interface).

Capa de adaptación ATM (ATM Adaptation Layer)

Permite a la Capa ATM transportar diferentes protocolos y servicios de capas superiores.

Tiene dos subcapas:

-CS (Convergence).

-SAR (Segmentation and Reassembly).

Si bien ATM se maneja con celdas a nivel de capas inferiores, las aplicaciones que generan la información a ser transportada por ATM no trabajan con celdas. Estas aplicaciones interactuarán con ATM por medio de una capa llamada (ATM Adaptation Layer). Esta capa realiza una serie de funciones entre las que se incluyen detección de errores (celdas corruptas).

En el momento de establecer la conexión el host debe especificar el protocolo de capa de adaptación que va a usar. Ambos extremos de la conexión deben acordar en el uso del mismo protocolo y este no puede ser modificado durante la vida de la conexión.

Hasta el momento solo se han definido dos protocolos de la capa de adaptación para ser usados por ATM. Uno de ellos se encuentra orientado a la transmisión de información de audio y vídeo, y el otro para la transmisión de datos tradicionales.

ATM Adaptation Layer 1 (AAL1). Transmite información a una tasa de bits fija. Las conexiones creadas para trabajar con vídeo deben usar AAL1 dado que requieren un servicio de tasa constante para no tener errores de parpadeo en la imagen.

La transmisión de datos tradicionales trabaja con la AAL5. Envía paquetes de un nodo a otro. Ahora, si bien ATM trabaja con tramas o celdas de tamaño fijo. Los protocolos de capa superior generalmente manejan datagramas de longitud variable. Una de las funciones de la AAL5 consiste en adaptar estas tramas a celdas. En particular la AAL5 puede recibir datagramas de hasta 64 kbytes de longitud.

Cada una de las tramas de AAL5 deben ser fraccionadas en celdas para poder ser transportadas por la red para luego ser recombinadas en el nodo remoto. Cuando el datagrama es un múltiplo de 48 bytes el resultado de la división da un número entero de celdas. En caso contrario la última de las celdas no se encontrará completa.

Para poder manejar paquetes de longitud arbitraria, AAL5 permite que la celda final pueda contener entre 0 y 40 bytes de datos y coloca la información de control al final de la misma antecedida por los ceros de relleno necesarios. En otras palabras, la información de control (8 bytes) se coloca al final de la secuencia de celdas donde puede ser encontrada y extraída sin necesidad de conocer la longitud del datagrama fraccionado.

Convergencia (CS), Segmentación y Reensamblado (SAR)

Cuando una aplicación envía datos sobre una conexión ATM usando AAL5, el host pasa los datos a la interfase AAL5. Esta divide los datos en celdas, genera el trailer y transfiere a cada una de ellas a través de la red ATM. En el nodo receptor AAL5 recibe las celdas y las reensambla en base a la información contenida en el «trailer» para regenerar el datagrama original.

El nodo origen usa el byte menos significativo del campo de datos de la celda, para indicar la celda final de un datagrama.

En ATM el término convergencia se usa para identificar el método usado para detectar el final de cada datagrama fraccionado.

Una de las fortalezas de ATM, es que, se paga solamente por la carga de celdas que es efectivamente transportada y conmutada para el usuario.

En varios aspectos, ATM es el mejor servicio de voz, vídeo por un lado y datos por otro, de manera eficiente, usando una simple tecnología de conmutación y multiplexación de celdas.

ATM combina la simplicidad de la multiplexación por división en el tiempo (Time Division Multiplexing, TDM) encontrado en la conmutación de circuitos, con la eficiencia de las redes de conmutación de paquetes con multiplexación estadística.

Básicamente, ATM es la tecnología que administra el ancho de banda asignado a cada una de las señales que circulan por la red, sean éstas voz, datos o imágenes, de manera que el usuario final la reciba en forma integrada.

La tecnología ATM comprende un tendido físico (cable de cobre, cable coaxial, enlace de microondas, enlace mediante satélite o cable de fibra óptica), elementos de conmutación (switch), dispositivos de adaptación (routers, etc.), y dispositivos de interfaz (tarjetas de comunicación, cámaras de vídeo, centrales telefónicas, etc).

El modo más usual de acceso a ATM es la fibra óptica, la cual es un cable de silicio del grosor de un cabello humano, a través del cual viaja un rayo láser de alta densidad o un haz infrarrojo, el que transmite bits (ceros o unos) mediante una codificación digital.

Para transmitir datos o señales de audio o vídeo sobre un cable de fibra óptica, es necesario digitalizar previamente la señal. De eso se encarga un procesador situado en el interior del dispositivo de tarjeta de interfaz, sea una cámara de vídeo, una central telefónica, etc.

ATM promete ser la tecnología de red empresarial virtual del futuro, un término que refleja tanto la evolución del modelo empresarial global y el énfasis en la conectividad lógica, donde los usuarios obtienen acceso a los recursos que necesitan y el administrador de la red provee las rutas de conexión y asigna el ancho de banda necesario a fuentes de tráfico muy diferentes (voz, datos y vídeo). Aquellos que construyen y operan redes deben volver los ojos a las capacidades de la tecnología ATM, ya que aspiran a la interconectividad global, escalabilidad de tecnologías y satisfacción del usuario.

CAPÍTULO IV PROTOSCOLOS

4.1 CONTROL DE ENLACE DE DATOS DE ALTO NIVEL (HDLC)

Control de Enlace de Datos de Alto Nivel (High Level Data Link Control, HDLC) es un protocolo orientado a bit, lo que significa que se realiza la supervisión de los datos bit a bit. No tiene códigos especiales de control, sin embargo, la información de la trama contiene ordenes de control y de respuesta. HDLC da soporte a transmisión (full-duplex), donde los datos se transmiten simultáneamente en dos direcciones, lo que proporciona un mayor rendimiento.

HDLC es deseable para las conexiones punto a punto o multipunto. Esta especificación de red es utilizada principalmente en las transmisiones por líneas telefónicas para comunicaciones de datos, y las redes públicas de conmutación de paquetes.

Los subconjuntos de HDLC se utilizan para proporcionar señalización y enlaces de control de datos para redes X.25, ISDN (Integrated Services Digital Network) y Frame Relay.

Cuando se establece una sesión HDLC, una estación denominada *estación primaria* queda designada para gestionar el flujo de datos. La otra estación (o estaciones) quedan designadas como estaciones *secundarias*. La estación primaria utiliza órdenes y las secundarias respuestas. Existen tres posibles métodos de conexión, como se ilustra en la Figura 4.1.1. Los dos modos superiores aceptan conexiones *punto a punto* entre dos sistemas, o conexiones *multipunto*. Entre una estación primaria y dos o más estaciones secundarias.

- El modo normal es no equilibrado, debido a que la estación secundaria puede transmitir únicamente cuando se lo permita la estación primaria.
- El modo asíncrono también es no equilibrado, pero la estación secundaria puede iniciar una transmisión por sí misma.
- El modo asíncrono equilibrado está diseñado para conexiones punto a punto entre dos computadoras sobre una línea dúplex. Cada estación puede enviar órdenes y respuestas sobre su propia línea y recibir ordenes y respuestas sobre la línea dúplex. Este es el modo utilizado para conectar estaciones a redes de conmutación de paquetes X.25.

Una sesión de comunicación comienza con el establecimiento de conexiones entre estaciones primarias y secundarias. La estación primaria transmite una trama especial a una única estación o múltiples estaciones, para iniciar un procedimiento de configuración. Las estaciones secundarias responden con la información utilizada para el control de errores y de flujo durante la sesión. Una vez que se ha realizado la configuración, comienza la transmisión de datos, y al finalizar ésta, la estación primaria envía una trama para iniciar la desconexión de la sesión.

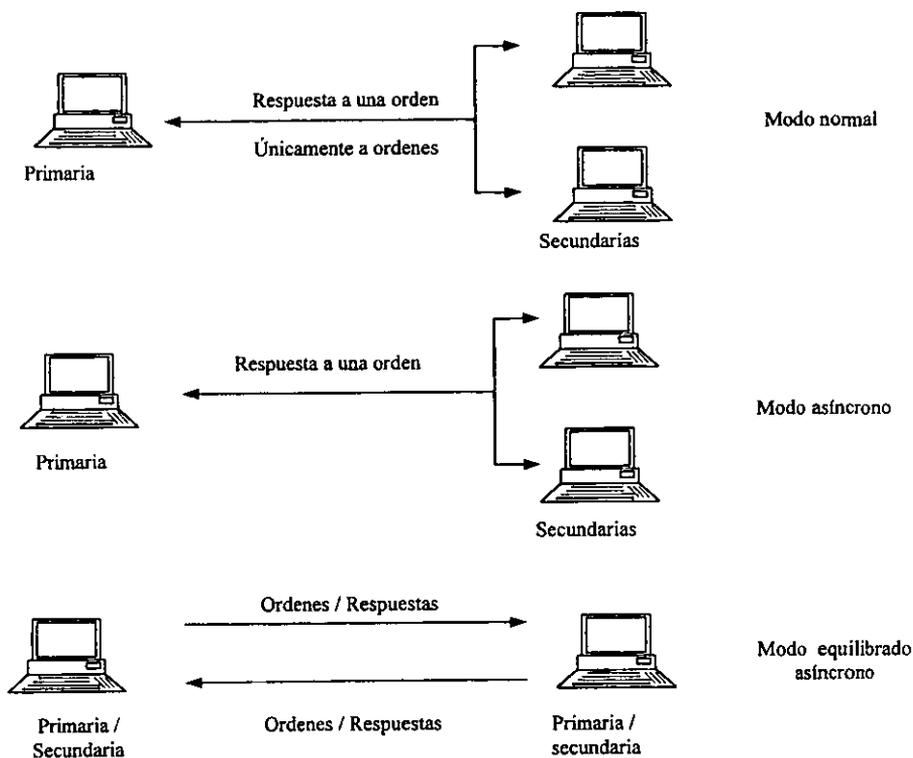


Figura 4.1.1. Métodos de Conexión HDLC.

La trama HDLC define la estructura de envío de mensajes de datos, de órdenes y respuestas entre los sistemas de comunicación. La trama HDLC se muestra en la Figura. 4.1.2.

- El campo de *marca* contiene la secuencia de bits 01111110, que indica el comienzo y final de la trama, si cualquier porción de los datos de la trama contiene más de cinco bits consecutivos con el valor 1, se utiliza una técnica de *inserción de un bit a 0* para asegurar que no se produce un error de delimitación.
- El campo de *dirección* generalmente contiene la dirección de la estación secundaria. Este campo contiene generalmente 8 bits, aunque es posible el direccionamiento extendido para conexiones multipunto, que necesitan muchas direcciones diferentes. Puede insertarse en este campo una dirección especial que permite enviar los mensajes a todas las estaciones en una conexión multipunto.
- El campo de *control* identifica la información contenida en la trama. Las ordenes las envía la estación primaria, y las respuestas la secundaria. La información de control puede

reconocer tramas, solicitar la retransmisión de una trama o una suspensión de la transmisión, así como otras ordenes y respuestas.

- El campo de *información* contiene los datos, ordenes o respuestas.
- El campo *FCS* lleva a cabo la secuencia de verificación de trama, el cual contiene información de control de errores para asegurar al receptor la integridad de la trama.

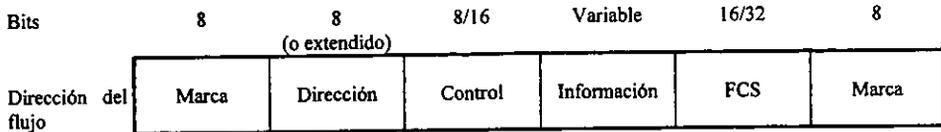


Figura 4.1.2. Definición de la trama HDLC.

4.2 CONTROL DE ACCESO AL MEDIO (MAC)

El protocolo Control de Acceso al Medio (Medium Access Control, MAC); opera en el nivel de enlace de datos del modelo de referencia OSI. Su tarea principal consiste en transportar paquetes de un nodo a otro en un segmento de la red. Se han definido varios protocolos MAC, muchos de los cuales pueden utilizarse con NetWare. Los Protocolos MAC más corrientes que se utilizan actualmente son:

- IEEE 802.5 (Token Ring)
- IEEE 802.3 (Ethernet)
- ARCNET

Los protocolos MAC definen el direccionamiento que identifica cada nodo en un segmento de red. El direccionamiento de nodo se amplía con el hardware de cada placa de la interfaz de la red. En el caso de las placas Ethernet, Token Ring y FDDI, las direcciones físicas se asignan en la fábrica. Es el IEEE quien administra las direcciones físicas para asegurarse de que dos fabricantes no utilizan las mismas.

Algunas direcciones físicas se asignan ajustando jumpers o conmutadores en la placa o mediante el software de configuración; éste es el caso de las placas ARCNET.

Los protocolos MAC también proporcionan comprobación de error a nivel de bit en forma de CRC (prueba de redundancia cíclica). La CRC se añade al final de cada paquete transmitido, también denominado final MAC. La CRC comprueba que ninguno de los paquetes recibidos esté corrupto.

Para recibir un paquete en el nodo de destino, los protocolos MAC colocan las direcciones de nodo y otra información en una cabecera MAC al principio de los paquetes que se han de enviar y la CRC en el final MAC.

Cabecera MAC

La cabecera MAC que se muestra en la figura 4.2.1 contiene los campos de dirección de nodos de origen y destino. Estos campos contienen las direcciones físicas que indican dónde se ha originado el paquete y cuál es su destino. La red comprueba el campo de Dirección de destino en la cabecera MAC de cada uno de los paquetes que recibe. Si la placa encuentra su propia dirección en este campo o si se trata de un paquete de difusión (constituido para todos los campos), la placa copia el paquete. A continuación el paquete pasa a un proceso de un nivel superior como IPX para que se examine y procese con más detalle.

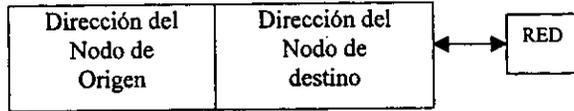


Figura 4.2.1. Cabecera MAC.

Las direcciones de destino y origen MAC son las mismas que los campos Nodo de destino y Nodo de origen en la cabecera IPX.

La cabecera y el final MAC encapsulan cada paquete con las direcciones de nodo, el protocolo de nivel superior, el CRC, la duración del mensaje e información adicional específica para el medio de la red, como se muestra en la figura 4.2.2. Esta información se especifica en un formato que se ajusta a un tipo de trama concreto.

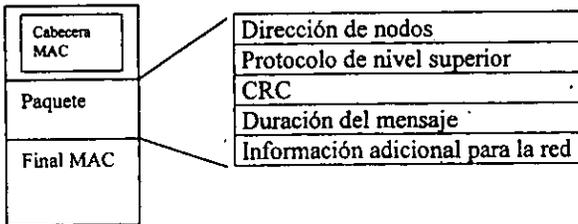


Figura 4.2.2. Paquete encapsulado.

Una trama es la unidad de datos que se utiliza para la comunicación entre dos nodos en una red. La cabecera de la trama MAC contiene información que especifica los nodos de envío y entrega.

Se pueden configurar varios tipos de tramas en el mismo enrutador o la misma estación de trabajo de NetWare. De todos modos, para que se comuniquen dos nodos en una red deben tener al menos un tipo de trama en común. Si un nodo sólo acepta tramas ETHERNET_802.3 y el otro sólo acepta tramas ETHERNET_802.2, los nodos no pueden comunicarse

directamente, aunque compartan la misma red física. Además, el uso de más de un tipo de trama en un nodo no incrementa el rendimiento.

4.3 INTERCAMBIO DE PAQUETES ENTRE REDES (IPX)

Intercambio de Paquetes Entre Redes (Internetwork Packet Exchange, IPX), es un protocolo de datagramas sin conexión. Sin conexión significa que cuando un proceso que está ejecutando un nodo particular, utiliza IPX para comunicar con un proceso en otro nodo, no se establece ninguna conexión entre los dos nodos. Por lo tanto, los paquetes IPX que contienen datos se direccionan y envían a sus destinos pero no se garantiza ni verifica que el paquete haya llegado efectivamente. Cualquier reconocimiento de paquete o control de conexión, los proporcionan los protocolos sobre IPX, tales como el SPX.

Datagrama significa que cada paquete se trata como una entidad individual, sin ninguna relación lógica o secuencial con ningún otro paquete.

IPX opera al nivel de red OSI. Del mismo modo que un protocolo de nivel de red, IPX direcciona y encamina paquetes desde una ubicación a otra de una red IPX, este basa sus decisiones de encaminamiento en los campos de dirección en su cabecera y en la información que recibe desde RIP y NLSP. IPX utiliza esta información para reenviar paquetes al nodo de destino o al siguiente enrutador, proporcionando una vía de acceso al nodo de destino.

Estructura del paquete IPX

El paquete IPX consta de dos partes:

- *Cabecera IPX de 30 bytes*: Incluye las direcciones de red, nodo y zócalo tanto para el destino como para el origen.
- *Datos*: Incluye la cabecera de un protocolo de un nivel superior, tal como el SPX.

El tamaño mínimo de un paquete IPX excluyendo la cabecera MAC es de 30 bytes (solamente cabecera IPX), tradicionalmente el tamaño máximo de los paquetes IPX encaminados era de 576 bytes (cabecera IPX y datos). Hasta hace poco, todos los paquetes IPX encaminados oscilaban entre 30 y 576 bytes. Sin embargo, el protocolo IPX siempre ha aceptado paquetes de un tamaño de hasta 65,535 bytes.

Las restricciones de los medios normalmente limitan el tamaño máximo del paquete permitido a algo menos de 65,535 bytes. Los paquetes Ethernet II, por ejemplo, se limitan a un tamaño de datos de 1,555 bytes, sin incluir la cabecera del MAC.

La cabecera IPX se sitúa después de cabecera del MAC y antes de los datos. La Figura 4.3.1. muestra la estructura de un paquete IPX.

A continuación se describen los campos del paquetes IPX.

Suma de comprobación: Comprueba la integridad del paquete. Se utiliza en el software de NetWare SFT (sistema de tolerancia a fallos), NetWare 4 y en versiones más recientes del Shell de NetWare (NETx.COM). Las versiones anteriores de NetWare no utilizaban la suma de comprobación del IPX y necesitaban definir este campo en 0xFFFF.

Longitud del paquete: Es la longitud, en bytes, del paquete entero constituida por la longitud de la cabecera IPX más la longitud de los datos, la longitud del paquete es al menos de 30 bytes para la cabecera IPX.

Control de transporte: Es el número de enrutadores que un paquete ha recorrido hasta su destino.

Tipo de paquete: Es el tipo de servicio ofrecido o requerido por el paquete.

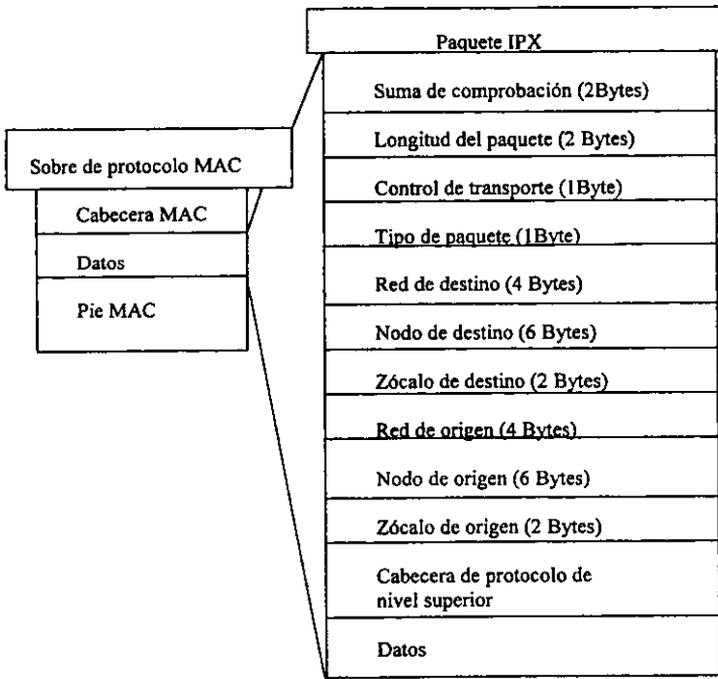


Figura 4.3.1. Estructura del paquete IPX.

Novell utiliza normalmente los tipos de paquete que se listan en la Tabla 4.3.1

Red de destino: Es el número de la red al que el nodo de destino se conecta.

Cuando un nodo de envío establece este campo en cero, se asume que el nodo de destino se encuentra en el mismo segmento de la red que el nodo de envío (u origen).

Nodo de destino: Es la dirección física del nodo de destino.

Zócalo de destino: Es la dirección de zócalo del proceso que recibe el paquete. Los zócalos encaminan paquetes a distintos procesos dentro de un nodo único.

Red de origen: Es el número de la red al que el nodo de origen se encuentra conectado. Si un nodo de envío establece este campo en cero, la red local a la que el origen se conecta es desconocida. Para los enrutadores, las reglas que se aplican al campo de la Red de destino también lo son para el campo Red de origen, excepto si los enrutadores pueden propagar paquetes que se recibieron con este campo establecido en cero.

Nodo de origen: Es la dirección física del nodo de origen.

Zócalo de origen: Es la dirección del zócalo del proceso que transmite el paquete.

En una situación de servidor de estación de trabajo, el servidor normalmente "escucha" un zócalo específico para obtener las peticiones de servicios. En tal caso, el zócalo de origen no es necesariamente él mismo ni tan solo es significativo. Lo importante es que el servidor responda al zócalo de origen. Por ejemplo, todos los servidores de archivos de NetWare tienen la misma dirección de zócalo, pero las peticiones que reciben pueden proceder de cualquier número de zócalo. Los números de los zócalos de origen siguen las mismas convenciones que los números de los zócalos de destino.

Cabeceras de protocolo de nivel superior: Son las cabeceras de protocolos NetWare de nivel superior, tales como NCP o SPX. Estas cabeceras ocupan la porción de datos del paquete IPX.

Tipos de paquete	Valor de campo (Hex.)	Finalidad
Protocolo de servicios de enlace de NetWare	0x00	Paquetes NLSP
Información de encaminamiento	0x01	Paquetes RIP
Notificación de servicio	0x04	Paquetes SAP
Secuenciado	0x05	Paquetes SPX
Protocolo central NetWare	0x11	Paquetes NCP
Propagado	0x14	NetBIOS
otros		Paquetes propagados

Tabla 4.3.1. Tipos de paquetes que utiliza Novell.

Direccionamiento IPX

IPX define su propio direccionamiento de red e intranodo. Para el direccionamiento de red (nodo), utiliza las direcciones físicas asignadas a la placa de interfaz de la red.

La dirección de red IPX identifica únicamente un servidor IPX y procesos individuales que se dan en un servidor. Una dirección de red completa IPX es un número hexadecimal de 12 bytes comprendidos entre los siguientes componentes:

- Un número de red de 4 bytes (servidor).
- Un número de nodo de 6 bytes (servidor).
- Un número de zócalo de 2 bytes (proceso del servidor).

Una dirección de red IPX completa puede tener este aspecto:
FEDCBA98A1A2B3C5D7ED0453.

- Cada número está contenido en un campo en la cabecera del IPX, y representa una red de origen o destino, un nodo o un zócalo.
- El número de la red se utiliza sólo para las operaciones de nivel de red, es decir, de encaminamiento.
- El número de nodo se utiliza para transmisiones de paquetes locales o de igual segmento.
- El número de zócalo envía un paquete a un proceso que opera dentro de un nodo.

Número de red: El número de red es la dirección hexadecimal de cuatro bytes que sirve de base para el encaminamiento de una red IPX. Cada segmento de red en una red IPX, se asigna a un único número de red. Los enrutadores de NetWare utilizan este número para reenviar paquetes a su segmento de destino final.

El número de red puede contener hasta ocho dígitos, incluyendo los ceros, (los ceros a la izquierda normalmente no se visualizan). Por ejemplo, FEDCBA98, 1234567D y C7 son todos números de red válidos. Los números 0 y FFFFFFFF no se encuentran disponibles para el direccionamiento de red; los servidores IPX los reservan para propósitos especiales.

Número de nodo: El número de nodo IPX es la dirección hexadecimal de seis bytes que identifica un dispositivo en una red IPX. Este dispositivo puede ser un servidor de archivos, un enrutador, una estación de trabajo o una impresora. El número de nodo es idéntico a la dirección física asignada a una placa de interfaz que conecta el dispositivo a la red.

IPX requiere que el número de la red sea único sólo dentro de la misma red IPX. Por ejemplo, un nodo en la red FEDCBA98 puede utilizar el número 1A2B3C5D7E y un nodo en la red 1234567D también puede utilizar el número 1A2B3C5D7E9F. Debido a que cada nodo tiene un número de red distinta, IPX reconoce que cada nodo tiene una dirección única y legítima.

Número de zócalo: El número de zócalo es el número hexadecimal de dos bytes que identifica el último destino de un paquete IPX que se encuentra en un nodo. Este destino, de hecho, es un proceso como el de encaminamiento (RIP) o notificación (SAP) que opera dentro de un nodo.

Debido a que varios procesos operan normalmente en cualquier momento, los números de zócalo proporcionan un tipo de "ranura de buzón" por la que cada proceso puede identificarse ante el IPX.

Un proceso que debe comunicar en la red requiere que se le asignen peticiones a un número de zócalo. Cualquier paquete que el IPX recibe y que se encuentra direccionado a un zócalo pasa por este proceso. Los números de zócalo proporcionan un método rápido de encaminamiento dentro del nodo.

La tabla 4.3.2 lista algunos de los números de zócalos y procesos que se utilizan en el entorno NetWare.

Número de zócalo	Proceso
0x451	Protocolo central del NetWare (NCP)
0x452	Protocolo de notificación de servicios (SAP)
0x455	NetBIOS de Novell
0x456	Diagnósticos
0x9001	Protocolo de servicios de enlace de NetWare (NLSP)
0x9004	Protocolo IPX WAN

Tabla 4.3.2. Número de zócalo y proceso que utiliza Netware.

Los números de zócalo entre 0x4000 y 0x7FFF son zócalos dinámicos; las estaciones de trabajo utilizan estos números para comunicar con servidores de archivos y otros dispositivos de la red. Los números de zócalo entre 0x8000 y 0xFFFF son zócalos muy conocidos; Novell los ha asignado a procesos específicos. Por ejemplo, 0x9001 es el número de zócalo que identifica el NLSP. Los técnicos del Software que escriben las aplicaciones de NetWare pueden contactar con Novell para reservar zócalos prácticos.

Encaminamiento IPX

Los enrutadores NetWare interconectan diferentes segmentos de red IPX y reciben instrucciones para el direccionamiento y encaminamiento de paquetes entre estos segmentos, desde el protocolo IPX, este cumple éstas y otras tareas de nivel de red con la ayuda del RIP, SAP y NLSP.

Cuando una estación de trabajo de NetWare que desea enviar información a otra estación de trabajo, si ambas estaciones de trabajo comparten el mismo número de red (ambas se encuentran en el mismo segmento), la estación de trabajo direcciona y envía paquetes directamente a la dirección física de la estación de trabajo. Si dos estaciones de trabajo tienen diferentes números de red (cada uno se encuentra en un segmento diferente), la estación de trabajo de envío debe encontrar primero un enrutador en su propio segmento que pueda enviar paquetes al segmento en el que se encuentra la estación de servicio de destino.

Para encontrar este enrutador, la estación de trabajo que envía difunde un paquete RIP que hace una petición de la ruta más rápida al segmento de destino. El enrutador que se encuentra en el segmento que envía, con la vía de acceso más corta al segmento de destino, responde a la

petición. En su respuesta, el enrutador incluye, en la cabecera IPX, su propia dirección de nodo y red, como se muestra en la figura 4.3.2.

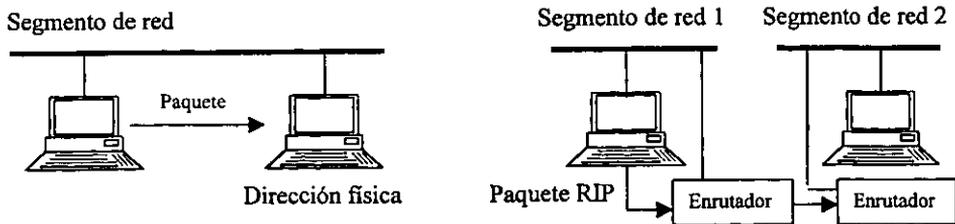


Figura 4.3.2. Encaminamiento IPX.

Si el nodo de envío no es un enrutador sino una estación de trabajo, no necesita difundir una petición RIP para obtener esta información; el enrutador la obtiene de su tabla de encaminamiento interna.

Cuando la estación de trabajo que envía, conoce la dirección del nodo del enrutador, direcciona y envía paquetes a la estación de trabajo de la manera siguiente:

- 1.-La estación de trabajo de envío sitúa la dirección de red IPX del nodo de destino, red, nodo, números de zócalo en los campos de destino correspondientes de la cabecera del IPX.
- 2.-La estación de trabajo de envío sitúa su propia dirección de red IPX, red, nodo y número de zócalo en los campos de origen correspondientes de la cabecera de IPX. La estación de trabajo de envío envía también llenos todos los campos de la cabecera.
- 3.-La estación de trabajo de envío sitúa la dirección de nodo del enrutador que ha respondido a la petición del RIP en el campo Dirección de destino de la cabecera MAC.
- 4.-La estación de trabajo de envío sitúa su propia dirección de nodo en el campo dirección de origen en la cabecera del MAC.
- 5.-La estación de trabajo envía el paquete.

