3
2

# UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

## ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

## A C A T L A N

# ANALISIS DE CONFIABILIDAD EN UNA RED DE AREA LOCAL



# T E S I S

QUE PARA OBTENER EL TITULO DE:

**LIC. EN MATEMATICAS APLICADAS Y C O M P U T A C I O N**

P R E S E N T A N :

**FRANCISCO ARGÜELLES ARREDONDO**
**RAUL BAÑUELOS PONCE**

ASESOR: RUBEN ROMERO RUIZ

NAUCALPAN, EDO. DE MEXICO ABRIL DE 1996



TESIS CON
FALLA DE ORIGEN

***AGRADECIMIENTOS.***

En esta parte de nuestro trabajo que es la última en escribirse, pero no por eso deja de ser de lo más importante se presentan en mi mente recuerdos de todo lo vivido para llegar hasta aquí, la conclusión oficial de nuestra licenciatura; los maestros que desde el primer día del primer semestre nos impartieron sus conocimientos, los compañeros que en aquel entonces eran desconocidos y que ahora representan grandes amigos, los desvelos para acreditar examenes que ahora nos harían reír, los deportes que practicamos dentro de la escuela, las fiestas y reuniones con amigos, las desmañanadas para las clases de las 7 am, en fin todo aquello que nos hace recordar a la ENEP Acatlán y que nunca por más que pase el tiempo olvidaremos. Así pues, Yo Francisco Argüelles Arredondo doy gracias a Dios por ayudarme siempre y en todo momento en estos años de vida.

A mis padres: Irene Arredondo y Roberto Argüelles por darme la oportunidad de vivir para lograr este pequeño triunfo. Quiero dedicarles este trabajo y compartir este éxito que también es de ellos.

A mis hermanos Roberto Flavio, Luis Enrique y Carlos Gabriel que sin sus consejos y su presión no habría realizado esta tesis.

A Araceli Luna, que siempre me apoyó y que sin ella la vida sería distinta.

A mi amigo inseparable ***Snoopy*** que siempre me ha acompañado en todo lugar y que sin su ayuda la vida en este planeta sería distinta.

A mi amigo Héctor Duque por quien siempre demostraré admiración.

A mi compañero y amigo durante toda la carrera Raúl, que sin él esta tésis no sería lo que es.

A mi amigo Ernesto Hernández que me dió mis primeras lecciones sobre redes de área local y por la amistad que me ha brindado hasta el día de hoy.

A E.T. por ayudarnos las noches en vela para la consecución de nuestros objetivos.

A todos aquellos que en alguna ocasión preguntaron y se interesaron por nuestro trabajo, **GRACIAS**.

***Francisco Argüelles Arredondo.***

Mis más sinceros agradecimientos:

A mis padres, Carlos Bañuelos y Reyna Ponce, por la oportunidad brindada para vivir esta experiencia, ya que sin ellos y sin Dios no existiría.

Los quiero mucho.

A mis hermanos, Marino e Israel, por ayudar a superarme día a día.

A todos mis profesores, por permitirme compartir una porción de sus conocimientos.

A Francisco Argüelles y Héctor Duque, por compartir buenas experiencias durante la Universidad.

A mi abuelita Rita, donde quiera que te encuentres.

A todos GRACIAS.

---

Oscar Meza y Luz María Lavín, gracias por brindarme su amistad, cariño y por compartir muchos momentos gratos e inolvidables.

Porque en ellos encontré dos grandes amigos, que me han enseñado a respetar y amar a mi pareja.

Son muy especiales.

Consolación Herrada, gracias por ser tan noble y paciente, por darme la fuerza para afrontar los obstáculos presentados durante el desarrollo de esta investigación.

Eres la persona que me impulsa a seguir en forma ascendante día con día.

Te amo.

---

Dedicatoria.

Para la persona más maravillosa que he conocido y que jamás igualará nadie.

Mi esposa.

A veces es increíble que teniendoté a mi lado no pueda expresarte cuanto te quiero. Este trabajo es una forma de expresarte mi amor.

*Raúl Bañuelos Ponce.*

# *INDICE*

**Objetivo.**

Examinar la confiabilidad de una LAN (Red de Area Local) en base a las distintas topologías existentes, y a los componentes que constituyen la misma.

**Hipótesis.**

La principal causa de fallas en una Red de Area Local se basa en la calidad del software, lo cual trae una disminución en la confiabilidad, aunado la resistencia de los componentes físicos de la red hacen que disminuya aún más la confiabilidad de la red.

**Hipótesis Alternativa.**

La redundancia (o el trabajo en paralelo) es un enfoque adecuado de la garantía de operación si el costo del tiempo que un sistema permanece inactivo es muy alto.