Cuando un enrutador recibe un paquete IPX, realiza las siguientes tareas:

- 1.-El enrutador comprueba el campo de Control de transporte de la cabecera del paquete IPX. Un enrutador RIP descarta el paquete si el valor en este campo es superior a 16. Un enrutador NLSP descarta el paquete si el valor en este campo es mayor que el valor del parámetro límite de la cuenta de saltos.
- 2.-El enrutador comprueba el campo de la cabecera IPX (Tipo de paquete). Si el tipo de paquete es 20 (0x14, NetBIOS), el paquete se referencia de la manera siguiente:

- a) El enrutador examina el campo Control de transporte de la cabecera IPX. Si este valor es ocho o mayor, el enrutador descarta el paquete.

- b) El enrutador compara cada entrada de número de red que se encuentra en el paquete con el número de red del segmento en el que el enrutador recibe el paquete. Si el enrutador encuentra una coincidencia, descarta el paquete para evitar transversales en el mismo segmento de red. Si el enrutador no encuentra ninguna coincidencia lleva a cabo el siguiente paso.
- c) El enrutador sitúa las direcciones del segmento de la red desde las que llegó el paquete en el siguiente campo de Número de red disponible.
- d) El enrutador aumenta el campo de Control de transporte de la cabecera de IPX y difunde el paquete a todos los segmentos que no se encuentran representados en los campos Número de red.

3.-El enrutador comprueba los campos de la cabecera de IPX de Dirección de destino, red nodo, y números de zócalo para determinar cómo encaminar el paquete. Si el paquete se direcciona al enrutador, el proceso de zócalo apropiado lo referencia internamente; de otro modo él enrutador reenvía el paquete.

Los paquetes que requieren referencia interna incluyen los que se dirigen directamente al enrutador y las difusiones generales (Nodo de destino = 0xFFFFFFFF) para cualquiera de los segmentos de la red a los que el enrutador está conectado directamente. Normalmente, sólo RIP, SAP y los paquetes de diagnóstico se encuentran en esta categoría.

Cuando un enrutador reenvía un paquete IPX o cuando se remiten paquetes, el enrutador puede realizar una o dos acciones posibles. Si el paquete está destinado a un número de red al que el enrutador se conecta directamente, realiza las siguientes tareas:

- 1.-El enrutador sitúa la dirección del nodo de destino desde la cabecera del IPX en el campo dirección de destino de la cabecera del MAC.
- 2.-El enrutador sitúa su propia dirección de nodo en el campo dirección de origen de la cabecera del MAC.
- 3.-El enrutador amplía el campo de Control de transporte de la cabecera IPX y remite el paquete al segmento del nodo de destino.

Si el campo Control de transporte es igual al máximo permitido en la cuenta de saltos antes de ampliar el campo, el enrutador descarta el paquete. Para los enrutadores RIP, el límite de la cuenta de saltos es 16; para los enrutadores NLSP, este límite puede determinarse en cualquier número entre 8 y 127.

Se debe de tener en cuenta también que los paquetes de difusión nunca se vuelven a difundir sobre el mismo segmento de red del que provienen. Si el enrutador no está

directamente conectado al segmento en el que reside el nodo de destino final, envía el paquete al siguiente enrutador que se encuentra en la vía, al nodo de destino del modo siguiente:

- 1.-El enrutador sitúa la dirección del nodo del siguiente enrutador en el campo dirección de destino en la cabecera del MAC.
- 2.-El enrutador obtiene esta información de su tabla de información de encaminamiento.
- 3.-El enrutador sitúa su propia dirección de nodo en el campo Dirección de origen de la cabecera del MAC.
- 4.-El enrutador aumenta el campo Control de transporte en la cabecera del IPX y remite el paquete al siguiente enrutador.

Los siguientes protocolos dirigen la comunicación entre los enrutadores de NetWare y las estaciones de trabajo y definen el formato de los paquetes que utilizan estos dispositivos para intercambiar información.

Control de Acceso al Medio, (Medium Access control, MAC).

Intercambio de paquetes entre redes, (Internetwork Packet Exchange, IPX).

Intercambio de paquetes secuenciados, (Sequenced Packet Exchange, SPX).

Protocolo de ruta de información, (Routing Information Protocol, RIP).

Punto de acceso de servicio, (Service Access Point, SAP).

Protocolo de control de red, (Network Control Protocol, NCP).

Sistema básico de red de entrada y salida, (Network Basic Input/Output System, NetBIOS).

La figura 4.3.3 muestra la asignación relativa de los protocolos de NetWare al modelo de referencia de la interconexión de sistemas abiertos (OSI). Como este modelo sólo constituye una parte básica para la funcionalidad de la conectividad, no todos los protocolos de NetWare encajan completamente en un sólo nivel funcional.

Los protocolos de alto nivel (NetBIOS, SAP, NCP, SPX, NLSP y RIP) se basan en los protocolos MAC e IPX para manejar comunicaciones de bajo nivel como la dirección de nodos. Exceptuando NetBIOS, NCP y SPX cada uno de los protocolos desempeña un papel en la operación del encaminamiento de IPX.

4.4 INTERCAMBIO DE PAQUETES SECUENCIADOS (SPX)

Intercambio de Paquetes Secuenciados, (Sequenced Packet Exchange, SPX) es un protocolo orientado a la conexión que opera en el nivel de transporte OSI. Orientado a la conexión significa que cuando un nodo utiliza el protocolo SPX para comunicarse con otro nodo, se establece una conexión dedicada entre los dos. Esta conexión debe establecerse antes de que los nodos puedan intercambiar los paquetes.

El SPX garantiza la entrega de paquetes a sus destinatarios y que la entrega se realiza en la secuencia apropiada. Aunque el SPX garantiza la entrega de cada paquete que envía, es más lento que el IPX. La cabecera del SPX incluye la cabecera del IPX de 30 bytes pero añade 12

bytes adicionales para secuenciamiento, control de flujo, conexión e información de reconocimiento.

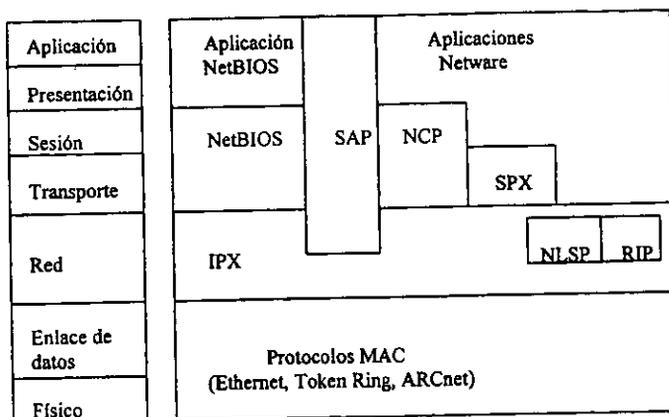


Figura 4.3.3. Asignación de Protocolos NetWare para el modelo de Referencias OSI.

4.5 PROTOCOLO DE RUTA DE INFORMACIÓN (RIP)

Los enrutadores utilizan el Protocolo de Ruta de Información (Routing Information Protocol, RIP) para intercambiar la información de encaminamiento con vecinos en una red IPX. A medida que un enrutador reconoce los cambios en la red IPX, difunde inmediatamente a los enrutadores vecinos ésta información.

Un enrutador RIP difunde periódicamente un paquete que contiene toda la información de encaminamiento conocida por el enrutador. Estas difusiones guardan todos los encaminamientos sincronizados en la red y proporcionan un medio de duración de las redes que se han convertido en inaccesibles desde la última difusión. Una red puede ser inaccesible porque un enrutador quedó fuera de servicio, o porque soltó un paquete que contenía información según la cual la ruta a la red es inaccesible. Las redes anteriores no aparecen en la difusión de información de encaminamiento.

Las estaciones de trabajo de NetWare también utilizan RIP para localizar la ruta más rápida a una red distante. Una red de trabajo inicia una demanda de ruta a través de la difusión de un paquete RIP y entonces "escucha" la respuesta del RIP que contiene la información de la ruta.

Estructura del paquete RIP

La estructura del paquete RIP se muestra en la Figura 4.5.1 Como en la mayoría de protocolos de nivel superior, el paquete RIP se encapsula dentro del área de datos del paquete

IPX. Los paquetes RIP se definen en la cabecera IPX como paquetes del tipo 1 y número de zócalo 0x453.

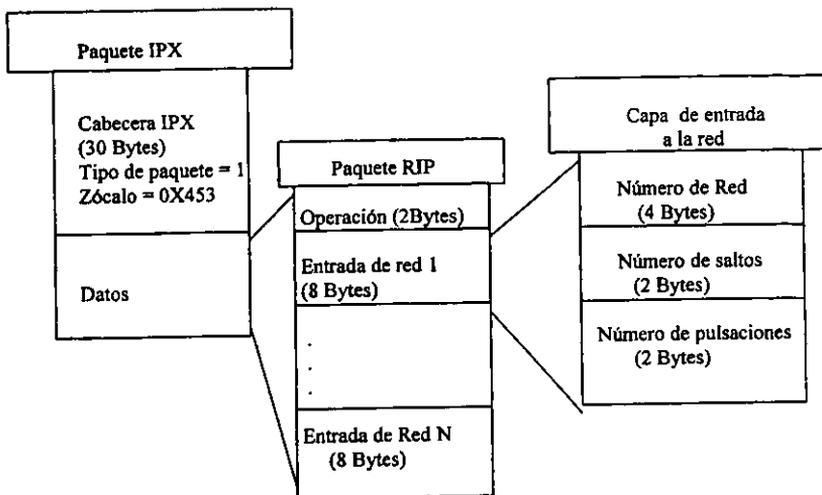


Figura 4.5.1. Estructura del paquete RIP.

Operación: Un indicador le especifica si el paquete es una petición o una respuesta. El valor 1 representa una petición RIP; el valor 2 representa una respuesta RIP.

Entrada de red: El sujeto de la petición o respuesta RIP. Cada entrada de red tiene una longitud de ocho bytes.

Un paquete RIP puede contener hasta 50 entradas de red. Así pues, dependiendo de la cantidad de información que el paquete contenga, el tamaño del paquete RIP puede variar de un mínimo de 40 bytes (cabecera IPX y una entrada de red RIP) hasta un máximo de 432 bytes (cabecera IPX y 50 entradas). Cada entrada de red RIP comprende los siguientes campos:

Número de red: El número de red que constituye el sujeto de la petición o respuesta de RIP. Para las peticiones RIP, este campo puede establecerse en 0xFFFFFFFF para indicar una petición general.

Número de saltos: El número de enrutadores que deben atravesarse para alcanzar el número de red asociado a esta entrada. Para los paquetes de respuesta, el número de saltos debe ser al menos de 1.

Número de pulsaciones: El tiempo de retraso, contado en "pulsaciones", para alcanzar el número de red asociado a esta entrada. Una pulsación representa 1/18 de segundo, (existen 18.21 pulsaciones en un segundo). El valor en éste campo es siempre de una pulsación como mínimo, para las respuestas RIP. Para un protocolo RIP que opera en una LAN, el tiempo de retraso es siempre una pulsación.

Si existen varias rutas hacia un número de red, un enrutador utiliza la vía de acceso con el menor número de pulsaciones cuando remite paquetes a ese número de red. Si dos vías de acceso tienen el mismo valor de pulsaciones, el enrutador selecciona la vía con el menor número de saltos.

Los enrutadores IPX utilizan RIP para crear y conservar una base de datos de información de encaminamiento, ver la Tabla 4.5.1. Esta tabla contiene información sobre todos los segmentos de la red, en la red del protocolo IPX. El enrutador utiliza esta información para enviar paquetes a su destino a través de la mejor ruta posible.

Número de red	Saltos a la red	Pulsaciones a la red	Placa interfaz de red	Direccionamiento inmediato de los enrutadores de envío	Temporizador de actualización
00000001	1	2	A	-	0
00000002	1	2	B	-	0
FEED0033	1	20	C	-	0
FEED0035	2	3	B	00001B029927	1
000000FF	2	3	A	00001B0349B2	2
FEED0036	3	4	A	00001B0349B2	2

Tabla 4.5.1. Información de encaminamiento de muestras.

Número de red: Es el número de red de cada segmento de red que el enrutador reconoce actualmente. Para obtener las instrucciones de envío de un paquete, el enrutador coloca el número de red de destino en la cabecera del IPX, con una entrada en este campo.

Saltos de red: Es el número de enrutador (saltos) que deben atravesarse para alcanzar el segmento de destino.

Pulsaciones a la red: Es una estimación del tiempo necesario para alcanzar el segmento de destino.

Placa de interfaz de red: Es la placa en el enrutador a través de la que se puede alcanzar el segmento de destino. Las letras A, B y C en la Tabla 4.5.1 son representaciones simbólicas de tres placas de interfaz diferentes.

Direccionamiento inmediato del enrutador de envío: Es la dirección del nodo del enrutador que puede enviar paquetes a cada segmento. Este campo se mantiene vacío si el segmento se encuentra directamente conectado al enrutador.

Temporizador de actualización: Se trata de un temporizador que asegura que la información sobre el segmento de destino está actualizada. Cada vez que el enrutador recibe información sobre la red, restablece el Temporizador de actualización a cero. Si el valor alcanza los tres minutos, el enrutador asume que la ruta a la red está fuera de servicio y difunde ésta conexión a sus segmentos conectados.

4.6 PUNTO DE ACCESO DE SERVICIO (SAP)

El protocolo Punto de Acceso de Servicio, (Service Access Point, SAP), es conceptualmente similar al protocolo RIP. Aunque los enrutadores utilizan RIP para intercambiar información, SAP proporciona a los enrutadores y servidores un medio para notificar e intercambiar información.

Los servidores de archivos de NetWare, los servidores de impresión, los servidores de compuerta (gateways) y las PC's que ejecutan un software del enrutador multiprotocolo de NetWare utilizan SAP para notificar sus direcciones de red y de servicios. Los enrutadores reúnen esta información y la comparten con otros enrutadores. Las estaciones de trabajo de la red determinan cuáles serán los servicios disponibles en la red y obtienen las direccionamientos IPX de los servicios. Las estaciones de trabajo utilizan esta información para iniciar una sesión con un servicio.

A medida que un enrutador va reconociendo cualquier cambio en la disposición física del servidor de la red, esta información se difunde inmediatamente a todos los enrutadores. Se envían periódicamente cada 60 segundos por defecto, paquetes de difusión SAP que contienen toda la información. Estas difusiones mantienen sincronizados todos los enrutadores en la red y proporcionan un medio de retirar a los servidores que se convierten en inaccesibles porque un enrutador o servidor ha quedado fuera de servicio desde la última difusión. Un servidor puede ser inaccesible porque un enrutador quedó fuera de servicio o porque soltó un paquete que contenía la información según la cual la ruta al servidor se hizo inaccesible. Los servidores obsoletos no aparecen en la difusión del SAP.

Del mismo modo que el RIP, el protocolo SAP utiliza el IPX y los protocolos MAC para su transporte.

Estructura del paquete SAP

La estructura del paquete SAP se muestra en la Figura 4.6.1. Como ocurre con la mayoría de los protocolos de nivel superior, el paquete SAP se encapsula dentro del área de datos del

IPX. Los paquetes SAP se definen en la cabecera del IPX como paquetes del tipo 4 y número de zócalo 0x452.

Operación: Tipo de operación que el paquete SAP lleva a cabo. Este campo puede definirse en uno de los siguientes valores:

- 1 (Petición).
- 2 (Respuesta).
- 3 (Peticiónes de obtención del servidor más cercano).
- 4 (Obtener respuestas del servidor más cercano).

Dependiendo del tipo de operación, el campo Operación va seguido por un campo único o bien por uno o más grupos de campos. Para todas las peticiones SAP (operaciones 1 y 3), el paquete incluye sólo el primer campo tipo de servicio. Esto significa que todas las peticiones SAP tienen una longitud de 34 bytes, sin incluir la cabecera de medios (cabecera IPX más los campos operación y tipo de servicio = $30 + 2 + 2 = 34$ bytes). Todos los demás campos se aplican solamente a las respuestas SAP (operaciones 2 y 4).

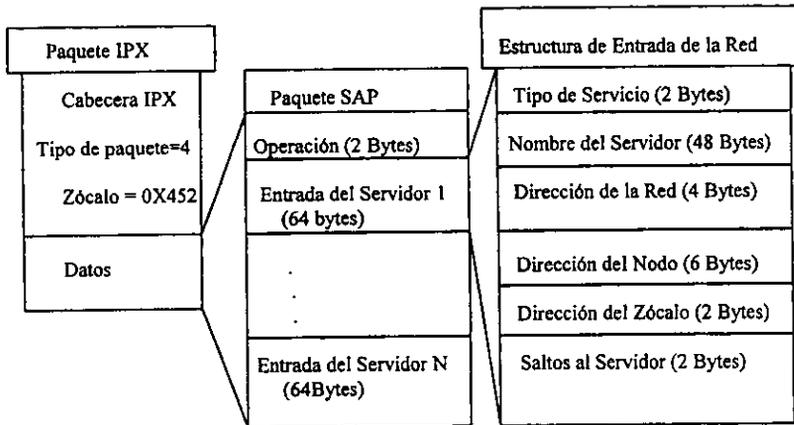


Figura 4.6.1. Estructura del paquete SAP.

Entrada de servidor: Es la información sobre el servidor que informa del servicio. Una respuesta SAP puede incluir de una a siete entradas de servidor. Así pues, los paquetes de respuesta SAP pueden variar de 96 bytes (cabecera IPX y una entrada de servidor) hasta 480 bytes (cabecera IPX y siete entradas). Cada entrada incluye información sobre un servidor particular y comprende los siguientes campos:

Tipo de servicio: Es el tipo de servicio que proporciona el servidor. Novell asigna a cada tipo de servidor un tipo de servicio único. Por ejemplo, un servidor de archivos Novell se notifica a

ESTA TESIS NO DEBE SALIR DE LA BIBLIOTECA

sí mismo como tipo 4. Este valor se convierte en el objeto tipo para este servidor. La Tabla 4.6.1 lista algunos de los tipos de servicio más comunes.

Tipo de servicio	Valor de campo (Hex.)
Desconocido	0x0000
Cola de impresión	0x0003
Servidor de archivos	0x0004
Servidor de tareas	0x0005
Servidor de impresión	0x0007
Servidor de respaldo	0x0009
Servidor de bridge remoto	0x0024
Reservado hasta	0x8000
Comodín	0xFFFF (-1)

Tabla 4.6.1. Tipos de servicio más comunes.

Nombre del servidor: Se trata del nombre de la cadena de caracteres de 48 bytes que se asigna a un servidor. El nombre del servidor, junto con el tipo de servicio, únicamente identifica un servidor en una red. Aunque los paquetes de respuesta SAP incluyen siempre todos los 48 bytes para este campo, los nombres del servidor son, normalmente, inferiores a esta longitud de 48 caracteres.

Dirección de red: Es la dirección de la red en la que reside el servidor.

Dirección de nodo: Es la dirección del nodo en donde reside el servidor.

Dirección de zócalo: Es el número de zócalo en el que el servidor recibe las peticiones de servicios.

Salto al servidor: Es el número de redes intermedias que han de atravesarse para alcanzar el servidor asociado con esta entrada. Cada vez que el paquete pasa a través de una red intermedia, el campo se incrementa en uno.

Un nombre de servicio identifica un receptor en un nodo de la red. En lugar de enviar el nombre del servicio en cada mensaje del IPX, el servicio se asigna a un número de zócalo. El número de zócalo tiene una capacidad de hasta 65,000 receptores en cada nodo del IPX. Cada servicio de un servidor NetWare tiene su propio número de zócalo y un tipo y nombre de servicio único en la red IPX.

Cuando se entra en un servidor de NetWare, el comando LOGIN lee la lista de servicios del servidor conectado. Desde ahí, obtiene la dirección del IPX y el número de zócalo del servidor de archivos con el nombre proporcionado. Esta dirección y número de zócalo se ponen en mensajes que llegarán hasta el receptor designado. Esto significa que cada servidor debe tener una copia de todos los servicios de la red IPX.

4.7 PROTOCOLO DE CONTROL DE RED (NCP)

El Protocolo de Control de Red (Network Control Protocol, NCP) permite comunicarse a las estaciones de trabajo de NetWare y a los servidores de archivos, definiendo dos aspectos de su interacción: control de conexión y codificación de la petición de servicio.

El Protocolo de Control de Red conserva su propio control de conexión y error de nivel de paquete controlando por sí mismo estas funciones, en lugar de confiar en otros protocolos. Las conexiones se establecen y terminan a través de las peticiones del NCP, que emiten las estaciones de trabajo de NetWare, y a través de las respuestas NCP, que emiten los servidores de NetWare.

Una estación de trabajo envía una Petición de NCP a un servidor para recuperar los siguientes tipos de información:

- Acceso y transferencia de archivos (con el comando NCOPY).
- Asignaciones de unidades virtuales (con el comando MAP).
- Búsquedas de directorios (con la utilidad FILER).
- Estado de cola de impresión (con la utilidad PCONSOLE).

Los servidores responden a estas peticiones con las Respuestas del NCP. Cuando el servidor ha procesado y cumplido la petición, la estación de trabajo termina la conexión enviando una petición de destrucción de conexión del servicio al servidor como se muestra en la figura 4.7.1.

4.8 SISTEMA BÁSICO DE RED DE ENTRADA Y SALIDA (NETBIOS) / INTERFAZ EXTENDIDA DE USUARIO DE NETBIOS (NETBEUI)

IBM y Microsoft diseñaron los protocolos del Sistema básico de entrada-salida en red (Network Basic Input Output System, NetBIOS) y de la interfaz extendida de usuario de (NetBEUI, NetBIOS Extended User Interface, NetBIOS) para dar soporte a las comunicaciones en entornos de red de área local de pequeño y medio tamaño. En la figura 4.8.1 se representa el entorno completo de los protocolos.

Redireccionador: Dirige las peticiones de red a los servidores de la misma y las órdenes locales al sistema operativo local.

Bloques de mensajes del servidor: Proporciona el lenguaje par a par y los formatos necesarios para que las computadoras se comuniquen unas con otras.

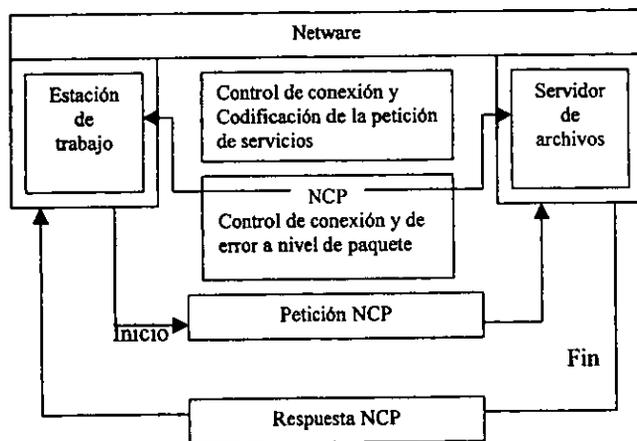


Figura 4.7.1. Comunicación NCP.

NetBIOS: Un protocolo del nivel de sesión relacionado con el modelo de protocolos OSI. Establece y mantiene las sesiones de comunicación entre computadoras.

NetBEUI: Proporciona los servicios subyacentes para el transporte de los datos.

NDIS: Especificación de la interfaz del controlador de red (NDIS, Network Driver Interface Specification), proporciona una forma de dar soporte a otros protocolos, como TCO/IP como una única interfaz de red.

NetBIOS y NetBEUI se implementan en diversos sistemas operativos de equipos de escritorio y de red, incluidos OS/2, Windows para trabajo en grupo, Windows NT, LAN Manager de Microsoft y LAN Server de IBM. Sin embargo Microsoft también da soporte a la pila de protocolos del Protocolo de Control de Transmisión / Protocolo Internet (Transmission Control Protocol / Internet Protocol, TCP/IP) en todos sus productos de red. Una razón para esto es que NetBIOS no es un protocolo enrutador y no es adecuado en un entorno de red de área extensa.

Sistema Básico de Entrada-Salida en Red (NetBIOS)

El Sistema Básico de Red de Entrada y Salida (Network Basic Input/Output System, NetBIOS), proporciona servicios a nivel de sesión, tales como direccionamiento nombrado y ensamblajes y desensamblajes de paquetes. Tal como ocurre con el SPX, NetBIOS también proporciona servicios a nivel de transporte, tales como la entrega de paquetes garantizada y el secuenciamiento de paquetes.

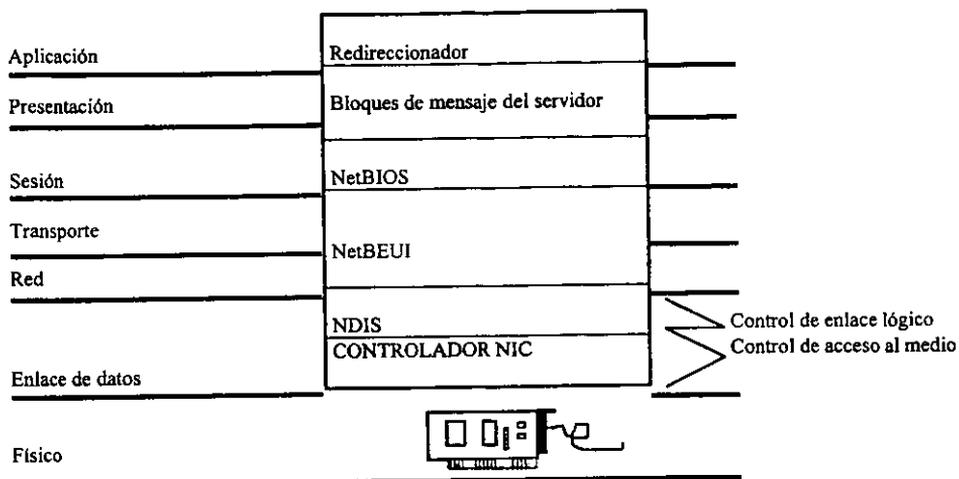


Figura 4.8.1. Entorno de protocolo NetBIOS/NetBEUI.

Para que NetBIOS pueda operar en el entorno NetWare, los enrutadores IPX deben ser capaces de propagar paquetes NetBIOS a través de una red. NetWare cumple con esta condición definiendo un tipo de paquete IPX especial, el tipo 20 (0x14), para designar un paquete propagado. El tipo de paquete 20 y el número de zócalo 0x455 juntos identifican el paquete NetBIOS. Adicionalmente, el campo Nodo de destino en la cabecera de IPX se define en 0xFFFFFFFFFFFF. Esto da la instrucción a cada enrutador que recibe el paquete, de difundirlo a todos los nodos en la red de destino, como se muestra en la figura 4.8.2. Los paquetes NetBIOS requieren un manejo exclusivo por parte de un enrutador.

NetBIOS se diseñó con la premisa de que las PC's en una LAN solo necesitan comunicarse con otras PC's en la misma LAN.

NetBIOS es una interfaz de programación de aplicaciones (API, Application Program Interface) que los programadores utilizan para crear aplicaciones LAN para los entornos LAN server de IBM, LAN manager de Microsoft y OS/2. Los conductos nominados son una extensión de red hacia OS/2 que proporciona características parecidas pero más avanzadas. NetBIOS y los conductos nominados en el entorno LAN son protocolos donde se construyen distintas aplicaciones. NetBIOS ofrece los servicios siguientes:

- NetBIOS establece nombres lógicos para los nodos de la red, así simplifica la tarea de referenciar otros sistemas. El nombre tiene una longitud de 1 a 15 caracteres e identifica una estación de trabajo en concreto, tanto en las computadoras como para los usuarios. Este nombre se especifica cuando una computadora se asigna o se incluye por primera vez en la red. Los grupos de nombres se les pueden enviar mensajes.

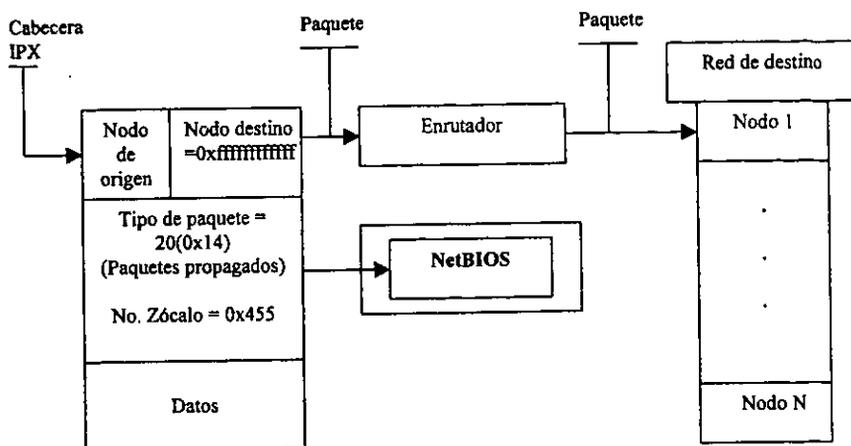


Figura 4.8.2. Protocolo NetBIOS.

- NetBIOS establece una sesión orientada a la conexión sobre la cual los nodos se comunican entre ellos. La sesión tiene lugar sobre un circuito o conexión lógica. NetBIOS establece, mantiene y finaliza una sesión, las estaciones de trabajo se comunican en tiempo real, con el envío de datos garantizado a través de la confirmación de envío de los mensajes.
- NetBIOS también puede proporcionar servicios de datagramas no orientados a la conexión en los cuales los mensajes se dirigen a otros sistemas sin el establecimiento de una conexión o la supervisión del flujo de paquetes previos.
- Las aplicaciones de red que se ejecutan en redes compatibles con NetBIOS, lo usan para localizar y establecer conexiones con otros recursos para el intercambio de datos. Los recursos podrían ser otras aplicaciones.
- NetBIOS transmite información sobre la ubicación de los servidores y los nombres de estos servidores. Esta transmisión puede sobrecargar la red con exceso de paquetes y causar problemas en las redes. Sin embargo el filtrado en puentes (bridges) y enrutadores (routers) puede resolver estos problemas.
- NetBIOS no es enrutable, en parte debido a su sistema de nombres de 15 caracteres. NetBIOS se debe de empaquetar en los paquetes de otros protocolos para su distribución sobre las redes. El protocolo TCP/IP consta de un procedimiento para el empaquetamiento de NetBIOS. Novell da soporte a NetBIOS en sus redes IPX, mientras que el DEC lo hace en sus redes DECnet.

Los servidores utilizan la utilidad de difusión de NetBIOS para localizar dispositivos y estaciones de trabajo en sus dominios. Si una estación de trabajo responde a los mensajes, el

servidor no le envía más. Si una estación de trabajo no responde porque esta apagada o tiene una tarjeta de interfaz defectuosa, el servidor envía mensajes cada pocos minutos para intentar obtener una respuesta. Debido a que los mensajes se envían a cualquier parte de la red, incluso a los enlaces de WAN, en lo que se refieren al uso del ancho de banda estos enlaces se consideran caros y costosos. Se puede utilizar una función de Directorio de nombres remotos (RND, Remote, Name Directory), para introducir estas transmisiones en los datagramas que no se han difundido y que no atraviesan los enlaces de WAN.

Interfaz Extendida de Usuario de NetBIOS, (NetBEUI)

La Interfaz Extendida de Usuario de NetBIOS, (NetBIOS Extended User Interface, NetBEUI), fue desarrollado por IBM en 1985 como un protocolo de transporte de red para LAN's de pequeño a medio tamaño. Microsoft a través de sus productos de red, incluso Windows para trabajo en grupo y Windows NT dan soporte a NetBEUI. Las redes de IBM y Microsoft pueden comunicarse debido a la implementación de NetBIOS y NetBEUI.

NetBEUI es un protocolo de los niveles de transporte y de red del modelo de referencia OSI. Se integra con NetBIOS para ofrecer un sistema de comunicaciones eficiente en el entorno LAN de grupos de trabajo. NetBEUI proporciona los servicios de transporte que NetBIOS necesita. Por ejemplo en una llamada telefónica NetBIOS es la persona que hace la llamada y NetBEUI es como el programa de control que trabaja con el sistema subyacente de conmutación para completar la llamada.

4.9 X.25

El protocolo X.25 cubre la conexión de terminales de datos, computadoras y otros sistemas de usuario o para dispositivos de redes de conmutación de paquetes. Los sistemas de usuario se llaman genéricamente equipo terminal de datos (ETD). Su conexión a la red se hace por medio de un equipo de red llamado equipo de terminación de circuitos de datos (ETCD). Normalmente un ETD desea establecer comunicación con otro ETD (otro sistema de usuario) y utiliza la red con ese propósito. A su vez, ese ETD se conectará a un ETCD que controla su acceso a la red, y esta será responsable de administrar las comunicaciones entre los ETCD. El protocolo X.25 regula el flujo de datos entre ETD y ETCD solo en cada extremo de la red, esto se muestra gráficamente en la figura 4.9.1.

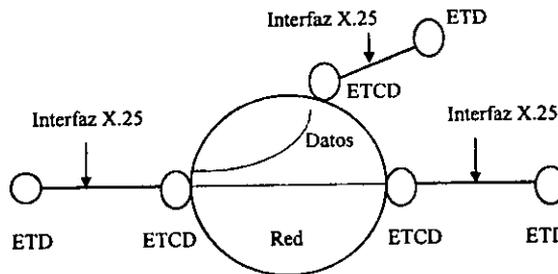


Figura 4.9.1. Concepto X.25.

En la figura aparece un ETD en comunicación con otros dos ETD diferentes y dispersos geográficamente. En un principio las especificaciones X.25 incluían un modo de operación de datagrama además del servicio de circuito virtual. Por lo tanto X.25 es solo una especificación de interfaz, que gobierna las interacciones entre un ETD y un ETCD a los que esta conectado. Los detalles de la comunicación entre ETCD, usando la red que los conecta, se deja al dueño u operador de esta. Tales detalles quedan ocultos a los ETD, que son los usuarios del servicio de conmutación de paquetes.

El protocolo X.25 esta organizado como una arquitectura de tres niveles, que corresponde a tres niveles del modelo de referencia OSI, los tres niveles de X.25 se muestra en la figura 4.9.2.

De los tres niveles de X.25, el de nivel físico se usa para asegurar la existencia de una conexión física valida entre el ETD y el ETCD.

El protocolo de nivel de enlace en el nivel de enlace de datos es un subconjunto de HDLC etiquetado como LAPB (Link Access Procedures Balanced, procedimientos balanceados de acceso al enlace). A la capa de nivel de paquetes en X.25, que esta en el tercer nivel de red, se distingue como una arquitectura de interfaz.

La relación de nivel por nivel con la arquitectura OSI se muestra en la figura 4.9.3.

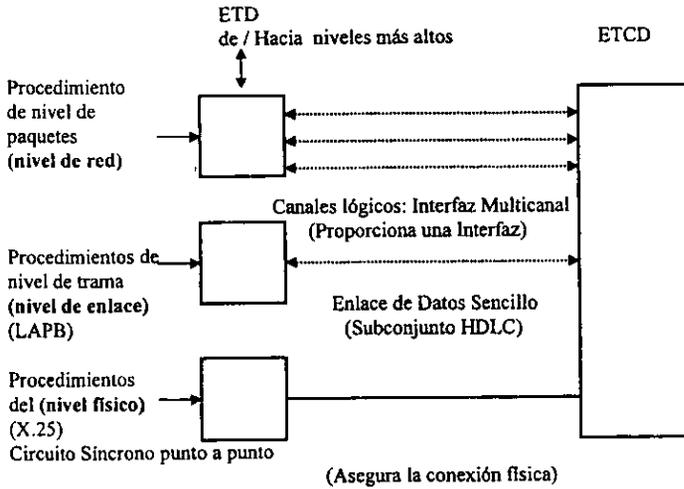


Figura 4.9.2. Capas del X.25.

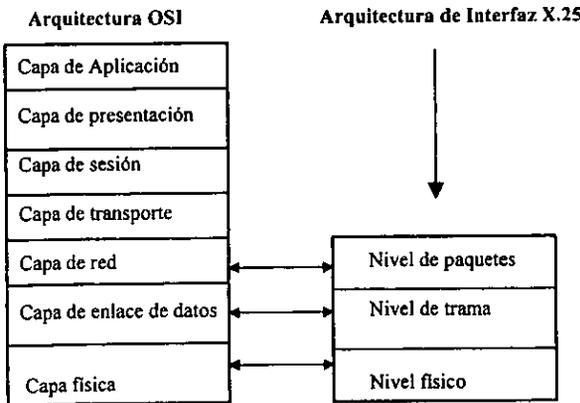


Figura 4.9.3. Relación entre las arquitecturas OSI y X.25.

X.25 se enfoca a conexiones de Circuitos Virtuales (Virtual Circuit, CV). Para este propósito, se asignan números de canal lógico en una conexión X.25 en particular, hay disponibles hasta 4095 de estas conexiones entre cualquier ETD y ETCD que tiene como interfaz, para ello se usa un campo de dirección de 12 bits, esto implica que hasta el mismo número de llamadas de (CV) pueden simultáneamente realizarse entre un ETD dado y los otros ETD, una vez establecida la llamada, cada paquete de datos que sale de un ETD lleva su

propio número de canal lógico de 12 bits, todos se multiplexan o comparten el mismo enlace de datos y usan el mismo proveedor de servicios, el nivel de enlace de datos inferior.

Cada interfaz ETD - ETCD asigna su propio conjunto de números de canales lógicos, así, un CV completo, de extremo a extremo entre dos ETD que se comunican entre sí, pueden usar diferentes números de canales lógicos en las dos interfaces en cada extremo del circuito virtual.

Como en los diferentes niveles de la arquitectura OSI, se requieren tres fases de comunicación para la operación de (CV) estas son:

- Fase de establecimiento de la llamada.
- Fase de transferencia de datos.
- Fase de desconexión o liberación de la llamada.

Se pueden usar (CV) permanentes en cuyo caso no se necesita establecer la llamada, la figura 4.9.4. muestra la fase de establecimiento y liberación de la llamada.

En donde las flechas indican los diversos paquetes de control (unidades de datos de protocolo de nivel de red) que se transmiten entre el ETD y el ETCD al que este se halla conectado. Estas son todas las unidades de datos de igual nivel que se transmiten entre protocolos de nivel de paquetes en cada uno de los sistemas (ETD y ETCD).

El paquete de solicitud de llamada de X.25 de la figura anterior notifica al ETCD al que se dirige que el ETD que lo emite, desea establecer comunicación con otro ETD conectado a la red. El paquete lleva un número de canal lógico para que lo usen en las conexiones lógicas ETD-ETCD, así como en las direcciones de los ETD emisor - receptor, los parámetros que especifican las características de la llamada, mas 16 octetos de datos, como máximo. Esta información se transmite a través de la red usando los procedimientos propios de ella, y alcanza al ETCD destino, luego, este sistema transmite el mismo tipo de paquete que lleva la misma información, excepto quizá por el número de canal lógico diferente, al ETD destino (receptor). Como este paquete lo emite un ETCD, se cambia su nombre a paquete de llamada entrante. El ETD contesta con un paquete de llamada aceptada, el cual, al avanzar a través de la red, aparece como un paquete de llamada conectada, emitido por el ETD emisor como respuesta a las peticiones originales de llamada de los ETD emisores, entonces, ahora se puede iniciar la transferencia de datos usando paquetes de datos (UDP), de datos de nivel de red. El procedimiento de la liberación de la llamada es similar, como se muestra en la figura anterior, la diferencia es que el ETCD receptor da la aceptación de inmediato al paquete de solicitud de liberación, sin esperar una confirmación del otro ETD. Al igual que los niveles OSI, este protocolo tiene control de errores y flujo al nivel de paquetes (red), para la transmisión expedita de datos y para otras operaciones similares incorporadas en los protocolos de los niveles OSI.

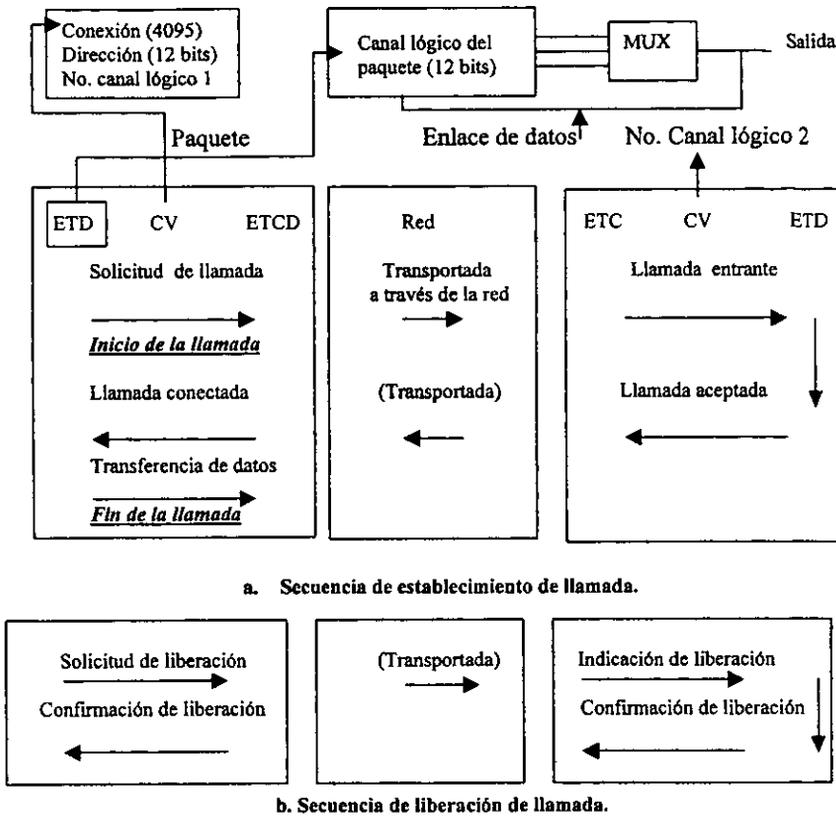


Figura 4.9.4. Procedimientos y paquetes X.25 para establecer y liberar un circuito virtual (a, b).

4.10 PROTOCOLO DE CONTROL DE TRANSMISIÓN/PROTOCOLO INTERNET, (TCP/IP)

Es un conjunto de protocolos, que consta de cuatro capas: física, de envío, de servicio y de aplicación, en donde la capa física no es especificada en realidad por TCP/IP, por lo que el usuario tienen la libertad de utilizar cualquier transmisión física, incluyendo a las redes de área amplia, de área metropolitana y de área local. El protocolo Internet (IP) de TCP/IP es aproximadamente equivalente a la capa de la red del modelo OSI, en tanto que TCP corresponde, cuando menos a la capa de transporte, aunque también a la capa de presentación, los otros protocolos asociados con TCP/IP se relacionan con la capa de aplicación, e incluyen al protocolo de transferencia de archivos (FTP) el protocolo simple de transferencia de correspondencias (SMTP) y los protocolos de emulación de terminales (Telnet).

Entre los estándares internacionales aproximadamente equivalentes se encuentran (File Transfer Access and Management , Acceso y manejo de transferencia de archivos, (FTAM), OSI DIS 8571), (Message Handling System , sistema de manejo de mensajes, X.400) y (Virtual Terminal Protocolo, protocolo de terminales virtuales, VTP,OSI DIS 9041). Pero en general los protocolos de OSI son más completos que los de TCP/IP.

Relación entre TCP/IP y OSI

El modelo OSI (Open Systems Interconnection) se utiliza para designar un conjunto de protocolos mas detallados que se utilizan como lineamientos para configurar una red OSI real.

El objetivo de TCP/IP es proporcionar un conjunto de protocolos de comunicaciones que sean independientes del fabricante, la figura 4.10.1 muestra la relación entre TCP/IP y OSI.

Aplicación	TELNET FTP SMTP	VTP FTAM X.400	Aplicación
Servicio	TCP	ISO 8823 ISO 8327 ISO 8073	Presentación Sesión Transporte
Envío	IP	ISO 8473	Red
Físico	*	LLC/MAC	Enlace de datos
	*	**	Físico

Figura 4.10.1. Relación entre TCP/IP y el modelo OSI.

Aunque TCP/IP se ha implantado frecuentemente en LAN estándar 802.3, TCP/IP es un conjunto de protocolos no relacionados con los estratos físicos y de enlace de datos, TCP/IP se puede implantar en casi cualquier medio físico de comunicaciones de datos y de protocolos de las capas física y de enlace de datos relacionados.

TCP/IP ofrece la secuencia de paquetes, control de errores y otros servicios que se requieren para generar comunicaciones confiables, en tanto que IP tomara el paquete de TCP y lo pasa a través de las vías de acceso que sean necesarias para enviarlo la capa TCP remoto a través de la capa IP distante, como se muestra en la figura 4.10.2, aunque algunas redes pueden utilizar al IP pero no al TCP optando por utilizar un protocolo alternativo en la capa de transporte, algunas veces se utiliza el termino TCP/IP para referir a varios protocolos diferentes, el

conjunto de protocolos se denomina conjunto o pila de protocolos Internet, este conjunto consta de no solo de TCP/IP sino también de algunos protocolos de la capa de aplicación.

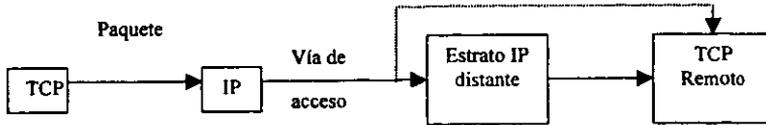


Figura 4.10.2. Secuencia de paquetes en TCP/IP.

Los servicios tradicionales de TCP/IP son soportados por los protocolos adecuados, estos protocolos son:

- **FTP:** Protocolo de transferencia de archivos, que hace posible la transferencia de archivos de una computadora de Internet a cualquier otra computadora también en Internet.
- **TELNET:** Protocolo de terminales de red ofrece un medio para permitir a un usuario en Internet, ingresar a cualquier otra computadora de la red.
- **SMTP:** Protocolo simple de transferencia de correspondencia, permite a los usuarios enviar mensajes entre sí en Internet.

Otros servicios que se ofrecen en el campo de acción de TCP/IP son:

- Sistemas de Archivos para Redes.
- Impresión distante.
- Ejecución distante.
- Servidores de nombres.
- Servidores de terminales.
- Sistemas de ventas orientados a redes.

TCP se comunica con aplicaciones a través de puertos específicos y cada uno de ellos tiene un número o dirección local propio. Si un proceso en el nodo A, asociado con el puerto 1, debe enviar un mensaje al puerto 2 (nodo B) ese proceso transmite el mensaje a su TCP de la capa de servicio con instrucciones adecuadas para dirigirlo a su nodo destino y puerto buscado. TCP envía el mensaje a IP con instrucciones para llevar el mensaje a la vía de acceso, que es el primer lóbulo del nodo b, esta secuencia de eventos es regulada anexando información de control de datos del usuario en diversas capas, como se muestra en la figura 4.10.3.

TCP segmenta los datos del usuario (Aplicación), en unidades manejables, luego anexa un encabezado TCP que incluye el puerto de destino, número de secuencia del segmento y suma de verificación para verificar si existen redes en la transmisión. Esta unidad recibe el nombre de segmento TCP. Una vez que se ha ensamblado el segmento TCP se pasa a IP, donde se anexa un encabezado IP. Un elemento importante almacenado en el encabezado IP es la dirección anfitrión/nodo destino, la unidad resultante es un datagrama IP, en general un datagrama puede definirse como un paquete de longitud finita con información suficiente para

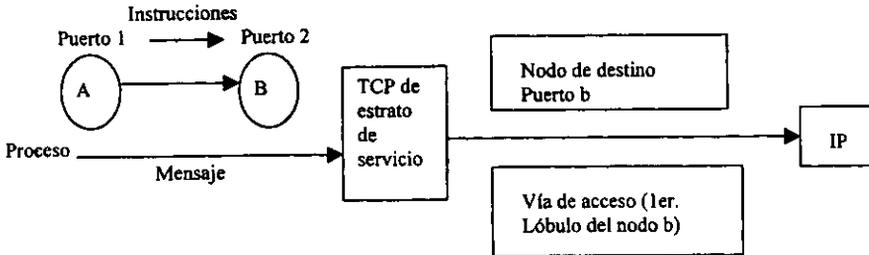


Figura 4.10.3. Comunicación de TCP/IP con aplicaciones.

ser enviado en forma independiente de la fuente al destino sin apoyarse en transmisiones anteriores, después el datagrama IP es entregado a la capa física donde el protocolo de acceso a la red anexa su información de control, creando así un paquete como se muestra en la figura 4.10.4. El paquete es enviado después por el medio físico. El encabezado del paquete contiene información suficiente para llevar el paquete completo del nodo A cuando menos a la vía de acceso.

Todos los nodos de una red TCP, podrían residir en una misma LAN, como una Ethernet. En tal caso TCP/IP operaría como un Sistema Operativo de Red (Network Operative System, NOS) de área local. Sin embargo el concepto original que respaldó a TCP/IP fue que ofreciera un estándar común para enlazar a muchas máquinas distantes y a muchas redes remotas, en consecuencia se debe de utilizar alguna clase de sistema de dispositivo de envío vía acceso/puente.

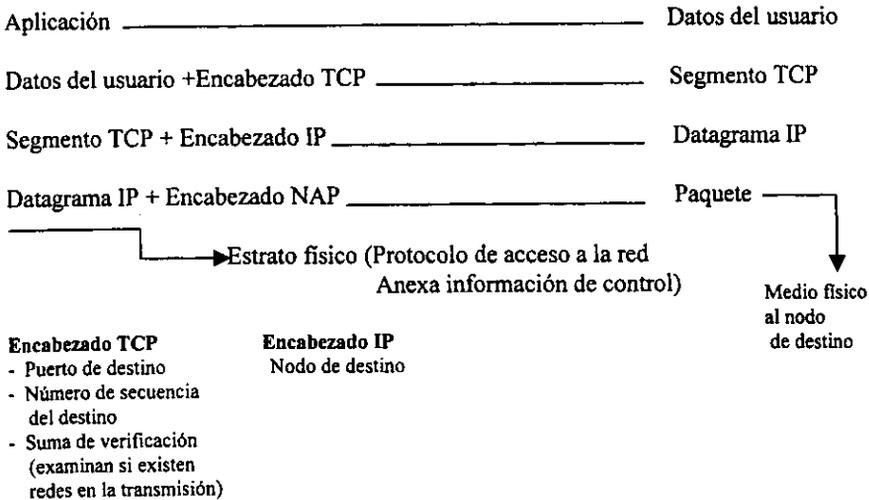


Figura 4.10.4. Formación del paquete de una red TCP.

CAPÍTULO V COMPONENTES DE UNA RED

5.1 MEDIOS FÍSICOS Y SISTEMAS DE TRANSMISIÓN

5.1.1 CABLES DE COBRE

Los cables de cobre utilizados para transmisión son conductores clásicos que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable.

Este tipo de cable es relativamente el más barato pero sus características eléctricas impiden su uso. Por ejemplo el cobre opone gran resistencia al flujo de electrones, por lo cual limita la distancia de los cables.

Sus características del cable de cobre son:

Los datos binarios transmitidos sobre cable de cobre pueden ser alterados por los fenómenos de atenuación de la señal, capacitancia, impedancia y distorsión, ruido e inductancia. La medida de estos efectos depende del material usado para construir el cable.

Atenuación: Se tiene grandes pérdidas en la amplitud de la señal, en transmisión de señales sobre grandes longitudes de cable. Esto causa errores y será necesario pedir retransmisión.

La atenuación se mide en decibeles (dB) o pérdida de la señal. Por cada 3dB de señal pérdida se produce un 50% de señal perdida.

Capacitancia: Es la capacidad que tiene el cable y el aislante de almacenar cargas electrostáticas en el cable, y entonces es así como se produce la distorsión de la señal, por almacenamiento de energía. La tolerancia en cable UTP es de 17 a 20 pF (picofarads).

Impedancia y distorsión: Una señal de varias frecuencias esta propensa a desfasar la señal causada por la impedancia, esto se debe que la resistencia que cambia por las diferentes frecuencias.

Ruido: Muchas de las líneas de transmisión llevan ruido, el cual es generado por fuentes externas. El ruido ambiental sobre circuitos digitales es causado por lamparas fluorescentes, motores, hornos de microondas, computadoras, teléfonos, copiadoras, etc.

Inductancia: La inductancia ocurre debido al flujo de corriente sobre dos conductores metálicos adyacentes. Los campos electromagnéticos creados por los flujos de corrientes pueden crear señales distorsionadas en ambos alambres juntos; pero el más grande problema la creación del near-end, crosstalk o NEXT (cruce de señales), ocurre cerca del transmisor y crea señales distorsionadas.

El trenzado en pares de alambres es el primer método para reducir los efectos de la

inductancia. El trenzado en los pares de alambres cancela la energía positiva y negativa sobre el cable. Con este método se permiten altas velocidades de datos y permite mas longitud del cable que un simple cable de cobre.

5.1.2 EL CABLE DE PAR TRENZADO

Es el tipo menos caro y más común medio de transmisión de la red, este cableado esta compuesto de por lo menos dos alambres aislados, trenzados de manera que cada unión recibe la misma cantidad de interferencia del ambiente, este ruido del ambiente se vuelve parte de la señal que se transmite, el trenzado de los alambres reduce el ruido, aunque no elimina, estos alambres vienen en un amplio rango de pares y calibres, los alambres tienen un numero de calibre designado por (American Wire Gauge, AWG) basado en su diámetro, los cables de par trenzado más comunes para redes son los de calibre 22 y 24.

El cable de par trenzado esta empaquetado en grupos de pares, él número de pares trenzados por grupo puede variar en un rango de 2 a 3000, entre más trenzados tenga el cable es menor la interferencia, muchas de las LAN's implementadas utilizan 25 pares, algunas utilizan el mismo cable de par trenzado sin blindar, que es más económico que se utiliza para los teléfonos, mientras que otras requieren un cable de mayor calidad para la transmisión de datos.

La principal desventaja de este tipo de cable es el rango limitado y la sensibilidad a las interferencias eléctricas, en un principio este tipo de medio podría manejar velocidades de transmisión de cerca de 1 Mbit por segundo (Mbps) a través de varios cientos de metros. En la actualidad la norma industrial 10baseT muestra los avances tecnológicos que hacen posible transmitir información a 10 Mbps a través de cable de par trenzado y hoy en día se logra transmitir a 100 Mbps por medio de un cableado de par trenzado no blindado.

La figura 5.1.2.1 muestra el cable de par trenzado de dos pares.

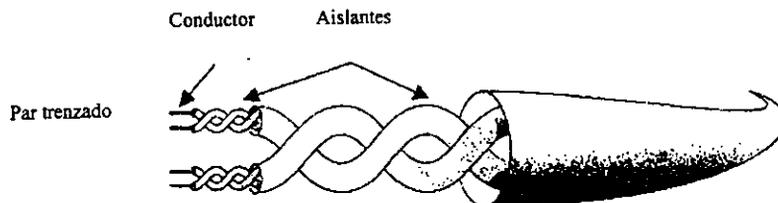


Figura 5.1.2.1. Cable de par trenzado (dos pares).

5.1.2.1 CABLE DE PAR TRENZADO SIN BLINDAJE (UTP)

El cable de Par Trenzado sin Blindaje (Unshielded Twisted Pair, UTP), consiste en alambres de cobre protegidos por un aislante. Dos alambres trenzados forman un par, y este par forma un circuito balanceado. El trenzado de los hilos fue diseñado para evitar la diafonía, interferencias. El cable UTP tiene múltiples pares trenzados, cada código de color, diferencia de los otros pares, UTP es muy usado en las redes telefónicas.

Según su calidad EIA/TIA 568 ha dividido categorías, que definen las propiedades eléctricas requeridas para cada tipo de red.

Categorías

Existen opciones típicas de sistemas de cableado estructurado, cada una posee características de producto y de funcionamiento particulares.

Categoría 1: Cable telefónico tradicional.

Categoría 2: Cable certificado para la transmisión de datos hasta 4 Mbits/seg.

Categoría 3: Este cable brinda soporte a la topología en anillo con testigo (4 Mbits/seg) y Ethernet 10Base-T a 10 Mbits/seg reúne los requerimientos básicos de cableado para telecomunicaciones.

Categoría 4: Este cable soporta a la topología en anillo con testigo a 16 Mbits/seg, brinda buena separación diafónica, acomoda todas las aplicaciones para datos como Token Ring/Ethernet.

Categoría 5: Acepta una velocidad de 100 Mbits/seg mediante nuevas tecnologías como Ethernet rápida. Este tipo de cable esta garantizado para un funcionamiento eléctrico de hasta 350 MHz. Acomoda todas las aplicaciones de ATM.

La figura 5.1.2.1.1 muestra el tipo de cable de par trenzado de 4 pares.

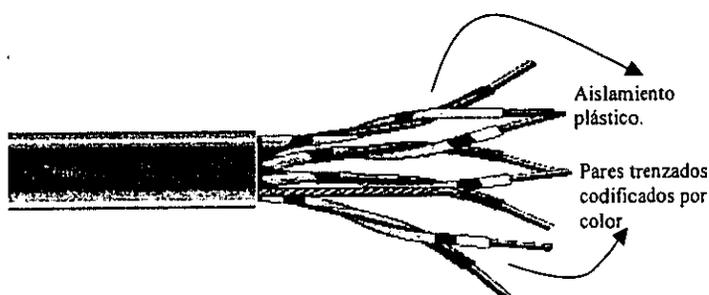


Figura 5.1.2.1.1. Cable de par trenzado (4 pares).

La figura 5.1.2.1.2 muestra los algunos tipos de cables UTP.

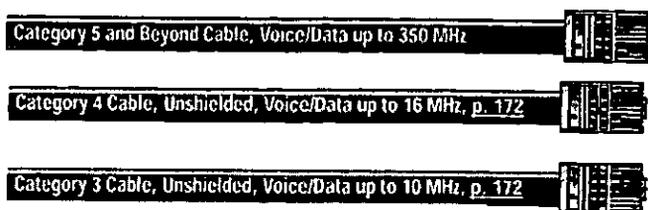


Figura 5.1.2.1.2. Algunos tipos de categorías de Cableado estructurado UTP.

5.1.2.1.1 CONECTOR Y BASE RJ-45

Los conectores y bases se utilizan en los cables UTP (y también en otros tipos de cable). Constan de ocho contactos numerados como se puede ver en la figura 5.1.2.1.1.1 que muestra el conector y base RJ-45, usados en cables UTP.