## INTRODUCCIÓN

"Eran las 3 de la mañana del 1º de noviembre de 1992. Las minicomputadoras de la marca Tandem existentes en Nueva Zelandia sufrieron un ataque de locura. Sus relojes internos se retrasaron cerca de nueve años, borraron transacciones financieras y obstruyeron servicios de transmisión de información en línea. Al tiempo que el sol se movía hacia el oeste, en dirección a Australia y Asia, los "bugs" ("bichos", palabra con que la jerga computacional llama a los errores de programación) despertaron súbitamente tal como lo hacen las esporas latentes.

Aquella no fue una noche tranquila para el principal fabricante de computadoras "tolerantes a errores" del mundo. Sin embargo, en sus oficinas centrales de Cupertino, California, el equipo de ingenieros de Tandem debió abandonar sus tibias camas para fumigar las máquinas. En poco tiempo se dio cuenta de que no había alguna esperanza de reparar el error antes de las 3:00 de la mañana, según lo indicaban los relojes de sus clientes en Europa, y pocas horas después, en América. De modo que debieron llegar a una solución de urgencia: aconsejaron a sus clientes apagar sus computadoras y luego volverlas a encender. La idea funcionó. Los relojes internos de las computadoras regresaron a la hora normal. Este fue un episodio muy vergonzoso para un producto conocido como NonStop CLX, un programa que nada podía detener.

Se trataba de un bug en el sistema operativo de Tandem -el software que dice a una computadora que operaciones llevar a cabo y en que orden-. Tandem aplastó el bug con prontitud y luego se dedico a escribir un clon del programa en el que el error no volviera a ocurrir. Para ello Tandem apartó un banco de sus computadoras, en las que instaló varios programas de aplicaciones utilizados por sus clientes, y puso las máquinas a trabajar programadas con fechas futuras. Desea eliminar el riesgo de que otro bug similar se "escabulla y ataque a sus máquinas"[1].(sic)

---

[1] Tomado de el Excelsior Sección Financiera 25 de abril de 1994. Página 6-F

Lo anterior es una clara muestra de lo que puede pasar en un sistema de cómputo, si bien se sabe, que ningún sistema de cómputo es 100% seguro y a prueba de errores, también se sabe que mediante la redundancia según el estudio presentado en este trabajo ayuda en mucho a los componentes del hardware. Pero, sin embargo en el software no se puede hacer la misma redundancia que en los componentes físicos.

Podemos considerar que en programas muy complejos y fuertemente relacionales con subsistemas que reaccionan con rapidez, de modo que un error se multiplica como avalancha, por ejemplo en los sistemas financieros, los sistemas telefónicos y los sistemas para el control de tráfico aéreo ocupan el tercer lugar en esta lista. Sobre estos últimos se puede agregar que los actuales sistemas ofrecen la oportunidad de que intervengan los humanos, pero los que están previstos para el futuro supuestamente manejarán flujos de tráfico más grandes, y no resulta obvia la manera en que los humanos puedan manipularlos.

Algunos bugs son, por naturaleza, casi imposibles de hallar en los laberintos de un programa de cómputo, uno de los primeros programas jamás escritos, en 1949, tenía 20 bugs en solo 126 líneas de código. Mucho más tarde, un ingeniero tardó más de diez años en descubrir al último de esos bichos.

La compañía Walgreen Co. en 1992 puso a trabajar a decenas de programadores durante tres días de pánico; los ingenieros debían encontrar una cura aunque fuera temporal, a la presencia de un bug que apareció en un programa de lectores ópticos de códigos de barras. El bug causó que cajas registradoras, a intervalos irregulares, tomaran un precio equivocado de la memoria central. Un comprador minorista no se encuentra en condiciones de pagar por esos errores, de modo que Walgreen debió retirar su enorme sistema de control de inventarios durante seis meses hasta encontrar una cura permanente al error, lo que logró con ayuda de Ernst & Young.

Desde hace algunos años la microcomputación ha tenido un gran auge en nuestro país, pues la mayoría de las empresas cuentan, por lo regular, con varios de estos equipos.

Debido a la necesidad de transferir información de una manera rápida y eficiente, esto aunado a las ventajas de compartir recursos (muchas de las veces de alto costo), las compañías que cuentan con estos equipos se han visto en la necesidad de instalar Redes de Área Local.

Desafortunadamente aún no se cuenta con el personal suficiente para dar una buena asesoría y menos llevar a cabo la correcta instalación de estos equipos, y si a esto le agregamos que no existen libros o manuales que capaciten en forma totalmente adecuada a las personas interesadas en el tema, llegamos a la conclusión de que es necesario recopilar la información de tal manera que se facilite el aprendizaje.

La finalidad de este trabajo es la de orientar en forma sencilla y práctica sobre las diferentes opciones del hardware, para una adecuada elección e instalación, así como la correcta conexión del software, tanto para las personas que se inician en este basto campo, como para los que cuentan ya con algunos conocimientos.

Cuando desarrollamos el capitulado de esta investigación se tuvo en mente un esquema quizás diferente, pero el resultado final del trabajo nos deja profunadamente satisfechos con los resultados.