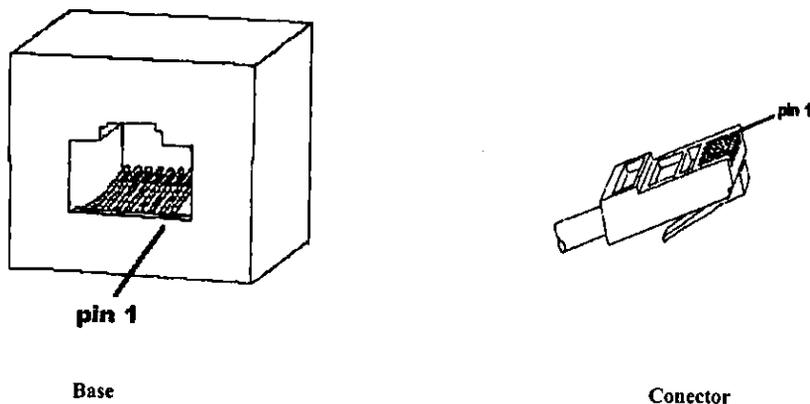


Figura 5.1.2.1.1.1. Conector y base RJ-45.

5.1.2.2 CABLE DE PAR TRENZADO BLINDADO (STP)

El Cable de Par Trenzado Blindado (Shielded Twisted Pair, STP) consiste de alambres de cobre protegidos por una cubierta exterior, un blindaje con metal trenzado y por un aislante dieléctrico. El trenzado en cada par de alambres forma un circuito balanceado. Este trenzado previene de problemas de interferencia. Los múltiples pares de alambres de cobre, están codificados por diferentes colores, proveen protección contra crosstalk externo.

La figura 5.1.2.2.1 muestra la forma del cable STP.



Figura 5.1.2.2.1. Cable STP.

5.1.3 CABLE COAXIAL

Este tipo de cable es el que más se utiliza para las LAN grandes, el cable coaxial está basado en una alma central de cobre envuelta por una cubierta de plástico o aislante dieléctrico, rodeada a su vez por una cubierta externa hecha de cobre o de aluminio que actúa como conductor, esto también proporciona protección contra la interferencia de otras señales. La señal se transmite a través del alma central y la cubierta externa que contiene metal trenzado que protege de la interferencia eléctrica externa, este tipo también se usa en las casas como parte integral de los televisores por cable.

En un principio el cable coaxial era el más común para las LAN debido a su alta capacidad y a su resistencia a la interferencia, pero como su grosor impide instalarlos a través de ductos de cables pequeños y ángulos estrechos, por lo que la mayoría de las redes se les prefiere instalar otro tipo de cables como el de par trenzado o el de fibra óptica, lo que hace que el cable coaxial esté declinando su uso.

La figura 5.1.3.1 muestra el esquema de un cable coaxial.

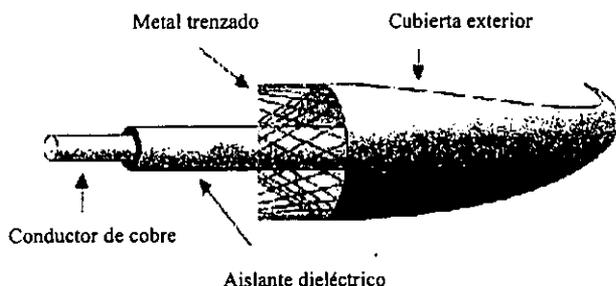


Figura 5.1.3.1. Cable coaxial.

Existen diferentes configuraciones para el cable coaxial para transmisión de señales: en banda base y banda ancha.

Banda base. Esta configuración tiene un canal que transmite un solo mensaje a muy alta velocidad. La información digital se envía de manera serial. Puede manejar una velocidad de transmisión de datos de 10 a 80 Mbps. Una de las desventajas es que posible utilizar un solo canal de la banda base, para enviar señales integradas compuestas por voz, datos o vídeo, pero una de las ventajas de este cableado es que, se puede ramificar, conectar y desconectar estaciones de trabajo sin afectar las operaciones de la red.

Banda ancha. Esta configuración porta varias señales diferentes, transmitidas en frecuencias diferentes de manera simultánea, por ejemplo las compañías de televisión por cable utilizan este tipo de cable de 75 ohms, todos los sistemas de banda ancha pueden usar un solo cable con amplificadores bidireccionales o sistemas de cable dobles. Para cualquiera de los dos casos las señales portadoras se envían a un punto central conocido como extremo de entrada (un dispositivo de traducción y transmisión) desde la cual se vuelve a transmitir a todos los puntos de la red.

El método de cable individual divide un cable mediante frecuencias para lograr una transmisión bidireccional de datos, esta división es de 6 MHz para cada trayectoria de comunicación, aunque es posible asignar 346 MHz para comunicaciones de envío (6 MHz/canal *56 canales) y 25 MHz utilizados por varios canales de banda angosta, para la trayectoria de datos de regreso (6 MHz/canal *4 canales). La figura 5.1.3.2 muestra conexiones con cable coaxial de banda ancha individual con amplificadores bidireccionales.

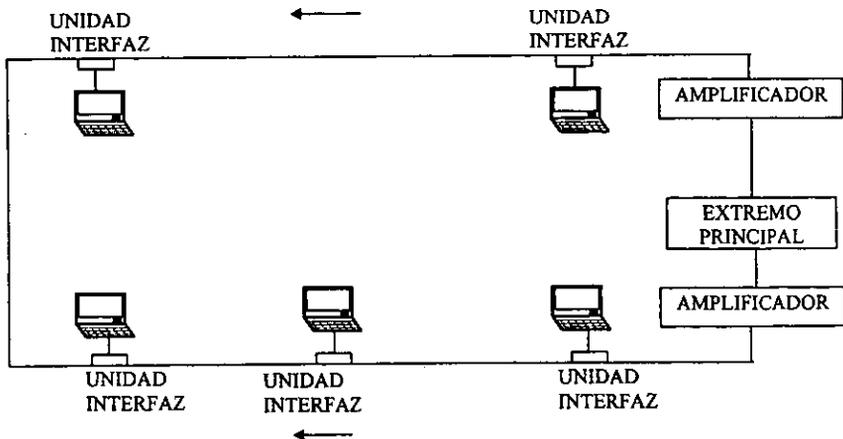


Figura 5.1.3.2. Cable coaxial de banda ancha individual con amplificadores bidireccionales.

El cable doble de banda ancha utiliza un cable para los datos de entrada que se transmiten hacia el extremo de entrada y un segundo cable conectado en circuito al extremo de entrada para los portadores de salida. Las instalaciones de cable banda ancha requieren mas planeación que las de banda base, como se transmiten señales de banda amplia, es necesario instalar

amplificadores para evitar que la señal se debilite. La figura 5.1.3.3 muestra una configuración de cable doble de banda ancha. Y la figura 5.1.3.4 muestra una configuración de cable coaxial con divisores.

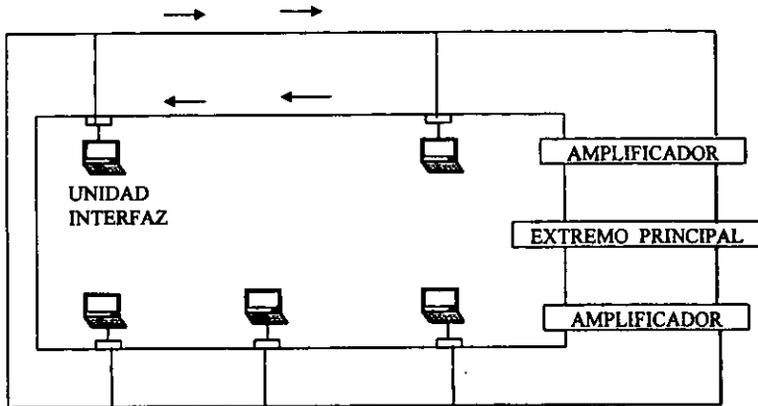


Figura 5.1.3.3. Configuración de cable doble de banda ancha.

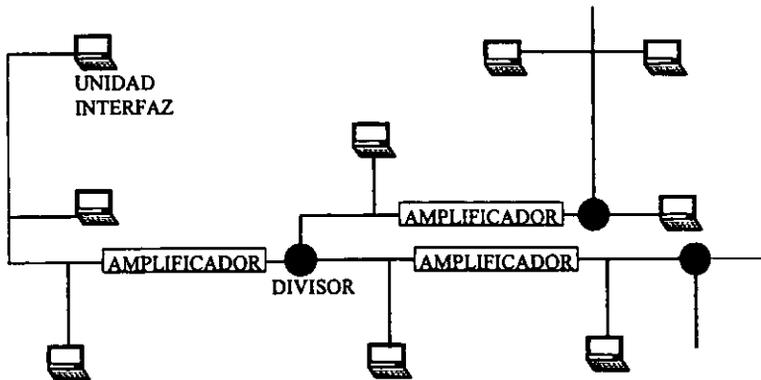


Figura 5.1.3.4. Configuración de cable coaxial con divisores.

5.1.4 CABLE DE FIBRA ÓPTICA

Un cable de fibra óptica está hecho con un núcleo de vidrio o plástico puro, estirado en tiras muy finas que forman el alma del cable, estas fibras están rodeadas por un revestimiento de vidrio el cual sirve como un espejo, que refleja la luz del núcleo. Es decir la fibra óptica está hecha por una capa de vidrio con índice de refracción menor y otra capa central de vidrio con

un índice de refracción mayor.

El cable de fibra óptica utiliza la luz para transmitir señales a través de una hebra de vidrio transparente. Las señales de las computadoras se envían a través de la fibra óptica mediante señales digitales. En un extremo del cable de fibra óptica se sitúa un diodo emisor de luz (LED) o un rayo láser y entonces un fotodetector se encargara de percibir el destello de la luz en el otro extremo, y convierte la luz en una señal eléctrica. La figura 5.1.4.1 muestra el cable de fibra óptica.

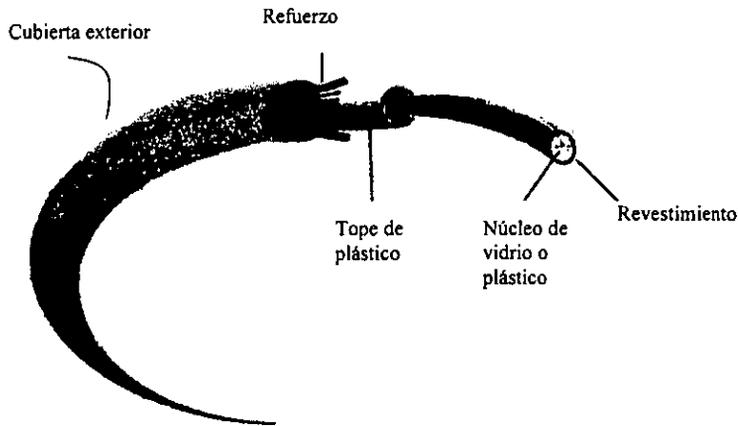


Figura 5.1.4.1. Cable de fibra óptica.

La transmisión de datos sobre fibra óptica tiene algunas ventajas sobre la transmisión de datos en cables de par trenzado y coaxial, la velocidad de transmisión de datos es mayor, el cableado es inmune a la interferencia de frecuencias de radio o electromagnética y es capaz de enviar señales a varios Km de distancia sin perder su fuerza, además de que también es inmune a la interceptación no autorizada.

Cada fibra es unidireccional, ya que un haz de luz se transmite solo en una dirección, la comunicación de doble sentido requiere de otra fibra dentro de un cable para que la luz pueda viajar en la dirección opuesta.

Cuando la luz pasa a través del núcleo, el revestimiento refleja la luz del núcleo en distinta forma dependiendo del ángulo de incidencia del rayo se tendrá un cierto tiempo de retardo en alcanzar el otro extremo del cable, aunque este retardo se mide en milmillonésimas de segundo, limita la longitud del cable a utilizar.

Los tipos de cable de fibra óptica se describen a continuación:

- **Cable de plástico:** Se utiliza en distancias de unos pocos metros. Es muy barato y también requiere componentes baratos.

- *Cable de sílice revestido de plástico*: Ofrece mayores prestaciones que el anterior y presenta un coste superior.
- *Cable de fibra monomodal de índice único*: Tiene una gran anchura de banda, pero debido a que su centro es muy diminuto hace que sea muy difícil de manejarla, además requiere de un láser en vez de un LED como fuente de señalización, lo cual es mas caro; pero brinda una longitud más extensa.
- *Cable de fibra multimodo de paso de índice*: Esta hecha de un diámetro de núcleo más grande, se usa en el entorno de redes de área local. La luz se genera a través de un LED.
- *El cable multimodo de índice gradual*: Tiene múltiples capas de vidrio que presentan una dispersión que permite aumentar su longitud. La luz se genera a través de un LED.

Las especificaciones del cable muestran los diámetros del núcleo y del revestimiento en forma de números fraccionarios. Por ejemplo, el menor tipo de cable recomendado en el diseño de FDDI es el cable de fibra óptica de 62.5/125 micras multimodo. Esto significa que el núcleo tiene 62.5 micras y el conjunto del núcleo con el revestimiento tiene un total de 125 micras.

En la actualidad, el cableado de fibra óptica se utiliza para conectar diferentes LAN's más que para conectar maquinas individuales a servidores de archivos. Esta conexión es una interconexión de alta velocidad de dispositivos de computación y también la fibra óptica puede usarse para conectar entre varias LAN's de baja velocidad.

El canal de fibra óptica es muy fácil de ampliar tanto en distancia como en numero de dispositivos en red. El protocolo de canal de fibra óptica permite hasta 16 millones de nodos en una única malla.

El canal de fibra óptica admite un alcance de red hasta 10Km. El alcance máximo de red depende del tipo de medio utilizado y la velocidad de transferencia implementada. La tabla 5.1.4.1 muestra las distancias admitidas por los diversos medios.

Velocidad de transferencia implementada	132.8 Mbps	265.6Mbps	531.25 Mbps	1.062 Gbps
Fibra monomodo	10 km	10 Km	10 Km	10 Km
Fibra multimodo de 50 micras	---	2km	1 km	---
Fibra multimodo de 62.5 micras	500m	1km	---	---
Cable coaxial	40 m	30 m	20 m	10 m
Par trenzado apantallado (STP)	100 m	50 m	---	---

TABLA. 5.1.4.1. Alcance máximo de red admitido por cada tipo de medio definido en la especificación de fibra óptica, cable coaxial y STP.

La tabla 5.1.4.2 muestra las distancias máximas permitidas entre un nodo de extremo y el concentrador raíz; observar que la distancia entre estos, varía en función del número de concentradores en cascada y el tipo de medio.

Tipo de medio	Número de concentradores entre concentrador raíz y nodo extremo.	Número de niveles en la red.	Distancias máximas recomendadas entre concentrador raíz y nodo extremo.
Categoría 3	1	2	100 m
Categoría 3	2	3	75 m
Categoría 3	3	4	50 m
Categoría 3	4	5	25 m
Categoría 5	1	2	200 m
Categoría 5	2	3	150 m
Categoría 5	3	4	100 m
Categoría 5	4	5	50 m
Fibra óptica	1	2	4 km
Fibra óptica	2	3	3 km
Fibra óptica	3	4	2 km

Tabla 5.1.4.2. Distancias máximas permitidas entre un nodo de extremo y el concentrador raíz.

La norma IEEE 802.3, recomienda que el número máximo de niveles de concentradores en cascada es tres, para condiciones óptimas, sin embargo algunas redes emplean hasta 5 niveles, pero obviamente el alcance de las señales es menor.

El cable de categoría 5, de acuerdo con EIA/TIA esta especificado para trabajar a 100 Mhz, el cable de categoría 4 esta especificado para redes que trabajan a 16 Mbps, la categoría 3 esta especificado para trabajar con redes Token Ring o Ethernet 10BASE-T a 4 Mbps.

Algunos tipos de conectores para fibra óptica se muestran en las figuras 5.1.4.2. y 5.1.4.3. El adaptador ST para fibra óptica tiene al final dos conectores ST. El conector ST es usado como sistema de cerradura bayoneta. Simplemente hay que presionar y dar un cuarto de giro a este, para fijar el conector. La limpieza de la fibra óptica es muy fácil.

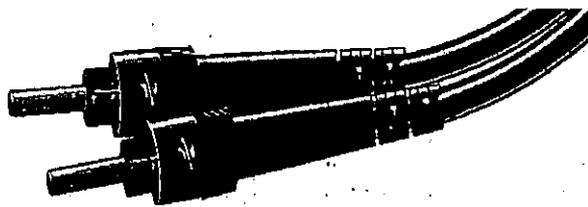


Figura 5.1.4.2. Conector para fibra óptica con terminales ST- ST.

El adaptador SC para fibra óptica contiene al final dos conectores SC. El conector SC contiene una pequeña cerradura, que al presionar el conector se escucha un audible click, para asegurarnos que la fibra está bien conectada.

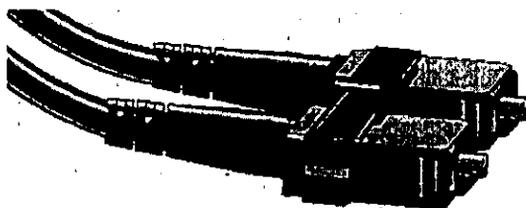


Figura 5.1.4.3. Conector para fibra óptica con terminales SC – SC.

5.1.5 GUÍAS DE ONDA

Las guías de onda, formadas por un tubo de sección rectangular o circular, que confinan las ondas electromagnéticas para obtener una atenuación muy inferior a la que se tendría con la propagación en el espacio libre, se pueden usar también como medio de transmisión a distancias considerables.

5.1.6 RADIO

Las ondas de radio fueron el primer medio utilizado para transmitir información y, gracias a los avances tecnológicos como la telefonía celular y el auge de los equipos portátiles, se están convirtiendo en uno de los medios de transmisión más utilizados en la actualidad.

5.1.7 LUZ

La luz se utilizó aún antes que la radio para transmitir información, los griegos ya utilizaban espejos para comunicarse con sus barcos en el mar. Hoy día ha sido necesario mejorar los sistemas de producción de luz láser para permitir transmitir información electrónica con velocidades similares a la de los cables. Ahora es posible establecer enlaces de varios kilómetros a varias decenas de Mbits/seg.

5.1.8 MICROONDAS

Las microondas están localizadas en el rango de frecuencias sobre 1000 MHz y los 1.3 GHz. Una típica microonda de horno tiene un tubo de electrones a 2.45 GHz suficiente para quemar. Los sistemas de comunicaciones de microondas pueden transmitir a través del aire, espacio abierto, estas son ampliamente usadas para transmitir frecuencias que van desde 2 hasta 25 GHz, con los grandes anchos de banda usados en redes privadas.

La transmisión de microondas es usada cuando se dificulta o es inadecuado tender cables entre dos puntos por ejemplo:

- Enlaces entre los satélites y la tierra.
- Enlaces entre dos edificios en una área metropolitana.
- Enlaces a través de amplias áreas abiertas en donde es impráctico tender el cable, así como desiertos, pantanos y grandes lagos.

Los sistemas de microondas consisten en dos antenas direccionales, en las cuales se emiten ondas radiadas de energía que esta enfocada de un punto, en un extremo, hasta otro punto, en el otro extremo. En las configuraciones punto a punto, las antenas deben de estar alineadas siguiendo la línea de la señal.

5.1.9 MODEMS

Los módems (moduladores/demoduladores) son dispositivos de equipos de comunicación de datos (Equipment Communication Data, DCE) que proporciona conexiones para computadoras sobre la red telefónica pública conmutada. Los módems convierten (modulan) las señales digitales de computadoras en señales analógicas que se pueden transmitir a lo largo de líneas telefónicas. Un módem en el otro extremo de enlace demodula la señal convirtiéndola de nuevo a bits digitales.

Ambos módems deben de usar técnicas de comunicación compatibles que cumplan varias normas, las más notables son las de la serie V del CCITT (ITU). Otras normativas de módem incluyen el protocolo de conexión de red Microcom (Microcom Networking Protocol, MNP). La conexión desde la computadora al módem típicamente es cable serial RS-232 y la conexión desde el módem al contacto telefónico de pared es mediante conectores RJ-11C. Los módem para computadoras están disponibles en modelos internos y externos. Un módem interno es una placa de circuito o adaptador que se ajusta a una ranura (slot) de una computadora y se conecta a su puerto de comunicación serie.

Cuando un módem "llama" a otro, el módem destino contesta y tiene lugar a un intercambio de señal, que establece los parámetros para una sesión de comunicación. El proceso de comunicación se negocia. El proceso de negociación determina la velocidad de señalización disponibles entre los módems así como el uso de compresión. El uso de líneas telefónicas impone algunas restricciones en la velocidad de transferencia de datos.

Las técnicas de codificación y compresión ayudan a aumentar el rendimiento hasta un rango de 28,800 bits/seg.

MÓDEMS de alta velocidad

Los módems de alta velocidad son aquellos que logran velocidades de bits superiores a 2400 bps.

Las normas más importantes del CCITT (ITU) son:

V.22	Norma de módem dúplex a 1200 bits/seg.
V.22bis	Norma de módems dúplex a 2400 bits/seg.
V.28	Definición de circuitos en la interfaz RS-232.
V.32	Norma asíncrona y síncrona a 4800/9600 bits/seg.
V.32bis	Norma asíncrona y síncrona de hasta 14,400 bits/seg.
V.35	Definición de velocidades altas de datos, sobre circuitos combinados.
V.42	Define las normas de verificaciones de errores.
V.42 bis	Define compresión de módems.
V.32 turbo	Una norma que proporciona velocidades de 19.2 Kbits/seg.
V.34	Una norma para velocidades de transmisión de 28 Kbits/seg.

V.34+ La superación de V.34 alcanza a 33.6 KBits/seg.

Mientras que los estándares definen el tope de las velocidades, el ruido en la línea, la distancia y la topología de los sistemas de conmutación entre los módems pueden ser mas bajas que la actual velocidad de datos que soportan los módems.

56K módems

Este estándar de módem esta tomando ventaja de una técnica que puede proveer velocidades de datos hasta 56 kbit/seg. Para módems de usuarios. U.S. Robotics (nueva parte de 3Com) llama a esta tecnología "X" y Lcent/ Rockwell Semiconductor Systems la llama tecnología K56flex. Solamente hay diferencia entre los conceptos y no en las tecnologías.

Los módems 56K están diseñados para realizar tareas pesadas de usuarios de Internet.

5.2 CABLEADO ESTRUCTURADO

5.2.1 HISTORIA DE LOS SISTEMAS DE CABLEADO

Los sistemas de cableado utilizados para servicios de telecomunicaciones, han evolucionado a través de los años. En un principio los sistemas de cableado para teléfonos fueron especificados e instalados por las propias compañías, mientras que el cableado para datos estaba determinado por los proveedores del equipo de computación, hasta que la Asociación de Ingenieros Eléctricos y la Asociación de Ingenieros en Telecomunicaciones (EIA/TIA) desarrollaron la norma 568 para el cableado de telecomunicaciones en edificios comerciales que define las distancias, las tipologías y especificaciones físicas para cablear sin conocer los ECD que lo utilizaran.

Anteriormente el único cable que se utilizaba para redes era el tipo POTS (Plain Old Telephone System) ó cable regular para teléfono que sólo manejaba comunicaciones de voz pero que necesitaba de un segundo sistema de cables para apoyar las comunicaciones de datos.

5.2.2 COMPONENTES BÁSICOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO

El cableado estructurado, planifica la distribución de una red pensando en el crecimiento de está. Un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar múltiples sistemas de computación y telefonía independientemente de quien fabricó los componentes del mismo, además proporciona un medio para la transmisión de datos, audio, vídeo, en donde cada estación de trabajo se conecta a un punto central, utilizando una topología estrella facilitando la interconexión y la administración del sistema, éste incluye cables, bases, conectores, baluns (equilibrados y no equilibrados), sistema de paneles de parcheo y componentes electrónicos. La figura 5.2.2.1 muestra un ejemplo de un sistema de cableado estructurado básico, que consta de:

1. Ensamblajes para conexiones provisionales de cables.
2. Salidas de información.
3. Cableado vertical.
4. Cableado horizontal.
5. Productos para interconexión.
6. Cable principal.
7. Conectores y bases.
8. Cableado paralelo.
9. Cableado cruzado.

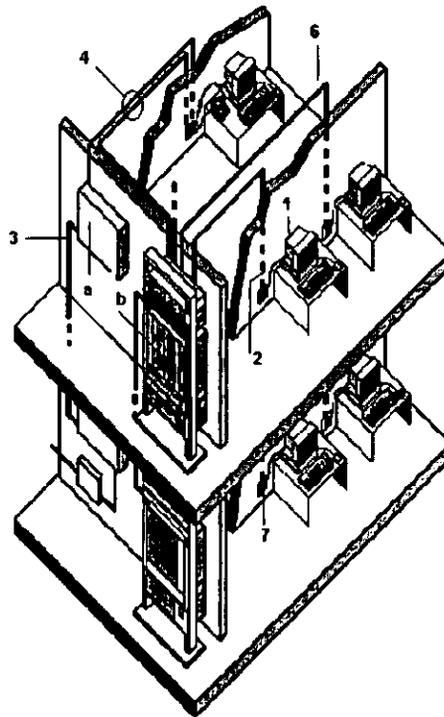
Ensamblajes para conexiones provisionales de cables:

Interconectan a los puertos del panel conmutador, y/o conectan estaciones de trabajo, a las salidas de información ("outlets").

Salidas de información:

Son los puntos de terminación para los cables que conectan a las estaciones de trabajo y se clasifican de acuerdo al lugar físico de instalación como:

- Montaje empotrado o embutido.
- Montaje sobre la superficie.
- Mueble modular.
- Piso elevado o que atraviesa.
- Número de puertos por salida.
- Tipo de conectores requeridos.



- a) Armario de cableado.
b) Armario de distribución.

Figura 5.2.2.1. Sistema de cableado estructurado básico.

Cableado vertical:

Es el cable que parte desde el armario de cableado de cada planta al equipo principal alojado en el sótano o en la primera planta del edificio. Como se puede ver en la figura 5.2.2.1 en un sistema de cableado estructurado básico o en la figura 5.2.2.2 que muestra el cableado estructurado vertical independiente.

Cableado horizontal:

Es el cable que parte desde un armario de distribución de cableado al equipo periférico de red como: estaciones de trabajo, impresoras, servidores, ruteadores, etc. Como se puede ver en la figura 5.2.2.1 en un sistema de cableado estructurado básico o en la figura 5.2.2.3 que muestra el cableado estructurado horizontal independiente.

Diagrama Cableado Estructurado Vertical

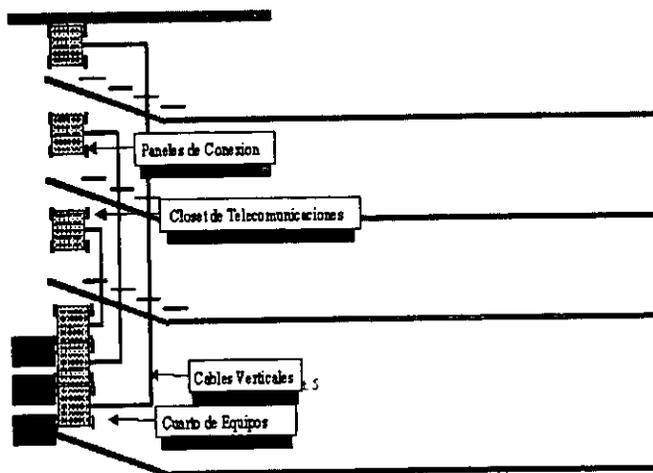


Figura 5.2.2.2. Diagrama de un cableado estructurado vertical.

Productos para interconexión:

Existen dos tipos de equipo para interconectar los "patch panels" (paneles conmutadores) y los "puch down" (bloques con perforaciones).

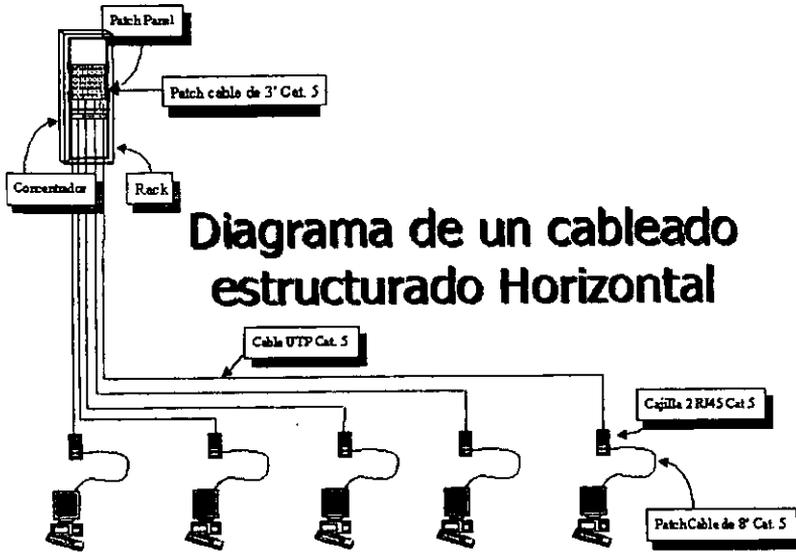


Diagrama de un cableado estructurado Horizontal

Figura 5.2.2.3. Diagrama de un cableado estructurado horizontal.

La figura 5.2.2.4 muestra un conjunto de computadoras conectadas a través de un sistema de cableado horizontal a un panel modular de conectores, en donde los cables de la parte frontal del panel se conectan a dispositivos de red, tales como: concentradores, ruteadores, estaciones de trabajo, servidores etc.

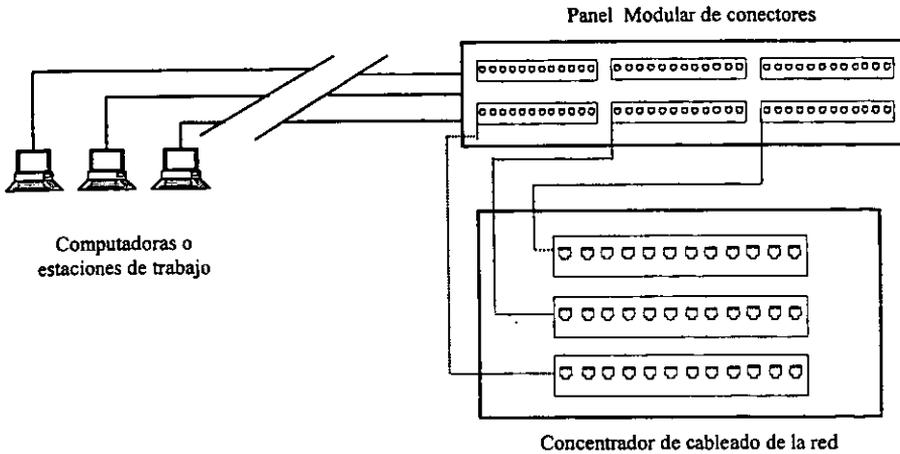


Figura 5.2.2.4. Sistema de cableado horizontal.

Cable principal:

Es el cable que parte del punto principal de distribución y se interconecta con todas las salidas de telecomunicaciones.

Conectores y base:

La figura 5.2.2.5 muestra el enchufe de pared y conectores de cableado para sistemas de categoría 5. La figura a) muestra el enchufe de pared que protege a la clavija de conexión cuando el cable no está conectado, además dispone de conectores para teléfono y datos, este último que va hacia la computadora y la figura b) muestra las dos formas de conexión para clavijas de 8 patillas.

Existen dos configuraciones de 8 patillas para los conectores de cableado; la configuración "T568A" (más usual) y la "T568B".

La norma EIA/TIA 568 establece el uso de cuatro pares trenzados por cable para las necesidades actuales como futuras de las redes y aplicaciones en telecomunicaciones.

Par 1: Blanco con franja azul / azul (BA / A).

Par 2: Blanco con franja naranja / naranja (BN / N).

Par 3: Blanco con franja verde / verde (BV / V).

Par 4: Blanco con franja café / café (BC / C).

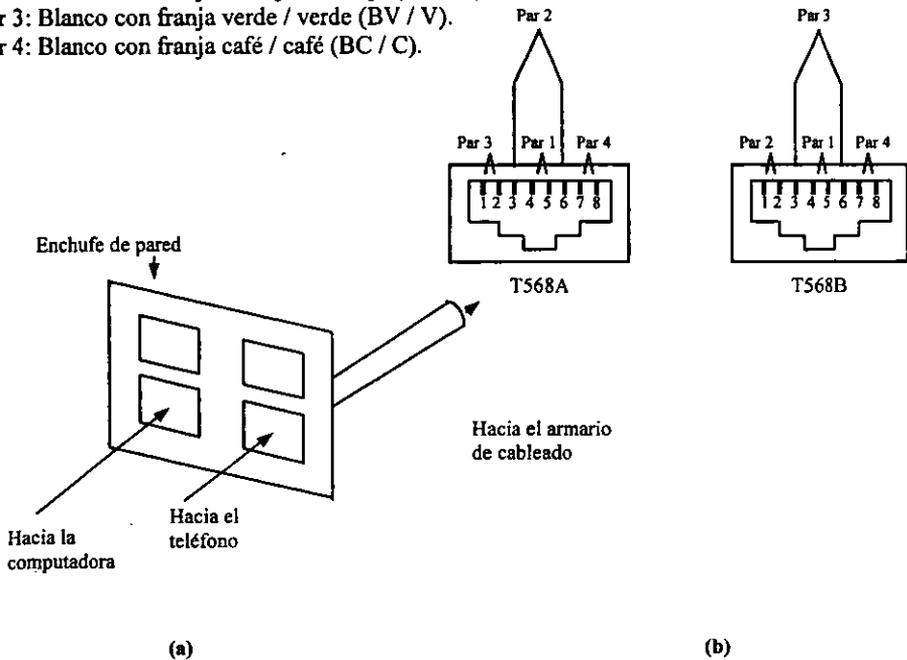


Figura 5.2.2.5. (a) Enchufe de pared (b) conectores de cableado para sistemas de categoría 5.

Cableado paralelo:

Es la conexión uno a uno entre la base y el conector RJ-45 categoría 5, como se muestra en la figura 5.2.2.6.

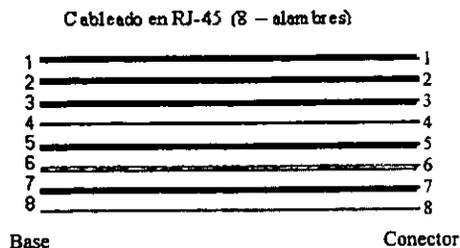


Figura 5.2.2.6. Cableado paralelo.

Cableado cruzado:

Es la conexión cruzada entre la base y el conector RJ-45 categoría 5, o sea que se conectan la patilla 1 de la base con la patilla 8 del conector RJ-45, la patilla 2 con la patilla 7 y así sucesivamente, como se muestra en la figura 5.2.2.7.

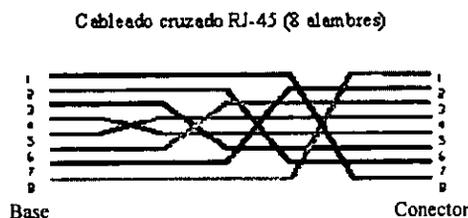


Figura 5.2.2.7. Cableado cruzado.

5.2.3 CAUSAS COMUNES DE ERRORES EN UNA RED

- Mal funcionamiento del concentrador principal.
- Mal funcionamiento de la tarjeta de interfaz de red.
- Falsos contactos del cable de red en los conectores o bases.
- Mal distribución de los hilos en los conectores o bases.
- Proximidad al cable de red de otros circuitos eléctricos.
- Diafonía.

5.2.4 DIAFONÍA O NEXT

Es la corrupción de la información producida por interferencias electromagnéticas causadas por tendidos de cableado, aparatos eléctricos, bucles (madejas) cercanos al cable de red.

5.2.5 PARES DIVIDIDOS

Es la fuga de información de un hilo a otro (pareado incorrecto) o sea que un hilo va trenzado con otro que no le corresponde.

5.2.6 ANCHO DE BANDA UTILIZABLE

La variedad de velocidad en la transmisión de los datos que un sistema de cableado puede aceptar, se conoce como el ancho de banda utilizable que depende del comportamiento eléctrico de los componentes del sistema de cableado.

5.2.7 APLICACIONES DEL CABLEADO ESTRUCTURADO

Las aplicaciones de cableado estructurado pueden ser desde telecomunicaciones básicas hasta sistemas de vídeo sofisticado como pueden ser:

- Servicios de telecomunicaciones que pueden ser transportadas por las líneas telefónicas como voz, fax, módem, etc.
- Conectividad a "Mainframes" y a minicomputadoras.
- Interconexión a redes (LAN's) y la conexión en red del equipo de computo para optimizar los recursos.

5.2.8 LINEAMIENTOS DEL CABLEADO ESTRUCTURADO

El cableado estructurado debe de tener los siguientes lineamientos:

- Estandarización.
- Orden.
- Rendimiento.
- Durabilidad.
- Documentación.
- Integridad.
- Crecimiento por etapas.
- Facilidad de expansión.

5.2.9 COSTO BENEFICIO DE HACER EL CABLEADO SÓLO UNA VEZ CON UN SISTEMA DE CABLEADO ESTRUCTURADO

El costo inicial de un sistema de cableado estructurado puede resultar un poco más caro pero requerirá menos actualizaciones por lo que garantiza que la inversión hecha representa a mediano y a largo plazo un costo/beneficio altamente rentable además de que puede soportar tecnologías de punta actual y futuras. Por esto es importante analizar los siguientes puntos:

- Características de los Productos. Considerar como se adaptan los componentes físicamente al lugar de instalación, hasta las características particulares que un producto ofrece.
- Requisitos Físicos del lugar de Instalación. Los productos seleccionados deben de cumplir con los requisitos físicos del lugar de instalación.
- Opciones del Equipo para Interconexiones. El equipo para interconexión puede variar ampliamente, dependiendo del tipo de medio utilizado, facilidad de uso y tamaño que se necesita.
- Identificación / Codificación con Cables de Color. Facilita la administración del sistema.
- Estilos de Terminación. Se encuentra disponible una variedad de estilos de terminación, los que dependen de la elección del cable utilizado y de la selección del equipo donde se conectan.
- Medios. Se pueden elegir cables tipo “plenum” o “non-plenum”, los que presentan un tipo de medios o la combinación de muchos de ellos bajo una misma cubierta.

Esta tecnología se aplica en cualquier tipo de edificio (comercial o residencial) y/o entre edificios, su diseño es principalmente para transmitir voz (analógica y digital), datos a baja y alta velocidad, imagen, vídeo, control, sistemas de seguridad, sistemas de flujo, sistemas de alarma etc. Los principales objetivos de tener un sistema de cableado estructurado son:

- Eliminar segmentos de red.
- Proveer rutas lógicas de acceso a datos (enlaces virtuales, Virtual Links VL).
- Asegurar los requerimientos físicos de comunicación.
- Simplificar instalaciones adicionales, movimientos y cambios.
- Rápida solución de problemas e identificación de fallas.
- Fácil administración de la red y subredes.
- Solución al sistema de cableado en forma integral.

5.3 HARDWARE

El Hardware es básicamente los componentes que se encuentran en la mayoría de las redes como son las tarjetas de interfaz para red (Network Interface Card, NIC), transeptores, repetidores, estaciones de trabajo, servidores, concentradores de cableado (HUB's), puentes (bridges), encaminadores (ruteadores), compuertas (gateway), switches, equipos híbridos hardware de respaldo, suministradores continuos de energía ("No-Breaks") o sistemas de alimentación ininterrumpida (UPS) y las impresoras de red.

5.3.1 ESTACIÓN DE TRABAJO INDIVIDUAL EN RED

Cada microcomputadora conectada a la red debe de conservar la capacidad de funcionar de manera independiente con su propio software, al mismo tiempo las computadoras se convierten en estaciones de trabajo en red con acceso a la información contenida en el servidor de archivos, esta capacidad de funcionar como una estación en red requiere una tarjeta interfaz, esta tarjeta se inserta en una de las ranuras de expansión de las microcomputadoras, de esta tarjeta sale un cable que la conecta a la red. El programa de redes funciona en conjunto con el sistema operativo de discos, al ejecutar el programa de software de la red y al registrar la entrada de un usuario de la red por medio de una identificación de usuario y una contraseña, una vez hecho esto el usuario puede hacer uso de los recursos de la red.

5.3.2 SERVIDORES

Algunas de las primeras LAN utilizaban un servidor con discos duros, con información para compartirla con las estaciones de trabajo de la red, las estaciones de trabajo individuales manejan el servidor de discos como si fuera una unidad de discos adicional, la estación de trabajo accesa la unidad de la red exactamente de la misma manera como lo haría con sus propias unidades de disco al almacenar archivos, pero el procedimiento se puede complicar cuando una estación de trabajo desea acceder un archivo específico que se encuentra en el servidor de discos. Por lo que algunas PC's que utilizan el DOS, emplean una tabla de localización de archivos (File allocation Table, FAT) para almacenar donde se encuentra almacenado un archivo en particular.

El servidor de discos de red lleva su propia tabla de localización de archivos (FAT) y envía una copia a cada estación de trabajo, cada una de ellas almacena la copia en RAM. Con el servidor de discos la integridad de la FAT se mantiene al dividir (o hacer la partición de) esta unidad de disco duro en varios volúmenes de usuario, cada volumen se reserva para uso exclusivo de una estación de trabajo específica con objeto de preservar la integridad de la FAT de ese volumen en particular, aunque es posible que ciertos volúmenes sean designados como volúmenes públicos de solo lectura, para garantizar su integridad; las estaciones de trabajo individuales pueden consultar esa información pero no pueden modificarla.

La figura 5.3.2.1 muestra estaciones de trabajo conectadas con tarjetas de interfaz de red y cables a un servidor de archivos.

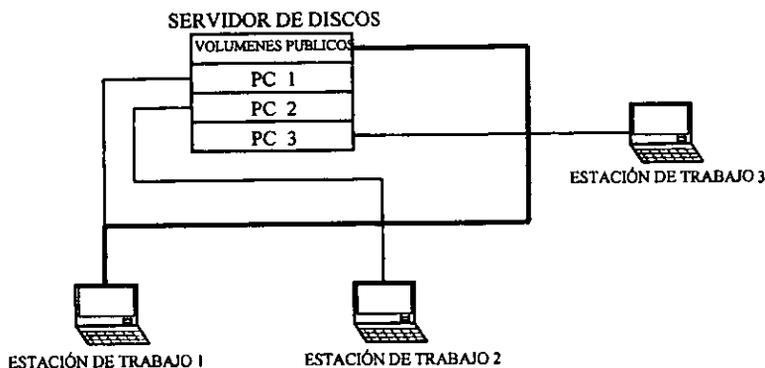


Figura 5.3.2.1. Estaciones de trabajo conectadas con tarjetas de interfaz de red y cables a un servidor de archivos.

5.3.3 SERVIDOR CENTRALIZADO

Para las redes de oficinas pequeñas un solo servidor de archivos es más que suficiente, a este se le llama servidor centralizado y funciona como minicomputadora, una unidad maneja todo el servicio de archivos y cada estación de trabajo espera su turno, si la LAN está diseñada para manejar varios departamentos diferentes o simplemente si se trata de un área más grande, entonces por regla general es mejor añadir más servidores de archivos a la red.

5.3.4 SERVIDORES DE ARCHIVOS

Los servidores de archivos son mucho más eficientes y complejos que los servidores de discos, un servidor de archivos contiene software que forma una protección alrededor del sistema operativo de discos normal de la computadora, esta protección de software filtra los comandos hacia el servidor de archivos antes de que el sistema operativo pueda recibirlos, este servidor cuenta con un sistema de archivos propio, cuando una estación de trabajo solicita un archivo específico, el servidor de archivos lo envía directamente a esa estación de trabajo, esta estación de trabajo no identifica al servidor de archivos como otra unidad de disco, como en el caso del servidor de discos. La estación de trabajo lleva una tabla de conexión de unidades mapeadas designadas de manera lógica que indican la ubicación de los diferentes directorios del sistema de archivos del servidor de archivos, el usuario solicita un archivo y el servidor de archivos responde enviando dicho archivo.

Además también es más eficiente debido a que no necesita enviar copias de la FAT a cada

estación de trabajo que solicita un archivo y también ya no es necesario dividir la unidad de disco duro de la red en volúmenes, debido a que las estaciones de trabajo individuales ya no necesitan preocuparse acerca de donde reside un archivo específico. Para la selección del servidor de archivos se requiere conocer que clase de potencia de procesamiento se requiere, por ejemplo, si se está utilizando un microprocesador 80486 de Intel a 33 MHz y no satisface las necesidades de procesamiento, entonces lo más conveniente sería cambiar a un 80486 a 100 MHz, y si los requerimientos de entrada/salida fueran más intensos, sería necesario cambiar el servidor de archivos basado en un procesador Pentium con capacidad de procesamiento mayor.

5.3.5 SERVIDORES DE ARCHIVOS DISTRIBUIDOS

Estas unidades adicionales se conocen como servidores de archivos distribuidos, por que dividen o distribuyen las tareas de servicio de archivos de toda la red; por ejemplo si todas las estaciones de trabajo de un departamento usan los mismos programas y tienen acceso a los mismos datos, sería muy ineficiente enviar esta información a un servidor de archivos que se encuentre a una distancia considerable, entonces un servidor de archivos distribuido ubicado en ese departamento puede aumentar la rapidez de acceso y reducir la carga en el resto de la red, este proporciona una velocidad óptima al resto de los usuarios de la red.

Los servidores de archivos distribuidos tienen otra ventaja, si un servidor de archivos deja de funcionar, las LAN's no necesariamente interrumpen su trabajo, si no que otro servidor de archivos distribuido (siempre y cuando se tenga espacio suficiente) puede dar servicio temporal a toda la LAN, mientras que los servidores de archivos distribuidos pueden proporcionar varias ventajas también pueden dificultar las tareas de seguridad, por lo que el administrador de la red debe asegurarse de que todas las unidades de disco duro de los servidores de archivos estén protegidos contra el acceso no autorizado. La figura 5.3.5.1 muestra el esquema de una conexión de estaciones de trabajo a un servidor de archivos.

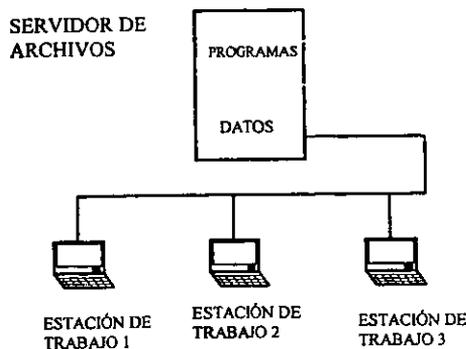


Figura 5.3.5.1. Estaciones de trabajo conectadas a un servidor de archivos.

5.3.6 SERVIDOR DE ARCHIVOS DEDICADO

El servidor de archivos dedicado es una microcomputadora con una unidad de disco duro que se usa exclusivamente como servidor de archivos, al dedicar todos sus recursos de procesamiento y de memoria al servicio de archivos, la computadora especial puede ofrecer mayor velocidad y eficiencia a la red.

5.3.7 SERVIDOR DE ARCHIVOS NO DEDICADO

El servidor de archivos no dedicado es una computadora que se utiliza como estación de trabajo además de funcionar como servidor de archivos, esto significa que la memoria RAM debe dividirse; para que una parte quede disponible para ejecutar programas, también significa que una estación de trabajo de la red quizá tenga que esperar el envío de un archivo mientras el usuario del servidor de archivos carga programas de la memoria utilizando el microprocesador de la máquina. Los servidores de archivos son por lo general las computadoras más rápidas y más caras de la red, es difícil decidirse en especializar la unidad o no (o sea utilizarla como dedicada o no), debido a que el dinero que podría ahorrarse haciendo que la máquina fuera no dedicada se pierde muchas veces, por degradación de la LAN completa. Por lo general un servidor de archivos centralizado para más de tres o cuatro estaciones de trabajo debe ser dedicado.

En una red de punto a punto los usuarios determinan que recursos de cómputo compartir con otros usuarios de la red, donde un usuario puede desear compartir su unidad de disco duro como servidor de archivos para otros usuarios de la red.

5.3.8 SERVIDOR DE IMPRESIÓN

Al igual que un servidor de archivos permite compartir una sola unidad de disco duro de la red, un servidor de impresión de la red hace posible que docenas de estaciones de trabajo compartan varios tipos de impresoras. Con una LAN y el software del servidor de impresión, se puede elegir cualquiera de las impresoras de la red.

Un servidor de impresión de red puede ser una microcomputadora dedicada que solo ejecute el software de impresión o puede ser una sección de software que se ejecute en el servidor de archivos de la red, existen diversas tarjetas para instalar en las impresoras para acelerar el proceso de impresión de la red, estas impresoras pueden recibir datos de la red a una frecuencia de varios millones de bits por segundo, son útiles para imprimir archivos gráficos extensos que tienen tantos datos que pueden obstruir el tráfico de la red mientras imprimen.

El uso de software de servidor de impresión no significa que una estación de trabajo no pueda tener su propia impresora dedicada. El administrador de la red cuando instala un programa en la red también debe de instalar un controlador de impresión por omisión, esto

significa que los archivos de los programas se imprimen en una impresora específica. El software para compartir impresoras debe de contener un integrador de impresión (print spooler) un tipo de software que crea una memoria temporal para almacenar las tareas de impresión mientras esperan su turno (en cola de espera), los integradores complejos tienen capacidades adicionales, incluyendo el traslado de un trabajo al inicio de la cola de impresión.

Existen otros servidores que pueden formar parte de una red como los servidores de fax, aunque un servidor de archivos de alto desempeño puede actuar también como un servidor de fax, servidor de comunicaciones y servidor de base de datos.

5.3.9 SISTEMAS DE RESPALDO DE RED

Los sistemas de respaldo de cartucho de un cuarto de pulgada son los más comunes, baratos y confiables, también existen cartuchos de cinta magnética digital de 4mm y 8mm, para el registro sonoro. Estas unidades pueden almacenar hasta 8GB de datos comprimidos, si esto se combina con un auto cambiador de 6 cartuchos, entonces la capacidad de almacenamiento disponible sería de 48GB. Los subsistemas de administración de almacenamiento (Storage Management Subsystem, SMS), almacenan en medios más baratos y de manera automática los archivos que no se usan y luego los recuperan cuando son necesarios.

Los arreglos redundantes de discos, son la solución en sistemas de respaldo en redes LAN. Los arreglos redundantes de discos, pueden implementarse a nivel de hardware (más eficientes) o software. Estos constan de múltiples unidades de disco que se usan en paralelo.

5.4 EQUIPOS DE INTERCONEXIÓN

Los equipos de interconexión son aquellos que nos sirven para conectar computadoras a una red de computadoras o para enlazar una red con otra. Algunos de ellos se mencionan a continuación.

5.4.1 TARJETAS ADAPTADORAS DE RED

La tarjeta adaptadora de red NIC/MAU Network Interface Card (Tarjeta de interfaz de red) ó Medium Access Unit (unidad de acceso al medio). Es el dispositivo que conecta la estación (ordenador u otro equipo de red) con el medio físico.

Las tarjetas de interfaz son de muy bajo precio y fáciles de conseguir pero tienen algunas características que las diferencian. Estas tarjetas vienen acompañadas con programas de software para configurarlas. Existen tarjetas de 16 y 32 bits aunque las de 16 son más lentas para el desempeño de un servidor de archivos y la de 32 bits lo mejoran considerablemente.

Otra de las características de estas tarjetas, es que el software que hace que el envío de

mensajes en la red sea mas seguro. Además en ocasiones la información que puede usarse como parte de la administración general de la red.

Los administradores de red que contienen medios combinados, como 10BaseT y cable coaxial delgado usan tarjetas que contienen múltiples interfaces para diferentes medios llamadas tarjetas "Combo". La ventaja de este tipo de tarjetas que pueden usarse en diferentes segmentos de la red sin contar con los diferentes tipos de medios que se encuentran en estos segmentos.

5.4.2 TRANSCEPTORES

A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico con la tarjeta de interfaz de red, bien porque no sea posible la conexión directa o porque el medio sea distinto del que utiliza la tarjeta.

5.4.3 REPETIDORES

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella aplican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio. La figura 5.4.3.1 muestra la interconexión de dos repetidores.

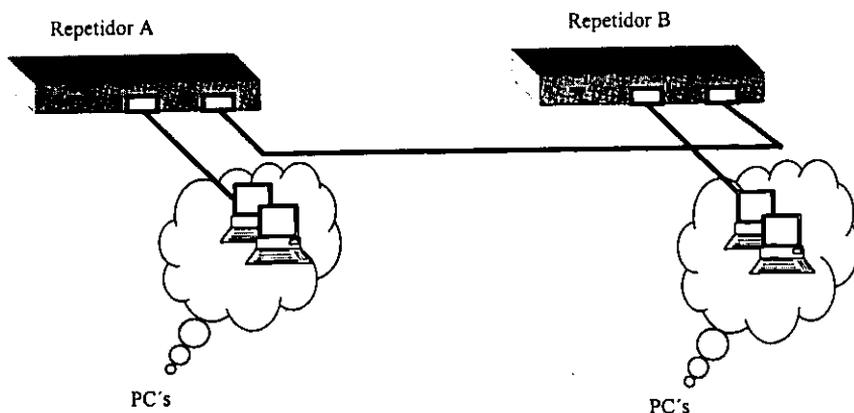


Figura 5.4.3.1. Interconexión de dos repetidores.

5.4.4 CONCENTRADORES DE CABLEADO DE REDES (HUB's)

Los concentradores de cableado son dispositivos que centralizan los cables procedentes de las estaciones y estructuran el cableado de una red para facilitar su manejo, la topología Token Ring fue la primera en utilizar este tipo de métodos de cableado y la Ethernet conocida como 10BaseT. Con el concentrador de cableado pueden manejar varias PC acomodadas en varios pisos, si un empleado se traslada de un departamento a otro, no es necesario volver a instalar el cableado de la LAN, en lugar de eso, lo único que cambia es la PC con su tarjeta de interfaz de red y se conecta a un conector de cableado, en el concentrador de cableado, el cable de esa PC solo se conecta en una parte diferente de concentrador.

Otra de las ventajas del concentrador de cableado es que puede manejar tarjetas de interfaz de red defectuosas de tal manera que no interfieran con la red. Un concentrador de cableado puede identificar el mal funcionamiento de una tarjeta de interfaz de red de una PC, entonces puede redirigir la trayectoria del envío de datos de manera que las otras PC de la red no reciban las señales generadas por la unidad defectuosa. La figura 5.4.4.1 muestra la forma de conexión de un concentrador 10BaseT.

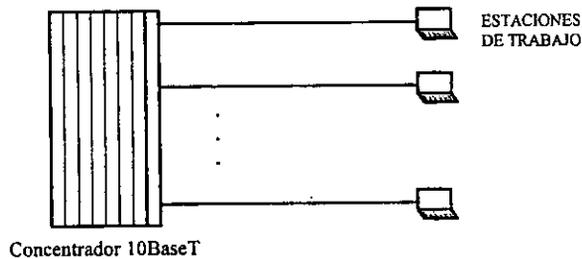


Figura 5.4.4.1. PC's de una LAN al concentrador.

Además existen los concentradores de cableado inteligentes que tienen la misma funcionalidad que los HUBS, pero además contienen "inteligencia" integrada para comunicar información de administración de la red a un paquete de software, esto hace posible que un administrador de red pueda manejar y controlar todas las funciones del concentrador, permite para el caso de las redes grandes que pueden tener cientos de nodos, múltiples redes LAN y ver toda la actividad de la red en una sola pantalla.

Para la selección de los concentradores inteligentes, se debe de saber a que topología de red se da soporte, si es posible interconectar redes en el concentrador; o sea, que LAN de diferentes tipos requieran la capacidad de rutear ó puentear paquetes a través de toda la red. También se requiere conocer si existen concentradores de cableado capaces de enviar información de una macrocomputadora SNA a las LAN manejadas en sus concentradores de cableado. Además de

cuantas LAN pueden manejar los concentradores y por último dentro de lo más importante, las PC's conectadas al concentrador de la LAN requieren un ancho de banda dedicado.

5.4.5 PUENTES Ó BRIDGES

Son equipos que unen dos redes LAN orientadas a paquetes iguales o distintas. Actúa sobre los protocolos de bajo nivel, opera en el nivel de enlace de datos en el control de acceso al medio del modelo OSI. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los puentes transmiten las señales, con lo cual no se envía ruido a través de ellos.

5.4.6 ENCAMINADORES Ó ENRUTADORES

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que el de los puentes pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

5.4.7 SERVIDOR DE COMUNICACIONES O COMPUERTAS (GATEWAYS)

Debido a que las grandes computadoras no ejecutan los mismos sistemas operativos que las microcomputadoras, es necesario realizar un proceso de traducción entre la microcomputadora y la mini/macrocomputadora, esto permite la comunicación entre las microcomputadoras y las computadoras más grandes, esta traducción puede ser manejada por cada microcomputadora o por un servidor de comunicaciones de la red, también llamado compuerta (GATEWAY), un servidor de comunicaciones de red puede permitir a muchas computadoras comunicarse con una sola mini/macrocomputadora, los servidores de compuerta permiten el fácil acceso a los datos de las macrocomputadoras y solo requieren un servidor de archivos que ejecute el software especializado.

Estos equipos interconectan redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación, que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicaciones, ni formatos de las estructuras de datos. Modifica el empaquetamiento de la información o su sintaxis para acomodarse al sistema distinto. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos. Las compuertas (gateways) trabajan en el nivel de aplicación del modelo de referencia OSI.

5.4.8 SERVIDOR DE COMUNICACIÓN ASÍNCRONA

Para que usuarios de redes de área local tengan acceso a computadoras externas y estos tengan acceso a la LAN se necesita un servidor de comunicaciones asíncrona, el servicio de entrada de llamadas telefónicas mediante estos servidores hace posible que un gran número de usuarios remotos se conecten con la red como si fueran usuarios locales. El servicio de salida de llamadas telefónicas permite que los usuarios locales de la LAN compartan recursos de comunicaciones, como módem; en una forma mucho más eficiente, en lugar de darle a cada usuario un módem que permanezca inactivo mucho tiempo durante el día.

La figura 5.4.8.1 muestra un servidor de comunicaciones asíncrona.

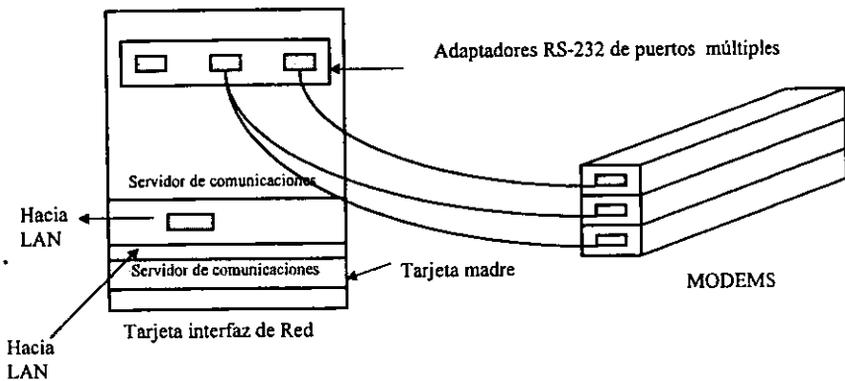


Figura 5.4.8.1. Servidor de comunicaciones asíncrona.

Para la selección de un servidor de comunicaciones asíncrono se deben de tomar en cuenta algunas consideraciones como: que software opera en el servidor, y si es compatible con el sistema operativo de red de la LAN.

También es necesario conocer cuantos módems puede manejar el servidor. La cantidad estimada de servicios de comunicaciones de entrada y salida en la LAN, determina el servidor de comunicaciones adecuado. Muchos de estos servidores vienen con interfaces seriales para un numero específico de módem, otra consideración que hay que tomar en cuenta, si se requiere multiprocesamiento para tener comunicaciones remotas más rápido, algunos servidores de comunicaciones asíncronas tienen ranuras para instalar tarjetas de circuitos con sus propios microprocesadores en donde estos tienen su propia capacidad de procesamiento. Por ultimo se necesita conocer la velocidad y protocolos de los módem.

5.4.9 SWITCH

Los switch son dispositivos de tecnología de conmutación digital que trabajan en la capa 2 del modelo OSI, sirven para el transporte de datos sobre las líneas síncronas de conmutación a 56 kbits/seg ó líneas asíncronas de conmutación a 57 kbits/seg. Aunque gracias a la compresión se puede conseguir hasta este ancho de banda. Los clientes usan los servicios de switch para vídeo conferencia, para conexiones de LAN a LAN, para interconexiones de FAX y para servicios de telecomunicaciones de alta velocidad.

5.4.10 EQUIPOS HÍBRIDOS

Los equipos híbridos son equipos que trabajan tanto en la capa 2 y 3 del modelo OSI, estos son ruteadores que hacen algunas funciones del switch y switch que hacen algunas funciones de ruteadores.

5.5 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI) (UNINTERRUPTIBLE POWER SUPPLY, UPS)

Los Sistemas de Alimentación Ininterrumpida (SAI) ó (Uninterruptible Power Supply, UPS) son equipos que permiten realizar suministro de energía eléctrica almacenada en baterías, durante un periodo fijo de tiempo, en el cual ocurre algún corte de suministro por la red eléctrica. Ésta energía almacenada permitirá seguir funcionando equipos electrónicos para llevar a cabo la salvaguarda de la información y cierre normal de la computadora.

Los UPS's están constituidos por baterías, cargador de baterías y un ondulator, la finalidad de este último, es convertir la corriente continua procedente de los acumuladores, en corriente alterna, y proporcionar un voltaje constante con un cierto rango de tolerancia de amplitud y frecuencia, de iguales características que las de la red, pero ya sin problemas de ruidos y variaciones que la afecta.

5.5.1 BENEFICIOS QUE APORTAN LOS UPS

Los beneficios principales que deben de aportar dichos equipos son:

- Aislar la carga que se alimenta de la red.
- Estabilizar el voltaje y la frecuencia de salida.
- Evita picos y efectos parásitos de la red eléctrica.

5.5.2 CAUSAS Y EFECTOS DE LOS PROBLEMAS DE LA RED ELÉCTRICA

Los problemas ocasionados en los equipos eléctricos e informáticos y las pérdidas de información son ocasionadas por interrupciones y perturbaciones en el suministro de la red eléctrica debido a problemas de: fenómenos naturales, mal operación de la red eléctrica, cambios de cargas ó interferencias causadas por equipos eléctricos como elevadores o ascensores, equipos de soldadura por arco, etc. Estas causas dan origen a problemas de tensión como regulación, cortes y microcortes, armónicos y ruidos. Todos estos efectos producen daños en los circuitos electrónicos y programas lógicos de la informática.

Regulación o Sobretensiones momentáneas. Son variaciones lentas en la tensión ó frecuencia, pudiendo durar desde algunos ciclos hasta algunas horas. Estas son causadas por cambios de cargas eléctricas y por el conexionado de interruptores de la compañía eléctrica. Los fenómenos que implican la regulación son: transitorios o picos, subidas y bajadas de tensión, etc.

Transitorios ó picos: Son sobrevoltajes producidos por descargas eléctricas producidas sobre la red eléctrica por rayos, incendios y paradas de equipos de alta potencia, estos picos pueden alcanzar valores superiores al 20% del valor nominal y durar algunos segundos, esto nos

produce destrozos en los circuitos electrónicos y corrupciones de datos informáticos. Solución: Incorporar un filtro de línea; un transformador de aislamiento, ó un UPS con doble Conversión para mayor seguridad, el cual más adelante se menciona.

Filtro de Línea: Es un circuito electrónico que filtra los picos de tensión de la red eléctrica de corta duración e intensidad.

Transformador de aislamiento: Un transformador de aislamiento galvánico como su nombre indica, desarrolla una función de aislamiento sobre la red eléctrica entre la entrada y la salida consiguiendo evitar los picos y transitorios además de ruido eléctrico de alta frecuencia.

Subidas y Bajadas constantes de tensión: Son producidas normalmente por conexiones y paros de motores, ó por encendidos de cargas muy inductivas en la red eléctrica. Esto nos causa paros involuntarios de software y en equipos que trabajen en procesos de control. Solución: Un estabilizador de tensión, un acondicionador de línea con transformador separador incluido, ó un UPS Interactivo ú On-Line para mayor seguridad el cual más adelante se menciona.

Estabilizador de Tensión: Este corrige la tensión de entrada de la red eléctrica dentro de unos márgenes de aproximadamente un 20 % por encima y 25 % por debajo ayudado por el devanado del transformador de entrada normalmente.

Acondicionador de Línea: Un acondicionador de línea se compone de un estabilizador y un transformador de aislamiento.

Cortes y Microcortes: Son causados por fallos de la compañía suministradora de energía eléctrica, rayos en las líneas ó sobrecargas de las mismas además del factor de error humano. Esto produce daños en todos los circuitos de cualquier equipo electrónico ó informático. Solución: Incorporar un UPS On-Line sería la solución ideal pero algunos equipos Interactivos pueden cumplir perfectamente con la función los cuales más adelante se mencionan.

Armónicos: Estos se generan por la integración de múltiples frecuencias fundamentales de las fuentes de alimentación, este problema se complica más por el consumo de cargas alinéales como fuentes conmutadas. Los armónicos impares son los más frecuentes, y están dentro del margen de frecuencias de 180 Hz hasta 1 KHz. Los problemas más frecuentes que presentan los armónicos son los inesperados flujos en los sistemas eléctricos, sobrecorrientes en los conductores del neutro y grandes pérdidas en los transformadores. Los interruptores termomagnéticos no alcanzan a dispararse. Para disminuir este problema, habrá que utilizar un sobredimensionamiento de neutros, utilizar UPS's, dado que incluyen filtros activos, para la transformación de cargas no lineales en lineales.

Ruidos: El ruido se compone de señales parásitas que se mezclan con la señal original. Y se tienen los siguientes tipos de ruidos:

Ruido eléctrico: Es el ruido sobrepuesto en la línea, en armónicos y archivo de datos.

Ruido en modo común: Es el ruido existente, entre los cables que llevan energía (fase y neutro) y la línea de tierra.

Ruido de tierra: Es el ruido que aparece entre las varias tomas de tierra, de diversos equipos, cuya línea es común.

La figura 5.5.2.1 muestra algunas formas de ondas de voltaje, originadas por fallos de suministro de energía en una red eléctrica.

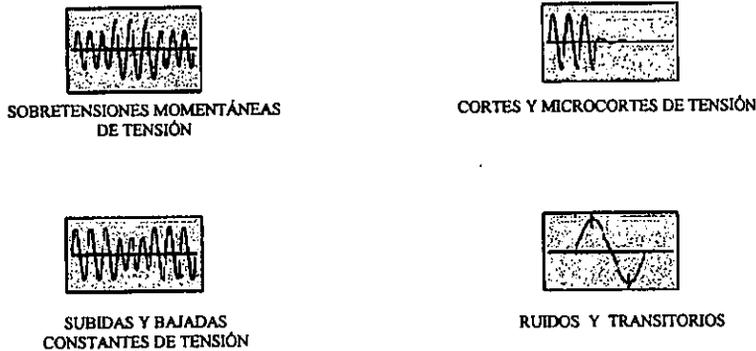


Figura 5.5.2.1. Fallos en el suministro de energía de la red eléctrica.

5.5.3 DIFERENTES TIPOS DE UPS

Existen diferentes topologías de UPS, cada una, para cada tipo de necesidad y condiciones de trabajo de la red eléctrica.

5.5.3.1 TOPOLOGÍA ON - LINE

En la topología ON-LINE la red alimenta al cargador de baterías y al ondulator (ver la figura 5.5.3.1.1) por tanto cualquier corte o microcorte queda suplido por las baterías. Se garantiza el aislamiento de la red, por medio del transformador separador existente en el cargador de baterías. La tensión de salida la proporciona el ondulator siempre, por tanto se garantiza la estabilización de salida.

Estos sistemas tienen el inversor constantemente en On con lo que no hay ningún tipo de transferencia (Red-UPS ni UPS-Red) al producirse una anomalía en la Red eléctrica eso les hace proveer una alimentación acondicionada y segura con protección de ruido eléctrico y estabilidad de frecuencia y tensión a los equipos conectados, puesto que el ondulator, es quién esta permanente trabajando y suministrando energía a la salida.

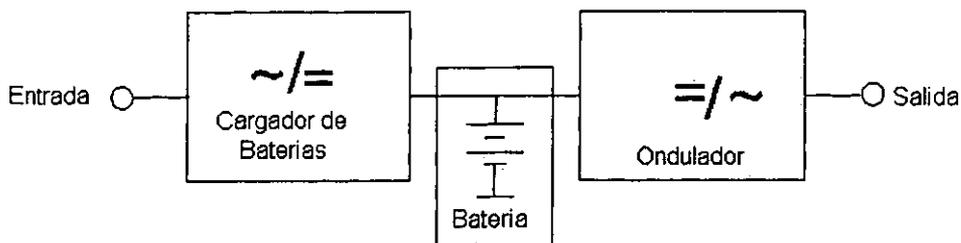


Figura 5.5.3.1.1. Topología On Line.

Los equipos ON-LINE suelen dar una protección del orden de entre 70% y 90%, al contrario del OFF-LINE no tienen tiempo de conmutación al estar actuando constantemente, con lo que los equipos no pueden ser afectados en ningún caso por cortes de fluido eléctrico ó perturbaciones.

5.5.3.2 TOPOLOGÍA ON-LINE DOBLE CONVERSIÓN

Son sistemas idénticos en funcionamiento que los On-Line con las ventajas añadidas de disponer de separación galvánica entre la entrada y la salida este tipo de sistema proporciona a los equipos conectados, la mayor garantía en protección.

La verdadera diferencia entre los SAI se encuentra en los equipos ON-LINE de doble conversión ya que los equipos OFF-LINE, Línea Interactiva y ON-LINE de una conversión están siempre dependientes de una manera u otra de que la entrada eléctrica al equipo cumpla unas mínimas condiciones para el correcto funcionamiento de los equipos cosa que en los equipos de doble conversión no depende de la línea de entrada para trabajar con una protección de más del 95 %.

5.5.3.3 TOPOLOGÍA ON LINE CON BYPASS

Existe también la posibilidad de Bypass, (ver la figura 5.5.3.3.1) el cual debe garantizar, por redundancia, el suministro de energía a la salida en caso de fallo de la red eléctrica. El conmutador de la salida, esta normalmente en la posición "O", por tanto el ondulador alimenta la carga y el control del Bypass supervisa esta alimentación, en caso de producirse alguna anomalía, el conmutador cambia a la posición "R", será por tanto, la red eléctrica quien alimentará a la carga en estas circunstancias.

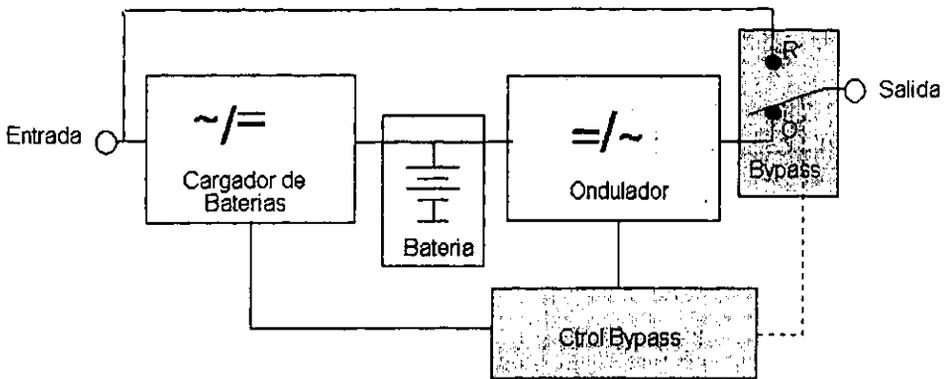


Figura 5.5.3.3.1. Topología ON-LINE con Bypass.

Cuando el control del BYPASS, observe restaurado el funcionamiento del ondulador, ó haya desaparecido la anomalía que ha provocado la intervención, devolverá la alimentación al ondulador.

Es importante observar que, dado que el Bypass, se comporta como sistema redundante de seguridad. Esta tecnología, es la primera históricamente en ser utilizada, es la que aporta mayor grado de protección en su salida, ya que ésta, es totalmente independiente de la entrada. Las condiciones de trabajo extremas desde un punto de vista de red eléctrica, es decir, referentes a la entrada, dependen de la concepción del cargador de baterías, a los que actualmente ya se dota de corrector de cos de p, con lo cual se consume corriente senoidal a la entrada, a la vez que se consigue bajar los niveles de tensión de red, a los que todavía se carga la batería. El ondulador, aporta las características eléctricas de salida.

5.5.3.4 TOPOLOGÍA STANDBY Ú OFF-LINE

Parte del criterio de reducir costes, por ello la base es proteger sólo en caso de necesidad, de tal forma que la red eléctrica alimenta a la carga normalmente y tan sólo interviene el ondulador en caso de fallo de red ó red excesivamente baja o alta, mediante la acción del conmutador C (Figura 5.5.3.4.1). Podríamos decir, que la red está controlada dentro de un intervalo de tensión máxima y mínima, y por tanto la carga que estamos alimentando, deberá soportar los límites de tensión a los que interviene el equipo. Normalmente no se produce un aislamiento entrada-salida y existe un inevitable tiempo de transferencia Red-UPS y UPS-Red. Dicho tiempo puede llegar a ser muy corto (1 mseg), sin embargo durante este tiempo, son los condensadores de filtro de la carga quienes mantienen la energía.

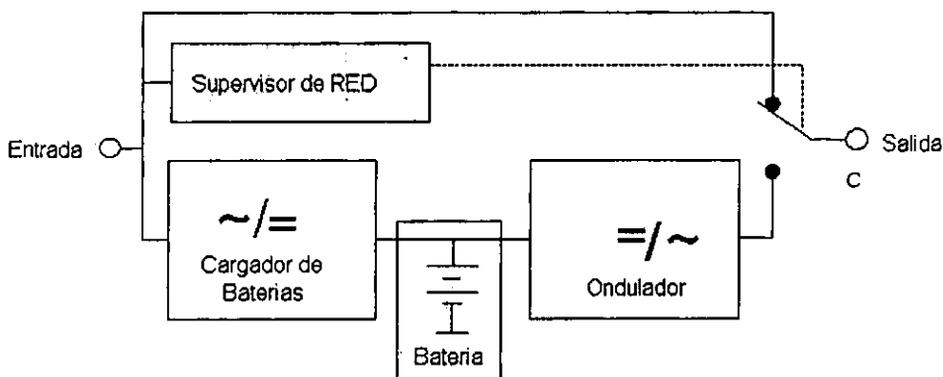


Figura 5.5.3.4.1. Topología OFF-LINE.

Como podrá observarse, existen los mismos bloques que en una configuración ON-LINE, cargador de baterías, baterías y ondulator, sin embargo se le añade un bloque más, que es el supervisor de red, elemento que permite detectar un posible fallo de ésta y conmutar "C", para que sea el ondulator, quien pase a alimentar la salida.

Bajo este criterio, el ondulator sólo trabajará el tiempo de descarga de la batería, apurándose hasta el límite, las características de los semiconductores de potencia. A su vez, la batería es cargada de forma lenta por el cargador, cuando existen condiciones correctas de red.

La topología OFF-LINE, es la más económica y en muchos casos, suficiente, dista de ser la más adecuada para realizar una protección total, parámetros como aislamiento, tiempo de transferencia y límites de protección, son sometidos a criterios económicos. El límite normalmente más conflictivo, es el punto de intervención, donde el ondulator empieza a trabajar y por tanto a utilizar batería, puesto que el equipo detecta la tensión de red baja. El SAI OFF-LINE, es útil prácticamente, sólo en lugares donde la red es estable y la protección a realizar, es frente a cortes momentáneos de suministro.

El tiempo de transferencia de un SAI es el tiempo muerto entre la conmutación de la Red eléctrica al Convertidor ó Baterías suele estar entre 1 a 10 mseg, dependiendo del momento de la conmutación, a partir de 4 mseg puede ser peligroso para los equipos informáticos con lo que es aconsejable utilizar equipos con el menor tiempo de transferencia posible y que realmente esta sea correcta.

Este equipo es recomendado para la protección de pequeñas cargas (PC's, Cajas registradoras, etc). Los OFF-LINE estarían entre 40% y 60 % con relación a la protección que deberían de tener los equipos informáticos, por supuesto de acuerdo con el tipo de equipos a proteger y la zona (Industrial, Oficinas, muy conflictiva en tormentas ó en cortes de suministro). Básicamente los equipos OFF - LINE actúan en el momento en que la red

desaparece ó baja por debajo del voltaje nominal, produciéndose en el cambio de red eléctrica a baterías un pequeño microcorte el cual para una mayoría de equipos eléctricos e informáticos es inapreciable, pero para los equipos muy sofisticados.

5.5.3.5 TOPOLOGÍA IN-LINE

Es una nueva técnica, que se aplican a equipos de elevada potencia, a fin de mejorar la fiabilidad y expectativas de vida. Comercialmente lo llaman ON-LINE. Por ello existen marcas que al ON-LINE nombran como "verdadero" o "doble conversión".

Originariamente, si está correctamente construido, las prestaciones y características que aporta, son prácticamente de ON-LINE. El sistema se basa en utilizar un ondulator reversible, capaz tanto de generar, como de rectificar para cargar la batería. Manteniendo al ondulator en marcha y variando la tensión y la fase generada por éste, se logra cargar adecuadamente la batería. Una etapa estabilizadora en la entrada, es obligada, para mantener al ondulator en los límites tolerables de trabajo como cargador y un elaborado filtro protegen al propio ondulator de picos de sobretensión, provenientes de la red eléctrica, que lo estropearían.

5.5.3.6 TOPOLOGÍA DE LÍNEA INTERACTIVA

Estos sistemas tienen el inversor generalmente en espera ó standby pero la lógica básicamente está funcionando al mismo tiempo que la red eléctrica, ya que el tiempo de conmutación es prácticamente nulo. Estos sistemas protegen de picos y sobretensiones a las cargas que conectemos a ellos y algunos suelen proteger de casi el 80% de las anomalías eléctricas, por su precio y calidad son equipos interesantes para algunas protecciones informáticas.

5.5.4 CARACTERÍSTICAS ELÉCTRICAS DE LOS UPS

5.5.4.1 REFERENTE AL ONDULADOR

- **Estabilidad de la tensión de salida en régimen estático.** Indica la estabilidad de la tensión de salida sin perturbaciones de red ni variaciones de carga.
- **Estabilidad en régimen transitorio.** Indica la variación de la tensión de salida cuando se produce una variación rápida de red ó bien con variaciones en la carga.
- **Distorsión armónica.** Indica la distorsión que contiene la tensión de salida.
- **Factor de potencia admisible (cos p).** Indica el desfase entre el voltaje y la corriente que admite el ondulator. La inclusión de correctores de cos p en los UPS,

- **Potencia de salida:** Indicada normalmente en VA (potencia aparente, S), expresa la potencia nominal que puede entregar el ondulator, a través del factor de potencia, se puede conocer la potencia activa W, que puede suministrar el equipo. ($W=S \cos p$).
- **Factor de Cresta.** El factor de Cresta, es el cociente de la división entre el valor pico de la corriente (I_p) demandada por la carga y el valor RMS o eficaz de la corriente (I_{RMS}).

$$\text{Factor de cresta} = \frac{I_p}{I_{RMS}}$$

El factor usual de una computadora es de 2 a 3. La inclusión de correctores de $\cos p$ en los UPS, minimiza el problema por el consumo de las computadoras hacia la red eléctrica, siendo el UPS quien proporciona la totalidad de energía de cresta, sin afectar a la red eléctrica.

- **Estabilidad en frecuencia.** Indica la variación en frecuencia que genera el ondulator, por tratarse de un generador, debe ser lo más cercana posible a la frecuencia de red.

5.5.4.2 REFERENTE AL CARGADOR DE BATERÍAS (ON-LINE) Ó AL SISTEMA (OFF-LINE)

- **Tensión de entrada.** Indica la tensión máxima y mínima tolerable por el UPS, será un dato importante la tensión de red a la cual todavía se carga la batería. En sistemas OFF-LINE indicará la tensión de intervención del equipo y por tanto los límites de protección.
- **Corriente de carga.** Su control es muy importante para evitar un deterioro prematuro de las baterías. La corriente ideal es $C/10$, la capacidad en Amperios/hora dividido por 10. El cargador debe ser capaz de mantener este máximo de carga sin descuidar la corriente que necesita la etapa ondulatora en los modelos ON-LINE para seguir funcionando.
- **Autonomía:** Es el tiempo que las baterías pueden seguir alimentando la carga, cuando no existe energía en la red eléctrica o está por debajo de la tensión mínima a la cual todavía se carga la batería. Debe de medirse a potencia nominal.

El tipo de baterías y número de éstas, da una idea de la autonomía, así como también también del coste del UPS y su esperanza de vida útil.

5.5.4.3 REFERENTE AL BYPASS

- **Bypass manual:** Es un conmutador que permite alimentar a la carga desde la red, en caso de fallo del ondulator o de mantenimiento del mismo.

- **El Bypass estático:** Es un elemento del UPS que le permite a este, conseguir que equipos que tengan una arrancada muy elevada puedan arrancar sin sobrecargar las etapas de potencia.
- **Aislamiento eléctrico:** Si el Bypass, no dispone de aislamiento, obligatoriamente una fase de entrada, está en permanente conexión, con una fase de salida, por tanto se está ofreciendo una vía inmejorable, para que el ruido o perturbaciones en modo común, llegue al sistema que se debería proteger.

5.5.4.4 GENERALES

- **Tipo de ventilación, temperatura, rendimiento.** Son valores indicativos de las pérdidas del equipo y del esfuerzo al que se somete a los semiconductores de potencia.
- **Numero de avisos e indicaciones.** Reflejarán la situación en la que se encuentra el equipo, y facilitarán su manejo, y comodidad al usuario.

5.5.5 RECOMENDACIONES PARA LA SELECCIÓN Y USO DE LOS UPS

Una vez que conocemos los diferentes tipos de tecnologías y como nos protegen, lo ideal, es centrarnos en saber cuál es el equipo ideal a nuestras necesidades, la tabla 5.5.5.1 muestra el tipo de problema eléctrico, su ubicación y el UPS recomendado.

Tipo de Problema Eléctrico	Ubicación ó entorno	UPS recomendado
Pocos cortes de red	Oficinas	OFF-LINE
	Zona Industrial	OFF-LINE
Muchos cortes de red	Oficinas e Industrias	On-Line
Variaciones de red	Oficinas	Interactivos
Subidas y bajadas constantes	Oficinas e industrias	On Line
Microcortes varios	Oficinas y Zona Industrial	On-Line
Ruido eléctrico y cortes	Zona Industrial	On-Line

Tabla 5.5.5.1. Muestra el tipo de problema eléctrico, su ubicación y el UPS recomendado.

Si la información de los VA no está disponible en los equipos a proteger normalmente detrás de los equipos a conectar existe una etiqueta con las características de los mismos cerca del número de serie indicando A, VA, ó W, con estos datos y las siguientes formulas es posible calcular los demás datos restantes.

Fórmulas para Calcular:

V: Voltaje [Volts]

A=I: Corriente [Amper]

VA: Potencia aparente [Volt Amper]

W: Potencia real [Watts]

Cos(p)= Factor de potencia

$$VA = V \times I$$

$$W = VA \times \cos(p)$$

Cos (p)= 0.8 en cargas informáticas aproximadamente

Por definición la potencia en corriente alterna viene dada por la siguiente formula $W=VI\cos(p)$, siendo p el ángulo de defase entre la tensión (V) y la corriente (I). El origen de este defase es por el consumo de cargas reactivas ocasionadas por bobinas y condensadores. Sin embargo actualmente debido a la alimentación de los equipos informáticos mediante fuentes conmutadas; este problema no existe. La figura 5.5.5.1 muestra el defasamiento entre voltajes y corrientes.

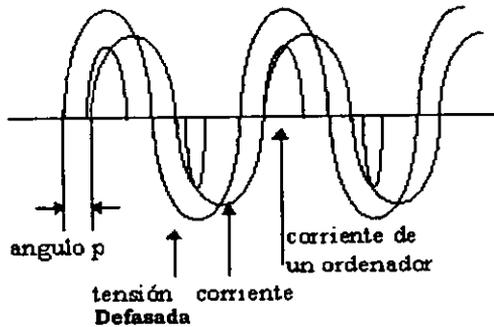


Figura 5.5.5.1. Defasamiento entre el voltaje y la corriente.

Por otro lado el porcentaje de crecimiento que se debería de dejar en el UPS debería de ser normalmente del 30 % de la capacidad del UPS en KVA. Ejemplo en un UPS de 10 KVA debería utilizar normalmente un 70 % de la potencia 7 KVA.

La autonomía del equipo vendrá referida a la carga que se le aplique en cada momento por ejemplo: a un equipo de 1000 VA con 10' de autonomía si le aplicamos 700 VA de carga nos dará 12 - 15 minutos mientras que si aplicamos 500 VA nos dará sobre los 20' minutos con lo que siempre es aconsejable saber cual es el programa que más tiempo necesita para cerrarse y a partir de ahí adaptar las autonomías de los UPS a los equipos. Normalmente no es exacta la potencia registrada en la placa en los equipos electrónicos, ya que los fabricantes de los equipos suelen poner en las características los valores máximos para las condiciones de arranque de los mismos con un 125 % y 150 % de sobrecarga en el rango según normas UL (Underwrites Laboratories, las cuales son un requerimiento de ley en dispositivos electrónicos para garantizar el buen funcionamiento eléctrico). Pero normalmente una vez arrancados los equipos el consumo suele bajar sobre el 70 % de lo marcado por los fabricantes.

Una buena solución para un sistema de red eléctrica es:

- 1- Solo proteger el Servidor con un UPS y el resto de los equipos no.
- 2- Un UPS central para la protección del Servidor y las estaciones de trabajo juntos.
- 3- Múltiples UPS, uno para cada servidor y para cada estación de trabajo.
- 4- Si la proximidad del servidor con el resto de equipos, o bien si se dispone de una línea específica para UPS la mejor solución, precio y prestaciones es la de un UPS central para todos los equipos de la red.

Gracias a la avanzada y sofisticada tecnología algunos UPS tienen la posibilidad de comunicarse con las computadoras a través de uno de sus puertos y mediante software enviar información y control a la computadora para poder observar anomalías producidas en la red eléctrica y visualizar parámetros del UPS.

Las impresoras láser no se deben de conectar a los UPS, ya que disponen de un sistema de calentamiento del rodillo con resistencias de alto consumo y realizan este ciclo cada 30 segundos emitiendo ruido de la conexión desconexión dentro de la línea protegida del UPS, y al estar conectadas al UPS generarían ruidos que pueden perjudicar a los datos informáticos.

El cambio de baterías en un equipo convencional será evidentemente dependiendo de la utilidad del equipo, cada 3 ó 4 años y en equipos más sofisticados suelen ser del doble de 5 a 6 años. Éstas deberán trabajar en un sitio seco y a temperaturas no superiores a los 30 °C, para obtener un rendimiento óptimo.

5.5.6 PROCEDIMIENTO PARA ACONDICIONAR UPS's

1. **Liste el equipo.** Haga una lista de todo el equipo que necesita protección. Recuerde incluir monitores, terminales, discos duros externos, y cualquier otro equipo crítico.
2. **Calcule los requisitos de suministro del equipo.** Cada equipo tiene un requisito de voltaje y amperaje.
3. **Requerimiento total en VA.** Sume los requerimientos de VA para todos los equipos. Requisito de tiempo de funcionamiento, que suministrará la potencia necesaria al equipo. Puede ser que desee una UPS con mayor capacidad para tomar en consideración sus necesidades de expansión en el futuro.

5.5.7 EJEMPLOS DE CONSUMO MEDIO

- Estación de red. Workstation 120 VA.
- PC 386, 486 180 VA.
- PC Gran Torre 220 VA.
- Servidor Pentium 250 VA.
- Servidor gran Torre 300 VA.

- Estación de trabajo RISC 400 VA.
- Servidor RISC 600 VA.
- Micro computadora 850 VA.
- Monitor 14" - 15" 70 VA.
- Monitor 17" - 20" 180 VA.
- Impresora de Tinta 90 VA.
- Impresora matricial 80 columnas 90 VA.
- Impresora matricial 136 columnas 140 VA.
- Impresora láser de red 3850 VA.
- Plotter A 380 VA.
- Encaminador (router)150 VA.
- Concentrador (Hub), Conmutador (Switch), Puente (Bridge) o Fax 120 VA.
- Scanner 160 VA.
- Cajas registradoras o TPV 150 VA.
- Balanzas 100 VA.

Operación a realizar: Sumar todos los consumos en VA, teniendo cuidado de multiplicarlos antes por la cantidad de unidades requeridas para la protección, con ello sabremos el consumo en VA aproximado del UPS que necesitaremos para proteger nuestros equipos. La tabla 5.5.7.1 muestra una relación de la potencia soportada por los UPS's y la carga de equipos informáticos que se le pueden conectar a estos.

Ejemplo de cargas que pueden soportar los siguientes UPS

POTENCIA VA	CARGA INFORMATICA
700 VA	2 Pentium + impresora (no-láser)
1000 VA	3 Pentium, 1 impresora (no-láser) ó 4 PC 486 o similares + 1 impresora (no-láser)
1500 VA	5 Pentium + 1 impresora (no-láser) ó 7 PC 486 o estaciones de trabajo
2000 VA	7 Pentium + 1 impresora (no-láser) ó 9 PC 486 o similares +2 impresoras (no-láser)
3000 VA	10 Pentium + 2 impresora (no-láser) ó 13 PC 486 o similares+1 impresoras (no-láser)
4000 VA	14 Pentium + 1 impresora (no-láser) ó 17 PC 486 o similares+1 impresoras (no-láser)
5000 VA	17 Pentium + 2 impresora (no-láser) ó 20 PC 486 o similares+1 impresoras (no-láser)

Tabla 5.5.7.1. Relación de la potencia soportada por los UPS's y la carga de equipos informáticos que se le pueden conectar a estos.

Los Pentium y PC's descritos constarían de monitor de 14" y las impresoras serían del tipo Matricial de 80 ó 136 columnas ó bien del tipo Inyección de tinta.

CAPÍTULO VI SOFTWARE DE REDES

6.1 ARQUITECTURA CLIENTE / SERVIDOR

La introducción del OS/2 en 1987 y de Windows NT en 1993 marcó el inicio de un nuevo nivel en la computación distribuida en red, antes de estos productos, cuando una estación de trabajo solicitaba consultar una Base de Datos, la respuesta de la mayoría de los servidores de archivos LAN era enviar todo el archivo de Base de Datos a través de la red, y cuando la estación de trabajo dejaba de utilizar la base de datos, la información regresaba al servidor de archivos.

El término cliente/servidor, como se muestra en la figura 6.1.1 describe un sistema en el que una máquina cliente solicita a una segunda máquina llamada servidor que ejecute una tarea específica, o es un sistema en el cual un cliente emite solicitudes y recibe el trabajo realizado por uno o más servidores, el cliente puede ser una computadora personal común conectada a una LAN, y el servidor es por lo general, una máquina anfitriona, como un servidor de archivos PC, un servidor de archivos de UNIX. Cuando una estación de trabajo consulta una base de datos en una arquitectura cliente/servidor, un programa de aplicación frontal recibe la solicitud, encuentra la información en la base de datos solicitada y sólo envía esta información y no todo el archivo de la base de datos a la estación de trabajo, aunque no solo hay soluciones de base de datos se mencionan debido a que son las mas utilizadas por la gran cantidad de información que pueden contener, pero también hay aplicaciones frontales cliente que son: hojas de calculo, programas contables etc.

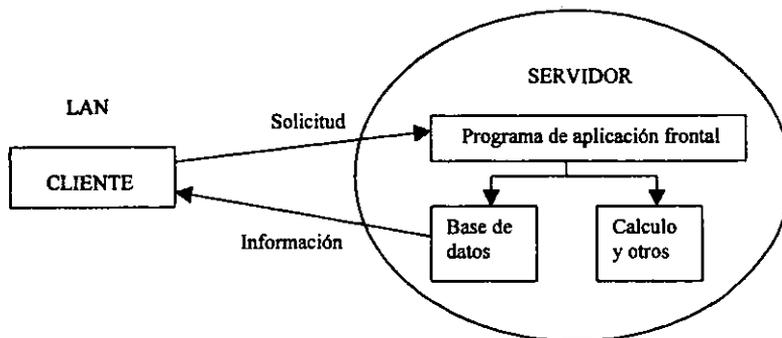


Figura 6.1.1. Arquitectura Cliente/Servidor.

El programa de aplicación frontal procesa la información solicitada y la despliega en la pantalla del cliente, mientras el servidor mantiene la integridad de la base de datos y se asegura que la red funcione con máxima eficiencia.

La idea de mejorar el rendimiento de las PC's, llevó a dividir las aplicaciones o actividades de una empresa de tal forma que parte del procesamiento se llevara a cabo localmente, o sea en el cliente, y otra parte remotamente en el servidor, adoptar esta idea era alejarse de los sistemas de computo centralizados (por lo general basados en una macrocomputadora), y confiar en un sistema de red de clientes y servidores.

En las principales LAN's cliente/servidor, los servidores son especializados en realizar trabajo para clientes. UNIX, LINUX, Windows NT server, Netware 3.x y 4.x de Novell, VINES de Bayan y LAN Server de IBM, todos estos sistemas operativos de red pueden operar y procesar solicitudes de aplicaciones que se ejecuten en clientes. Cada uno de estos sistemas puede operar con software adicional que puede ejecutarse en el servidor y que proporciona servicio a cada cliente de la red, estos productos de software pueden incluir bases de datos y programas de comunicaciones, de este modo, es muy posible que una LAN este constituida de servidores separados. Por ejemplo un servidor puede funcionar como servidor de base de datos que contenga toda la información de clientes, otro puede ser un servidor de comunicaciones que proporcione acceso a Internet, y un último servidor puede ejecutar el sistema operativo y la administración de la red, y los servicios de impresión y de archivos.

Los sistemas cliente/servidor tienen una gran seguridad, el usuario típico de un sistema normal se conecta con un solo servidor, pero en un sistema cliente/servidor el usuario puede conectarse a varios servidores diferentes, esto significa que los usuarios tienen que manejar una gran cantidad de guiones de registro de entrada, contraseñas e identificaciones del usuario para poder acceder a los diversos sistemas. Si un usuario necesita tener acceso a un servidor Windows NT, a la LAN de Novell, y a un servidor de UNIX, pueden existir tres diferentes contraseñas para el usuario, hay dos medios de cómo se debe manejar el acceso en los sistemas cliente/servidor.

El primer método establece que un solo registro una clave de contraseña pueden conectar al usuario con todos los sistemas en forma indistinta, los principales sistemas operativos están tratando de utilizar este método, aunque uno de los principales problemas que tiene este método es la seguridad, debido a que con una sola contraseña se puede tener acceso a los tres sistemas.

El segundo método es establecer distintas contraseñas para cada uno de los sistemas, esto da mayor seguridad, aunque tenga que incrementarse la cantidad de veces que un usuario tenga que registrarse en los diferentes sistemas.

6.2 SISTEMA OPERATIVO

6.2.1 MS-DOS

(MS-DOS, Microsoft - Disk Operating System). El sistema operativo de discos de Microsoft reside en la capa de presentación del modelo de referencia OSI, junto con el programa redirector que actúa como interfaz entre los programas de aplicación y el NETBIOS (que reside en las capas de presentación y de sesión). La figura 6.2.1.1 muestra la explicación anterior.

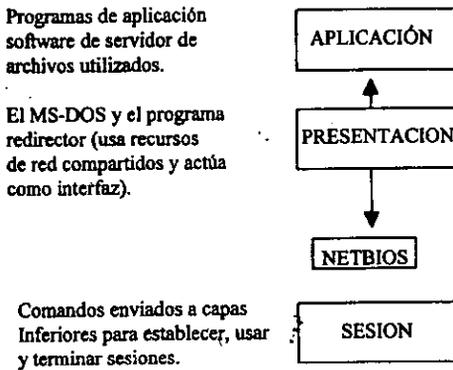


Figura 6.2.1.1. Representación del MS-DOS.

Bajo condiciones de red, el MS-DOS proporciona acceso a archivos a múltiples usuarios a través de su programa SHARE, este le permite al programador especificar que la primera estación de trabajo en usar un archivo tenga un cierto nivel de acceso, mientras que los usuarios subsecuentes tendrán otros niveles de acceso diferentes, por ejemplo un archivo usado por varias estaciones de trabajo diferentes, podría designarse como de lectura-escritura para el primer usuario que lo solicite, mientras este escriba en el archivo, los demás usuarios (bajo el modo de compartir lectura-escritura de SHARE sin derecho a escritura) solo podrán leer el archivo. También pueden bloquearse un rango de bytes, para que los demás usuarios no puedan escribir en él hasta que se libere ese rango de bytes.

6.3 SISTEMA OPERATIVO DE RED PUNTO A PUNTO

6.3.1 LANTASTIC

Es un sistema operativo de red que usa el método de punto a punto, el cual permite que cada estación de trabajo de red comparta sus recursos con otras estaciones de trabajo de la red. Cuando no se necesita seguridad ni otras características adicionales que ofrece un sistema de servidor de archivos centralizado, el método de punto a punto resulta más económico y eficiente. La figura 6.3.1.1 representa una red punto a punto.

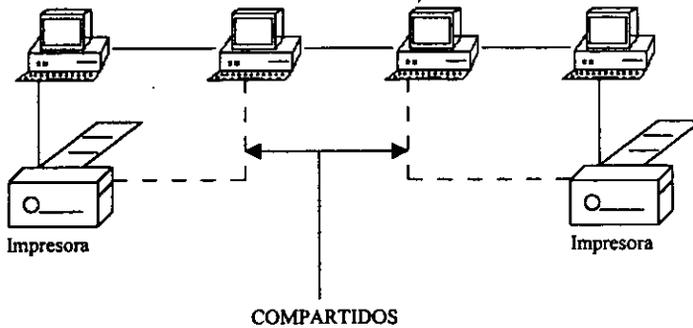


Figura 6.3.1.1. Red Punto a Punto.

6.3.2 MICROSOFT WINDOWS 95 / 98 / 98 PARA TRABAJO EN GRUPO

WINDOWS 95 / 98

Windows 95 cuenta con un sistema de red integrado de 32 bits que permite funcionar directamente con la mayoría de las principales redes, incluyendo Netware, Windows NT y otras de punto a punto. Además viene con versiones de 32 bits de un protocolo compatible con IPX/SPX y TCP/IP, y también maneja una variedad de otros protocolos y clientes de 16 bits.

WINDOWS NT para trabajo en grupo

Es un verdadero sistema operativo de 32 bits que esta disponible en versiones cliente y servidor, puede realizar multitarea prioritaria, procesos de multilectura. La primera permite la realización de múltiples tareas preferentes y subordinadas. Es NT y no los programas específicos quien determina cuando debe de interrumpirse un programa y empezar a ejecutarse otro. La segunda se refiere a los hilos que funcionan como agentes de ejecución, esto significa que un proceso ejecuta de manera simultanea, diferentes partes de un programa en diferentes procesadores.

6.3.3 NOVELL PERSONAL NETWORK

Este sistema operativo de red tiene la característica de que puede funcionar en varias topologías diferentes, dependiendo del Hardware que se seleccione, puede ejecutarse en una red configurada como estrella, agrupamiento en estrella, Token Ring e incluso en un Bus. Por ejemplo, la ejecución de Netware en Hardware bus Ethernet de 3Com produce una topología Bus, cuando se ejecuta en Hardware de ARCNET da como resultado una red Token Bus.

6.3.4 MACINTOSH APPLE TALK

La familia de protocolos de red de Apple Talk incluye los protocolos de red necesarios para transmitir datos en tres diferentes tipos de tipologías de red, estas tipologías son:

LocalTalk: Su tipo es propietario y transmite a velocidades de 230.4 Kbps a través de cableado de par trenzado.

EtherTalk: Son tarjetas de red colocadas en una Macintosh y pueden conectarse a una LAN Ethernet por medio de un cable coaxial o cable de par trenzado y manejan una velocidad de transmisión de 10 Mbps.

TokenTalk: Son tarjetas que hacen posible que las computadoras Macintosh sean parte de una red Token Ring.

6.4 OTROS SISTEMAS OPERATIVOS DE RED

6.4.1 IBM LAN SERVER

Es un sistema operativo de red que se ejecuta bajo OS/2, este software de servidor de archivos proporciona las relaciones cliente/servidor, cuando el software se ejecuta bajo un ambiente multitareas, permite que las bases de datos distribuidas en LAN sean una realidad, los usuarios solo necesitan solicitar un registro en particular y el procesamiento real se lleva a cabo en alguna otra parte de la red.

6.4.2 VINES DE BAYAN

Es un sistema de red virtual, además de que es un sistema operativo de red basado en una versión modificada de UNIX, VINES representa el patrón mas alto en la conectividad de redes, seguridad y transparencia de operación. VINES da soporte a una amplia gama de plataformas de hardware incluyendo Token Ring de IBM, ARCNET de SMC, Ethernet, etc. Solamente requiere de un servidor de archivos especializado.

6.4.3 LINUX

LINUX es un sistema operativo, compatible con Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (Kernel) y un gran número de programas (librerías) que hacen posible su utilización.

Las características principales de LINUX son:

Multitarea: La palabra multitarea describe la habilidad de ejecutar varios programas al mismo tiempo. LINUX utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados, siendo el sistema operativo el encargado de ceder tiempo de microprocesador a cada programa.

Multiusuario: Muchos usuarios pueden estar usando la misma máquina al mismo tiempo.

Multiplataforma: Las plataformas en las que en un principio se puede utilizar LINUX son 386, 486, Pentium, Pentium Pro, Pentium II, Pentium III, etc.

Multiprocesador: Soporte para sistemas con mas de un procesador (Intel).

Funciona en modo protegido 386: Protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.

Carga de ejecutables por demanda: LINUX sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.

Política de copia en escritura para la compartición de páginas entre ejecutables: Esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.

Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: A una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha. Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio. Este limite se puede aumentar fácilmente con el cambio de unas cuantas líneas en el código fuente. La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta puede a su vez ser reducida cuando se ejecuten grandes programas, además tiene librerías compartidas de carga dinámica (DLL's) y librerías estáticas.

Emulación de 387 en el núcleo: Realiza una emulación matemática, de tal manera que cualquier máquina que ejecute LINUX, simulará un coprocesador matemático, pero si la computadora ya tiene una FPU (unidad de coma flotante), esta será usada en lugar de la emulación, permitiendo e incluso compilar el propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

6.4.4 UNIX

UNIX es muy poderoso al igual que LINUX, este también brinda los beneficios de sistema multiusuarios, multitarea, es un sistema interactivo, multiprocesador y multiplataforma. Es interactivo porque responde a las entradas del usuario. Una desventaja que tiene este, es que no es un software libre.

Este sistema operativo de red ofrece ventajas sobre otros sistemas operativos, como es: procesamiento simétrico múltiple, lo que significa que es posible dividir la carga de procesamiento de un servidor, ofrece comunicaciones integradas, un poderoso lenguaje de guiones y portabilidad de programas desde una plataforma de Hardware UNIX hacia una segunda plataforma de hardware, además de que fue diseñado para redes grandes y para ofrecer seguridad en estas redes.

6.5 SERVICIOS DE RED

6.5.1 ACCESO A ARCHIVOS

Dentro de los servicios de red uno de los mas utilizados o indispensables es precisamente el de poder tener acceso a los archivos que se encuentran en la red, se podrá obtener información que se necesite de estos, dependiendo de los permisos (lectura o de escritura) que se tengan se podrá hacer uso de los archivos.

6.5.2 RESPALDO DE ARCHIVOS

Es uno de los servicios de red que los usuarios comunes no lo utilizan, ya que estos respaldan su información en discos flexibles o en el disco duro sin necesidad de utilizar el servicio de respaldo de archivos que debe de proporcionar una red informática, sobre todo en algunas instituciones donde se maneja gran cantidad de información y que es de vital importancia que la información pueda ser recuperada en dado caso de que se perdiera por alguna causa.

6.5.3 IMPRESIÓN DE ARCHIVOS

La impresión de archivos es utilizada por la gran mayoría de los usuarios, con este servicio de red es posible utilizar solamente una impresora para varias estaciones, lo que permite que no se tengan que utilizar gran cantidad de impresoras, además de que cada tarea de impresión (cola de impresión) esta guardada en una memoria temporal, que hace que el usuario pueda realizar otra actividad, sin necesidad de tener que esperar a que su impresión se haya realizado.

6.5.4 DETECCIÓN DE VIRUS

Las características principales de los virus informáticos son:

- Son programas de ordenador.
- Su principal cualidad es la de poder autorreplicarse.
- Intentan ocultar su presencia hasta el momento de la activación.
- Producen efectos dañinos en los discos de almacenamiento de datos y reducen la eficiencia del sistema.

Un virus informático es un programa de ordenador, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Obviamente ahí termina todo su parecido con estos típicos programas que casi todo el mundo tiene instalados en sus computadoras. Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a autorreplicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible.

Mientras el virus se replica intenta pasar lo más desapercibido que puede, intenta evitar que el antivirus se dé cuenta de su presencia, hasta que llega el momento de la "activación". Es el momento culminante que marca el final de la infección y cuando llega suele venir acompañado del formato del disco duro, borrado de ficheros. No obstante el daño se ha estado ejerciendo durante todo el proceso de infección, ya que el virus ha estado ocupando memoria de la computadora, ha hecho más lentos los procesos y ha dañado los ficheros que ha infectado. Los virus tienen un ciclo de vida muy concreto:

- Programación y desarrollo.
- Expansión.
- Actuación.
- Extinción.

6.5.5 CORREO

E-Mail (correo electrónico): Es un programa que se encarga de transmitir un mensaje escrito entre usuarios de la red. Para ello es imprescindible conocer la cuenta (identificador del usuario) y la dirección de la máquina del usuario al que queremos enviar un mensaje. Para aclarar el concepto se puede decir que el correo electrónico es como una carta normal y corriente. Sin embargo existen programas de e-mail basados en un sistema denominado MIME que permiten incluir en el cuerpo de la carta archivos binarios como imágenes, sonidos o archivos ejecutables. El programa de correo electrónico para PC's utilizado en muchos lugares se basa en este sistema. Y en la mayoría de los casos se usa la aplicación de PINE que es otro poderoso programa para el envío de e-mail y archivos. El cual trabaja bajo el sistema operativo de red UNIX.

6.5.6 GOPHER

Es un servicio de navegación por Internet anterior al WWW. Está basado en menús similares a la estructura de directorios en Unix, permitiendo enlaces entre servidores Gopher de todo el mundo.

También se le considera un servicio de información sobre los recursos de Internet, organizado en más de 3000 servidores interconectados. Cada servidor se encarga de organizar una porción local de la información, pero la creación de referencias cruzadas entre ellos permite que funcionen como una sola entidad en la práctica. La información se presenta clasificada por tipos y accesible mediante menús jerárquicos.

6.5.7 TELNET

Es un programa de inicio de sesión y emulación de terminal para redes de TCP/IP para uso principalmente de sesiones Internet. Su principal función es permitir a los usuarios iniciar una sesión en sistemas anfitriones remotos, mediante la cual es posible correr algunas aplicaciones, como PINE (Buzón y Editor de correos electrónicos).

Telnet es un proceso cliente-servidor en el cual el usuario invoca a la aplicación Telnet en el sistema local y establece un enlace a un proceso Telnet que se ejecuta en un anfitrión remoto.

6.5.8 PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS, (FILE TRANSFER PROTOCOL, FTP).

Esta aplicación permite transferir archivos de una computadora a otra o define una transferencia de archivo(s) entre dos computadoras, que pueden estar a una distancia considerable. La mayoría de las veces se usa FTP para copiar un archivo de una computadora remota a una computadora local. Este proceso se denomina carga. El proceso inverso se denomina descarga. Y el FTP anonymous permite a un usuario recuperar un archivo de un host (servidor) sin necesidad de estar registrado.

6.5.9 (World Wide Web, WWW)

WWW es un servicio o aplicación para navegación en Internet, basado en el hipertexto cuya función es buscar y tener acceso a recursos de Internet, y presentar esa información en forma de páginas que pueden contener texto, hipertexto y gráficos.

CAPÍTULO VII ANÁLISIS DEL PROBLEMA

7.1 SELECCIÓN DE LA MEJOR OPCIÓN Y JUSTIFICACIÓN DEL TIPO DE RED A INSTALAR

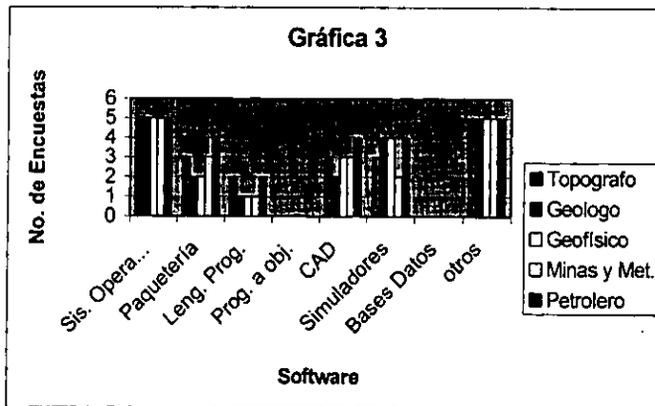
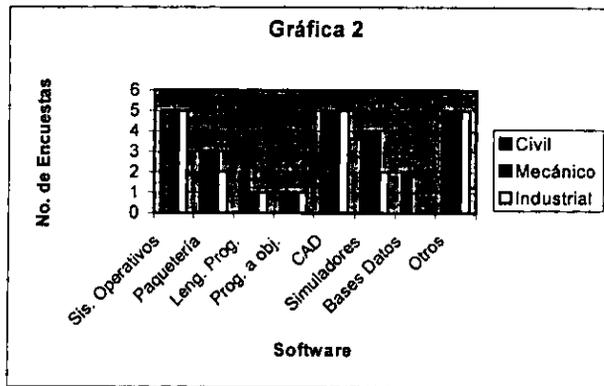
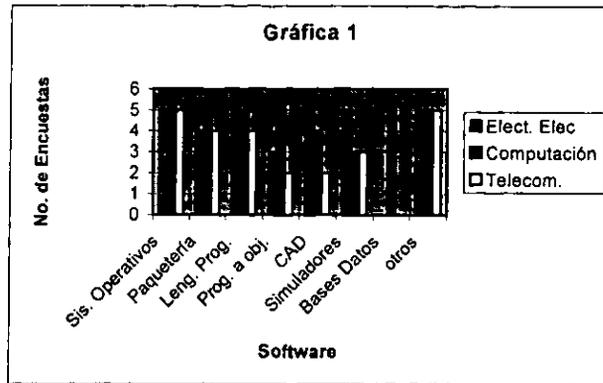
El tipo de cableado instalado fue el cableado horizontal con topología física en estrella, ya que concentra el cableado en un solo punto, por medio de un concentrador (HUB), de esta manera se puede agregar fácilmente mas estaciones de trabajo con solo conectar un cable que se conecte de la tarjeta de red a un puerto del concentrador utilizando cableado estructurado UTP de categoría 5, el cual permite la instalación de estaciones de trabajo a 100 metros de distancia desde el concentrador a donde esté esta, pero una desventaja de hacer este tipo de cableado en estrella; es de cuando falla el concentrador; también fallará todas las maquinas conectadas a este dispositivo. El cableado se realizó en estrella; pero con una topología lógica en bus ya que el tipo de red es Ethernet a 10 Mbps con par trenzado UTP categoría 5.

Una de las ventajas que tiene este tipo de cableado en estrella es: que todas las señales pasan a través del concentrador, es fácil hacer grupos de trabajo en esta red de área local, y poder comunicar una maquina con otra es decir se puede instalar software de redes punto a punto y poder instalar sistemas operativos como por ejemplo Windows 3.11, Windows 95, Windows 98 o Cliente/Servidor, como Windows NT, Novell, LINUX ó UNIX.

7.2 ENCUESTA SOBRE EL TIPO DE SOFTWARE MÁS UTILIZADO EN EL LABORATORIO

Las gráficas (1, 2, 3) muestran las encuestas de software más usado en licenciatura, maestría, doctorado, especialidad y también usado por profesores e investigadores; todos estos dentro de ciudad universitaria, en promedio fueron cinco por cada carrera, las gráficas están divididas para que se note con más claridad que software es el que más utilizaron o siguen utilizando en los lugares donde laboran.

De las gráficas podemos concluir que el software utilizado en mayor o menor grado, según coinciden diferentes carreras; son los sistemas operativos, en donde todos los entrevistados dijeron utilizarlo, también algún lenguaje de programación como Basic, Pascal, Fortran o "C", principalmente este último, por lo que es necesario tenerlo instalado en el laboratorio y de preferencia un lenguaje orientado a objetos como Visual Basic o "C++", pero además, el software denominado como (tipo de software "otros") los cuales manejan ambientes gráficos e Internet, en donde todos los entrevistados coinciden en que los utilizan. También contestaron que utilizan algún otro tipo de Software en los lugares donde laboran, pero que no es necesario de instalar en el laboratorio de computadoras, debido a que son herramientas muy específicas para el desarrollo de su trabajo y que es probable que nunca lo utilicen en el laboratorio.



Gráficas 1, 2 y 3. Muestran el tipo de software más utilizado según las entrevistas realizadas en Facultad de Ingeniería de Ciudad Universitaria México D.F.

7.3 DISEÑO E INSTALACIÓN Y PRUEBAS

Las consideraciones de diseño de cableado estructurado que hay que tener presente son: el costo de los materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal que pueden ser muy caros. Se implementó el cableado horizontal por ser capaz de manejar una amplia gama de aplicaciones de usuario, además por ser capaz de facilitar el mantenimiento y la localización de áreas de trabajo; se procuró que el cableado quedara bien a la primera vez y evitar costos de más.

El cableado horizontal se adapta a las necesidades de manejar diversas aplicaciones de usuario, como: comunicación de datos, comunicación de redes de área local, etc.

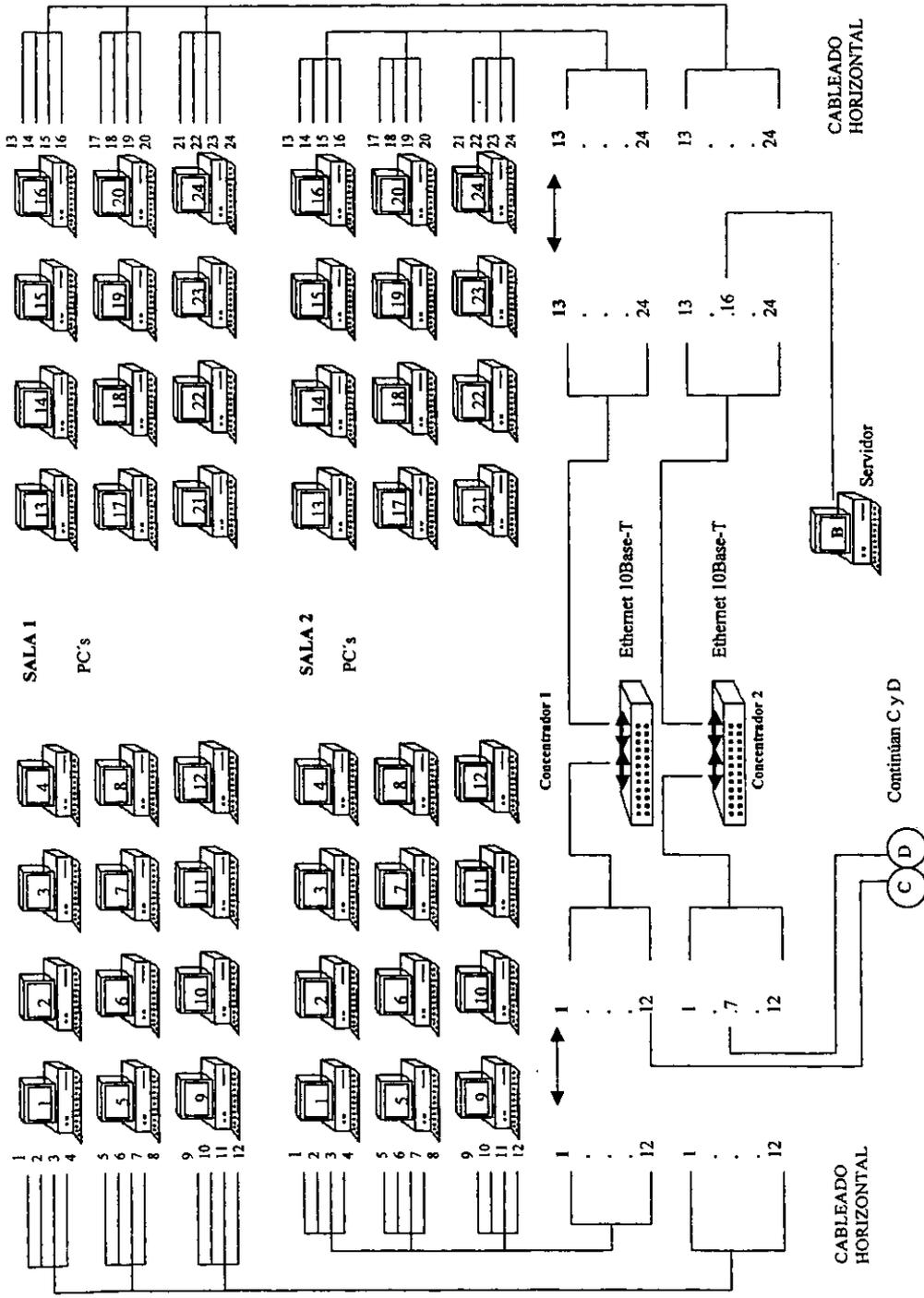
Además es importante considerar a futuro incorporar otros sistemas de información del edificio (por ejemplo comunicación de voz (teléfono), televisión por cable, control ambiental, seguridad, audio, vídeo, alarmas y sonido) al seleccionar y diseñar el cableado horizontal.

En base al estándar ANSI TIA/EIA T568-B de alambrado de Telecomunicaciones para edificios comerciales. Se sugirió tomar como base este estándar para tener un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar productos y proveedores múltiples. Para tener un buen diseño e instalación del cableado de telecomunicaciones e información básica acerca de los productos de telecomunicaciones para que posteriormente se pueda actualizar la red conforme avanza la tecnología.

En cuanto a las pruebas realizadas fueron: checar que los conectores RJ-45 de un extremo tuvieran continuidad hasta el otro extremo del cable UTP categoría 5, para ver si durante el tendido del cable no se dañó algún cable.

La figura 7.3.1 muestra la configuración de patillas usando la norma T568-B para cable UTP categoría 5, conectores y bases RJ-45.

El siguiente Diagrama de la Red de Computo del Laboratorio, muestra la distribución del cableado estructurado y conexión de los equipos de computo del laboratorio. Los concentradores (10Base-T) 1 y 2 distribuyen el cableado horizontal a cada una de las PC's, el concentrador 3, está conectado en cascada con el concentrador 4, el cual distribuye el cableado vertical a cada uno de los pisos del edificio, además conecta a una red 10Base-2; a través de éste concentrador se conecta por medio de fibra óptica (100Base-FX) a un switch periférico y luego éste se conecta al Backbone ATM de la RedUNAM, luego mediante un ruteador o encaminador se enlaza las redes 10Base-T a redes WAN e Internet a través de un gateway. El Backbone de RedUNAM agiliza el tráfico de comunicaciones de los switches periféricos que conectan a las redes LAN del campus universitario y brinda enlaces WAN e Internet. De alguna manera la Subdirección de Redes de la Dirección General de Servicios de Computo Académico (D.G.S.C.A), se encarga de la coordinación mantenimiento y operación de RedUNAM.



SALA 1

PC's

SALA 2

PC's

Concentrador 1

Ethernet 10Base-T

Ethernet 10Base-T

Concentrador 2

Servidor

Continúan C y D

CABLEADO HORIZONTAL

CABLEADO HORIZONTAL

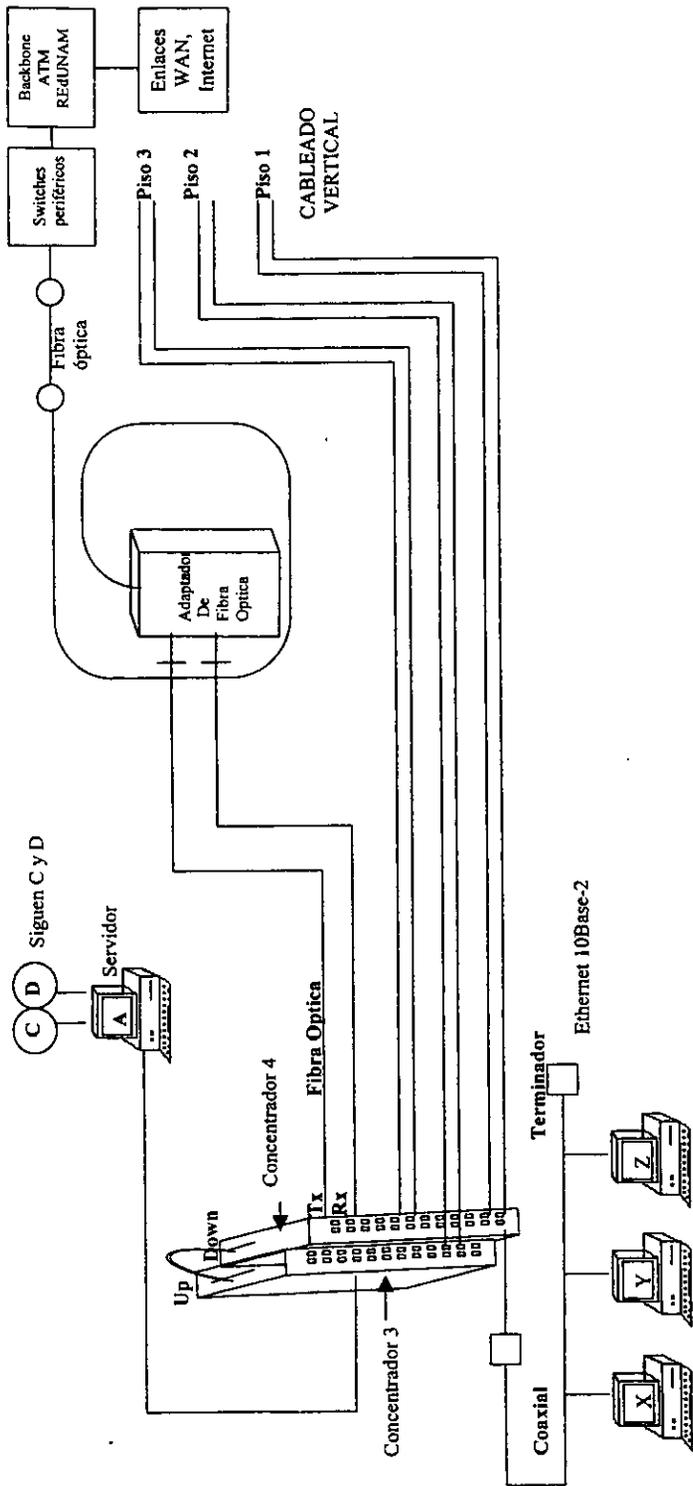


DIAGRAMA DE LA RED DE COMPUTO

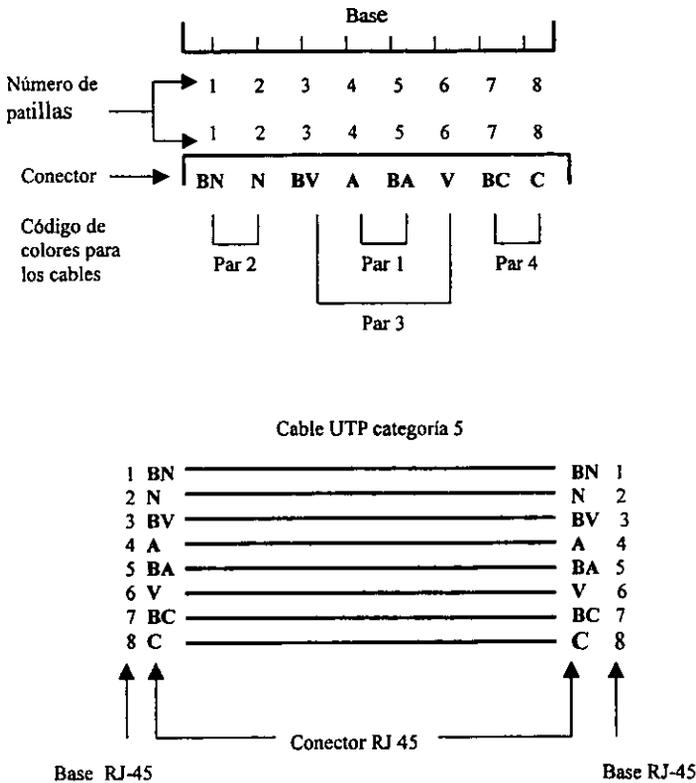


Figura 7.3.1. Configuración de patillas para los conectores y bases RJ-45, según la norma EIA/TIA T568B.

7.3.1. CARACTERÍSTICAS DE LOS ELEMENTOS DE RED

Equipo de computo utilizado como estaciones de trabajo:

- Equipos instalados, 42 PC's.
- Procesador Pentium MMX (para todas las PC's).
- Velocidad a 166 MHz.
- Memoria de 32 MB de RAM.
- Disco Duro de 2.5 GB.
- Memoria Cache de 512 KB.
- Tarjeta de vídeo 2 MB.

Monitores:

- Tipo de monitor SVGA 14 pulgadas.

Tarjetas de Interfaz para Red:

3COM Etherlink XLTP0, con adaptador Ethernet a 10 MB compatible con los siguientes protocolos:

- Protocolo IPX para redes Novell Netware IPX a 32-bits.
- Protocolo compatible con IPX/SPX.
- Protocolo TCP/IP.
- Protocolo NETBEUI.

Servidores:

- Servidor de archivos (2) del tipo PC con las mismas características a las estaciones de trabajo.
- Servidor para Windows NT (1).
- Servidor para Linux (1).

Concentradores:

Dos concentradores 10Base-T (1 y 2) con las siguientes características:

- Concentradores 3COM PS Hub 40 de 24 puertos con conectores RJ-45.
- Dos slots para instalar dos módulos transeptores.
- LED's indicadores.
- Dos puertos para conexión en cascada.
- Frecuencia de operación 60 Hz.
- Voltaje de entrada 100-240 VCA.
- Corriente 1A máximo.

Cable:

- Cable UTP categoría (5), 100 ohms, 22/24 AWG.
- Velocidad de transmisión 100 Mbits/seg.
- Distancia máxima 100 metros.

Conectores:

- Conectores RJ45 (84).

Gabinete de cableado:

- Panel de parcheo y Rack. Están ubicados dentro del cuarto de Telecomunicaciones.

Sistema de alimentación ininterrumpible (UPS), con las siguientes características:

ENTRADA**SALIDA**

- | | |
|---|------------|
| • 120 VCA. | 120 VCA. |
| • 725 VA. | 675 VA. |
| • 475 Watts. | 425 Watts. |
| • 60 Hz. | 60 Hz. |
| • Tiempo de recarga 2 a 4 Hrs. | |
| • Tiempo de autonomía a plena carga 15 minutos. | |
| • Tiempo de autonomía a ½ carga 45 minutos. | |
| • Puerto de comunicaciones tipo DB9 (serial). | |

Impresoras:

- Tipo LaserJet 6L.
- Velocidad de 6 ppm.
- Conexión por puerto paralelo.
- Memoria de 1MB, expandible a 9MB.
- Resolución de 600 dpi.

Servidor de impresión debe tener las siguientes características:

- Soportar varias impresoras.
- Software para manejar las colas de impresión.
- Comandos de redirección de impresoras disponibles para el usuario.

7.3.2 SISTEMAS OPERATIVOS

Para instalar los sistemas operativos se tuvo que particionar el disco duro; y así poder seleccionar el arranque de cada una de las máquinas en la plataforma que el usuario desee, estos son: Windows NT Server para el servidor, Windows NT WorkStation para las estaciones de trabajo y LINUX.

7.3.3 SERVICIOS DE RED, SOFTWARE NECESARIO

Los servicios de red son para envío de correos electrónicos a través de sesiones de Telnet, Pine, Eudora; para transferencia de archivos mediante FTP y como navegadores en Internet se tienen a Gopher, Netscape, Explorer y Mosaic.

Gracias a las aplicaciones como Gopher o World-Wide-Web (WWW) la búsqueda de información a través de Internet se puede hacer de una forma sencilla, cómoda y rápida. Ya es bien conocido el gran potencial que ofrece esta red en cuanto se refiere a comunicación y compartición de recursos (software, datos, documentos). Sin embargo, el usuario no le encontrará ningún valor a este potencial si tiene que dedicar un gran esfuerzo para descubrir los recursos de su interés. Por este motivo, en la actualidad se está dedicando un gran esfuerzo en implementar e implantar herramientas que ayuden al usuario a buscar y también organizar la información disponible en la red. Gopher y WWW son dos herramientas de este tipo imprescindibles para un usuario, tanto novato como experimentado de Internet. A estas dos aplicaciones se les da el calificativo de aplicaciones globales de información, ya que, al proporcionar una interfaz de acceso única para los diferentes tipos de información, integran y homogenizan la mayoría de las aplicaciones y servicios de red existentes en la actualidad en Internet.

Lo interesante está en ofrecer a los usuarios un sistema global de información para facilitar el acceso a los distintos servicios de Internet y organizar la información propia de una forma flexible y uniforme. Las dos aplicaciones anteriores se han estado probando y evaluando durante el último año. Esta labor aún continúa, debido al gran ritmo de evolución que están teniendo estas aplicaciones. El dilema está en que cual de los dos sistemas escoger. Las dos tienen un concepto totalmente distinto de conseguir su objetivo: Gopher está basado en menús y enlaces jerárquicos, mientras que WWW está basado en documentos en donde las palabras pueden tener enlaces a otros documentos (concepto de hipertexto). Una tiene unas ventajas respecto a la otra en algunos casos, mientras que en otros casos es al revés. Pero ninguna de las dos aplicaciones merece desprecio.

La arquitectura de WWW está basada en el modelo cliente-servidor. Los clientes presentan la información en el formato hipertexto y pueden llevar implementados varios protocolos tales como FTP, GOPHER, etc.

7.4 INFRAESTRUCTURA

En base al estándar ANSI TIA/EIA-606 de administración para la infraestructura de telecomunicaciones para edificios comerciales; es importante tener un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. Este estándar establece guías encargados, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

En cuanto a la infraestructura como ductos para cables de energía los cuales van al cuarto de suministro de energía y los ductos para la instalación del cableado estructurado los cuales llegan al cuarto de telecomunicaciones, ya estaban instalados; es decir toda la infraestructura; ya estaba instalada en lo único que se contribuyó para terminar este proyecto fue en distribuir el cable del cuarto de telecomunicaciones hasta donde están los concentradores y servidores que se enlazan a Red UNAM para dar salida a Internet a cada una de las máquinas.

7.4.1 DUCTERÍA Y CABLEADO ESTRUCTURADO

En cuanto a la ductería, se utilizó la que ya estaba instalada la cual sigue la norma de ANSI EIA/TIA-569 de rutas y espacios de Telecomunicaciones para edificios.

El número y tamaño de ductos utilizado para acceder al cuarto de telecomunicaciones varía con respecto a la cantidad de estaciones de trabajo, sin embargo se recomienda por lo menos de 100 m para la distribución del cable del backbone según ANSI TIA/EIA-569. Los ductos de entrada deben de contar con elementos de retardo de propagación de incendios. Sin embargo este estándar reconoce tres conceptos fundamentales relacionados con las Telecomunicaciones y edificios.

- Los edificios son dinámicos: Durante la existencia de un edificio, las remodelaciones son más la regla que la excepción. Este estándar reconoce de manera positiva, que el cambio ocurre.
- Los sistemas de Telecomunicaciones son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones, cambian dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores de equipo.
- Telecomunicaciones son más que datos y voz. También incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido; es decir incorpora todos los sistemas de bajo voltaje que transportan información en los edificios.

Este estándar recomienda la manera para que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, por eso es importante que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

En cuanto al cableado estructurado se instaló cable UTP de categoría 5, de 100 ohms, 22/24 AWG en base a la norma de cableado estructurado ANSI/EIA-T568B, tomando en cuenta que la distancia horizontal máxima del concentrador a la tarjeta de interfaz de red de la estación de trabajo es de 100 m. Por lo tanto se recomienda que el cuarto de telecomunicaciones esté lo mas cerca posible del área a servir. El destrenzado de pares individuales en los conectores y paneles de parcheo deben de ser menor a 1.25 m para cables UTP de categoría 5.

El radio de doblado del cable no debe de ser menor a cuatro veces el diámetro del cable. Así por ejemplo para UTP de categoría 5 el radio mínimo de doblado es de 2.5 cm.

En los extremos de los cables UTP categoría 5 se instalaron conectores tipo RJ-45. Bajo el código de colores T568B y siguiendo esta norma se realizó el cableado paralelo (uno a uno) entre los conectores. Los cables con sus conectores, conectan a las bases integradas a los concentradores con las bases de las tarjetas de interfaz de red de cada PC. Lo cual nos ahorra utilizar paneles de parcheo y paneles modulares de conectores, los cuales se verían muy bien en un Rack o armario de cableado; pero estos ahorros no serían convenientes para crecimientos futuros.

Para evitar la interferencia electromagnética se sugirió que la ruta del cableado estructurado a cada uno de los nodos, no pasara el cable por los siguientes dispositivos.

- Cables de corriente alterna:

- Mínimo 13 cm para cables con 2 KVA o menos.
- Mínimo 30 cm para cables de 2 KVA a 5 KVA.
- Mínimo 91 cm para cables con más de 5 KVA.

- Luces fluorescentes y balastos (mínimo 12 cm). El ducto debe de ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cm).
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

7.4.2 ENERGÍA REGULADA Y SISTEMAS DE TIERRA

En cuanto al suministro de energía: el laboratorio cuenta con los suficientes contactos tomacorriente para alimentar al equipo de computo. El estándar establece que debe de haber un mínimo de dos tomacorrientes dobles de 110 Volts CA dedicados de tres hilos. (El primer hilo del contacto, se conecta con el neutro (entrada grande), el segundo con la fase o corriente (entrada chica) y el tercer hilo (entrada redonda) con la tierra de la red eléctrica). Los circuitos suministran de 15 a 20 Amperes. Estos dos tomacorrientes se recomiendan que estén dispuestos a 1.8 m aproximadamente uno de otro.

Para tener la energía regulada se cuenta con un regulador de voltaje y supresores de picos así como también; se cuenta con alimentación eléctrica de emergencia con activación automática suministrada por medio de UPS's.

El cuarto de telecomunicaciones cuenta con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI TIA/EIA-607 que nos brinda los requerimientos de puesta a tierra y puentado de Telecomunicaciones de edificios comerciales.

7.5 CONCLUSIONES COMENTARIOS Y SUGERENCIAS

Durante el desarrollo de este proyecto, se fijaron las bases teóricas de redes de computadoras, telecomunicaciones y sistemas de suministro de energía eléctrica, con el fin de dar un panorama general de los conocimientos necesarios para poder diseñar, adaptar, cambiar e implementar la infraestructura con la que se cuenta el laboratorio.

En base a las necesidades y problemática detectada, se realizó una encuesta sobre el tipo de software y los más utilizados resultaron ser los sistemas operativos, los lenguajes de programación como Basic, Pascal, Fortran, C; así como también los lenguajes de programación orientado a objetos como Visual Basic y C++; de la misma manera resultaron ser los ambientes gráficos e Internet. Estas herramientas brindarán el servicio requerido por las necesidades actuales de tal manera que dicho laboratorio cumpla con sus funciones académicas. Estas implementaciones le serán útiles a las nuevas generaciones que estudien en el Laboratorio de Computadoras y Programación de esta Facultad de Ingeniería.

El cable coaxial fue reemplazado por el cable UTP categoría 5, esto permitirá la compatibilidad con nuevas tecnologías a 100Mbps/seg como Ethernet Rápida, etc. Se configuraron las patillas de los conectores y bases RJ-45 siguiendo la norma EIA/TIA T568-B, el cual se adaptaba al material ya existente.

En la instalación de la red 10Base-T se utilizaron computadoras personales con tarjetas de red a 10 Mbps/seg, servidores del tipo PC, concentradores 10Base-T, cable UTP categoría 5. Gracias a la infraestructura con que cuenta RedUnam, es posible, conectar esta red del laboratorio por medio de fibra óptica a los switches periféricos del Backbone ATM de RedUNAM y además poder aprovechar los enlaces a redes WAN e Internet.

Con estas actualizaciones los alumnos tendrán un fácil acceso a Internet, para que aprovechen la tecnología de punta y obtengan e intercambien información a nivel mundial.

Esta red además de trabajar con Linux, podrá soportar redes Windows 95 / 98 y Windows NT.

Apéndice A:

Lista de acrónimos y abreviaturas más usuales en el ambiente de las redes de computadoras y comunicaciones de datos.

- ADN: Avanced Digital Network.
- ANSI: American National Standard Institute (Instituto Nacional Americano de Normalización).
- API: Application Program Interface.
- AT&T: American Telephone and Telegraph.
- ATM: Asynchronous Transfer Mode (Modo de transferencia Asincrona).
- AUI: Attachment Unit Interface (Interfaz de la unidad de enlace).
- AWG: American Wire Gauge.
- BECCN: Backward Explicit Congestion Notification (Notificación de congestión explicita hacia atrás).
- B-ISDN: Broad-Integrated Services Digital Network (Redes Digitales de servicios integrados de Banda ancha).
- CAN: Campus Area Network (Redes de área de campo).
- CATV: Community Antenna Television.
- CAU: Controlled access unit.
- CCITT: Consultive Committee for International Telegraph and Telephone (Comité Consultivo Internacional para Telegrafía y Telefonía).
- CDDI: Copper Distributed Data Interface (Interfaz de datos distribuidos por cables de par trenzado).
- CIR: Committed Information Rate (Tasa de información asegurada).
- CPU: Central Processing Unit (Unidad Central de Proceso).
- CRC: Cyclical redundancy Checksum (Control de redundancia cíclica).
- CSMA/CD: Carrier Sense Multiple Access with Colisión Detección (Acceso múltiple con detección del portador /Detección de colisión).
- CV: Virtual Circuit (Circuitos Virtuales).
- D.G.S.C.A.: Dirección General de Servicios de Computo Académico.
- DAN: Departamental Area Network (Redes de área departamental).
- DAS: Dual-Attached Stations (Estaciones de acoplamiento doble).
- DE: Discard Eligibility.
- DEC: Digital Equipement Corporación.
- DLCI: Data Link Connection Identifier.
- DPA: Demand Priority Access (Acceso por Prioridad de demanda).
- ECD: Equipos de Comunicación de Datos.
- EIA/TIA: Electronic Industries Association/Telecommunication Industries Association.
- ETCD: Equipo de terminación de circuitos de datos.
- ETD: Equipo Terminal de Datos.
- FDDI: Fiber Distributed Data Interface (Interfaz de datos distribuidos por fibra).
- FECN: Forward Explicit Congestion Notification (Notificación de congestión explicita hacia delante).
- FPU: Unidad de Coma flotante.
- FSC: Frame Check Secuence (Secuencia de verificación de trama).
- FTAM: File Transfer, Access and Management (Acceso y manejo de transferencia de archivos).
- FTP: File Transfer Protocol (Protocolo de transferencia de archivos).
- GAN: Global Area Netwok (Redes de área global).
- GFC: Generic Flow Control.
- HDLC: High-Level Data Link Control (Control de Enlace de Datos de Alto Nivel).
- IBM: International Business Machines.
- IEEE: Institute of Electrical and Electronic Engineers (Instituto de Ingenieros Eléctricos y electrónicos).
- IP: Internet Protocol.
- IPX: Internetwork PacKet Exchange (Intercambio de Paquetes entre Redes).
- ISDN, RDSI: Integrated Services Digital Network (Red digital de servios integrados).
- ISO: International Standard Organization (Organización Internacional de Estándares).
- ITU: International Telecommunication Union.

LAN: Local Area Network (Red de área local).
LCP: Link Control Protocol (Protocolo de control de enlace).
LEN: Low-entry Networking node.
LLC: Logical Link Control (Control de Enlace de Datos).
MAC: Media Access Control (Control de acceso al medio).
MAN: Metropolitan Area Network (Red de área metropolitana).
MAU: Multistation access unit.
Mbps: Megabits por segundo.
MDI: Medium Dependent Interface (Interfaz Dependiente del Medio).
MIME: (Multipurpose Internet Mail Extensions).
NAP: Network Access Protocol (Interfaz de programación de aplicaciones).
NCP: Network Control Protocols (Protocolos de Control de Red).
NDIS: Network Driver Interface Specification (Especificación de la interfaz del controlador de red).
NetBEUI: NetBIOS Extended User Interface (Interfaz extendida de usuario de NetBIOS).
NetBIOS: Network Basic Input/Output System (Sistema básico de red de entrada y salida).
NIC: Network Interface Card (Tarjetas de interfaz para red).
NNI: Network to Network Interface.
NOS: Network Operating System (Sistema operativo de red).
OS/2: IBM Operating System/2.
OSI: Open Systems Interconnection (Interconexión para los sistemas abiertos, ISA).
PAD: Packet Assambler / disassembler.
POTS: Plain Old Telephone System.
PPP: Point-to-Point Protocol (Protocolo Punto a Punto).
PROM: Programmable Read-Only Memory (Memoria programable de solo lectura).
PVC: Permanent Virtual Circuit (Circuito virtual permanente).
RAM: Random Access Memory (Memoria de acceso aleatorio).
RIP: Routing Information Protocol (Protocolo de ruta de información).
RISC: Reduced Instruction-Set Computer.
RJ-11: Standard Modular Telephone Jack for a Single Line Instrument.
RJ-45: Standard Modular Network Jack.
RND: Remote Name Directory.
ROM: Read Only Memory (Memoria de solo lectura).
SAI: Sistemas de alimentación ininterrumpida.
SAP: Service Access Points (Puntos de acceso al servicio).
SAS: Single-Attached Stations (Estaciones de acoplamiento único).
SFD: Start Frame Delimiter (Delimitador de inicio de la trama).
SFT: Sistema de tolerancia a fallos.
SHARE: Society to Help Avoid Redundant Effort.
SLIP: Serial Line Internet Protocol (Protocolo Internet de Línea serie).
SMS: Storage Management Subsystem (Subsistemas de Administración de Almacenamiento).
SMT: Station Management (Gestión de estaciones).
SMTP: Simple Mail Transfer Protocol.
SNA: Systems Networks Architecture.
SPX: Sequenced Packet Exchange (Intercambio de paquetes secuenciados).
STP: Shielded Twisted Pair.
TCP/IP: Transmission Control Protocol/Internet Protocol (Protocolo de control de Transmisión/Protocolo Internet).
TDM: Time División Multiplexing (Multiplexación por división de tiempo).
TP-PMD: Twisted Pair Physical Medium Dependent.
UDP: User datagram Protocol.
UL: (Underwrites Laboratories).
UNI: User Network Interface.
UPS: Uninterruptible Power Supply.
UTP: Unshielded Twisted Pair (Cables de par trenzado sin blindaje).
VAX: Virtual Address Extension.

VCI: Virtual Circuit Identifier.
 VLAN: Virtual Local Area Network (Redes virtuales de área local).
 VPI: Virtual Path Identifier.
 VTP: Virtual Terminal Protocolo (Protocolo de terminales virtuales).
 WAN: Wide Area Network.
 WWW: World Wide Web.

APÉNDICE B.

Bibliografía utilizada para el desarrollo de este trabajo:

- Jenquins Neil, Schatt Stan; "REDES DE ÁREA LOCAL (LAN)", México, Prentice Hall Hispanoamericana, S.A., 1996.
- Sheldon, Tomas, "LAN TIMES ENCYCLOPEDIA OF NETWORKING / TOM SHELDON", U.S.A., Osborne McGraw-Hill, 1994.
- Black,Unyles; "REDES DE COMPUTADORAS (Protocolos, Normas e Interfaces)", México, Macrobit Editores, segunda edición, 1991.
- Catálogo Black Box; "TODO PARA CONECTIVIDAD", México, Primera Edición, 1995.
- IBM; "DICTIONARY OF COMPUTING", U.S.A., IBM BookMaster, Release 3.0, Ninth Edition (October 1991).
- IBM; "Local Area Network Concepts and Products", U.S.A., International Technical Support Centers, tercera edición, 1990.

Revistas

RED
 Año VII No. 98
 Noviembre 1998

Personal Computing
 Año 12 No. 134
 Julio 1999

Internet

UPS	http://www.mabis.com
UPS	http://www.tripplite.com
RED	http://www.red.com.mx
PERSONAL COMPUTING	http://www.percom.com.mx
Anixter, Inc	http://www.anixter.com
TIA (Telecommunication Industry Association)	http://www.tiaonline.org
3Com	http://www.3com.com
RedUNAM	http://www.dtd.unam.mx

VCI: Virtual Circuit Identifier.
 VLAN: Virtual Local Area Network (Redes virtuales de área local).
 VPI: Virtual Path Identifier.
 VTP: Virtual Terminal Protocolo (Protocolo de terminales virtuales).
 WAN: Wide Area Network.
 WWW: World Wide Web.

APÉNDICE B.

Bibliografía utilizada para el desarrollo de este trabajo:

- Jenquins Neil, Schatt Stan; "REDES DE ÁREA LOCAL (LAN)", México, Prentice Hall Hispanoamericana, S.A., 1996.
- Sheldon, Tomas, "LAN TIMES ENCYCLOPEDIA OF NETWORKING / TOM SHELDON", U.S.A., Osborne McGraw-Hill, 1994.
- Black,Unyles; "REDES DE COMPUTADORAS (Protocolos, Normas e Interfaces", México, Macrobit Editores, segunda edición, 1991.
- Catálogo Black Box; "TODO PARA CONECTIVIDAD", México, Primera Edición, 1995.
- IBM; "DICTIONARY OF COMPUTING", U.S.A., IBM BookMaster, Release 3.0, Ninth Edition (October 1991).
- IBM; "Local Area Network Concepts and Products", U.S.A., International Technical Support Centers, tercera edición, 1990.

Revistas

RED
 Año VII No. 98
 Noviembre 1998

Personal Computing
 Año 12 No. 134
 Julio 1999

Internet

UPS	http://www.mabis.com
UPS	http://www.triplite.com
RED	http://www.red.com.mx
PERSONAL COMPUTING	http://www.percom.com.mx
Anixter, Inc	http://www.anixter.com
TIA (Telecommunication Industry Association)	http://www.tiaonline.org
3Com	http://www.3com.com
RedUNAM	http://www.dtd.unam.mx