En el primer capítulo se describe el enfoque con el cual se entenderá la investigación, es decir se definen conceptos que para algunas personas que lean este trabajo les servirán de base para un fácil entendimiento de los capítulos siguientes. Se describe que es una red de área local, la forma de conectar computadoras, algunos aspectos de los que es la teoría de confiabilidad tales como sistemas en serie y paralelo, distribuciones de confiabilidad, etc. De esta forma en este capítulo lo que se pretende es arrancar de cero en el estudio de una red de área local o bien proporcionar un breve cursillo sobre redes.

Para el capítulo dos se empieza por hacer un análisis exhaustivo de los componentes físicos que constituyen la red, tal es el caso de tarjetas, cables, concentradores, etc. lo cual nos ofrecerá una forma de comparar diversos equipos y marcas que en algún momento podrían ser de utilidad. Se analiza la probabilidad de que los equipos fallen así como su tiempo promedio de fallas.

Dentro del capítulo tres se analizan los factores o elementos que conforman la red desde el punto de vista del software, tales como protocolos, sistemas operativos y fundamentalmente el desarrollo de las aplicaciones que trabajan en un entorno de red. El análisis de la confiabilidad en este capítulo se hace en base a los factores que influyen dentro de la red, es decir la aplicación y su relación con el sistema operativo, así como la utilización de los protocolos de los sistemas operativos.

El capítulo cuatro abarca el análisis de confiabilidad del software y hardware en conjunto, es decir que los principales factores que influyen en una red o bien los que dan el soporte a la red son estudiados a manera de un ejemplo en un breve estudio de la red de la ENEP Acatlán, en donde se aborda su descripción técnica así como el diagrama de conectividad de la red del plantel.

Por último se exponen conclusiones de la investigación y se ofrece un glosario de términos técnicos de los cuales no todos se utilizan en la tésis pero servirán a aquellas personas interesadas en el manejo de computadoras.

# CAPITULO I

## FUNDAMENTOS DE LA TEORÍA DE CONFIABILIDAD Y REDES

# FÚNDAMENTOS DE LA TEORÍA DE CONFIABILIDAD Y REDES

**RED.** Una red es un grupo de computadoras (y terminales, en general) interconectadas a través de uno o varios caminos o medios de transmisión. Su finalidad es transferir e intercambiar datos entre computadoras y terminales así como compartir recursos.

## 1.1 HISTORIA DE LAS REDES DE AREA LOCAL.

Para poder comprender el porque del auge de las Redes en Área Local, es conveniente hacer una reseña histórica del surgimiento de este tipo de sistemas.

Este análisis lo comenzaremos tomando en cuenta a partir de las década de los 70's, para ser más exactos a mediados, es cuando toma un impulso fuerte la tecnología del silicón (silicio) y la integración en miniatura de los componentes electrónicos que permitió a los fabricantes de computadoras construir "mayor inteligencia" en máquinas más pequeñas.

Estas máquinas llamadas microcomputadoras descongestionaron a las viejas máquinas centrales. A partir de este momento cada usuario tenía su propia microcomputadora en su escritorio.

A principios de la década de los 80's las microcomputadoras habían revolucionado por completo el concepto de la computación electrónica así como sus aplicaciones y mercado. Sin embargo los gerentes de los departamentos de informática fueron perdiendo el control de la información puesto que el proceso de la misma no estaba centralizado.

Otra de las dificultades o inconvenientes que se presentaron en esta época fue la poca capacidad de los disquetes, por lo que para transferir información de una micro a otra, era necesario llevar una gran cantidad de estos dispositivos de almacenamiento y aún más si la cantidad de información era muy grande.

Con la llegada de la tecnología Winchester se lograron dispositivos que permitían almacenar grandes cantidades de información, capacidades que iban desde 5 megabytes hasta 100 megabytes. Una desventaja de esta tecnología era el alto costo que significaba la adquisición de un disco duro. Además, los usuarios tenían la necesidad de compartir información y programas en forma simultánea.

Estas razones, principalmente, aunadas a otras como poder compartir recursos de relativa baja utilización y alto costo, llevó a diversos fabricantes y desarrolladores a la idea de las redes locales.

En un principio, las redes de microcomputadoras se formaban por simples conexiones que permitían a un usuario accesar recursos que se encontraban residentes en otra microcomputadora tales como los discos duros, impresoras, etc. Estos equipos permitían a cada usuario el mismo acceso a todas las partes de un disco causando obvios problemas de seguridad y de integridad en los datos.

Hacia 1983, la compañía Novell Inc. fue la primera en introducir el concepto "File Server", en el que todos los usuarios pueden tener acceso a la misma información, compartiendo archivos y contando con niveles de seguridad.

En el concepto de file server, un usuario no puede accesar a discos que se encuentren en otras microcomputadoras indistintamente. El file server es una microcomputadora designada como administrador de los recursos comunes. Al hacer esto, se logra una verdadera eficiencia en el uso de estos recursos así como una total integridad de los datos. Los archivos y programas pueden ser accesados en modo multiusuario guardando el orden de actualización por el procedimiento de bloqueo de registros. Es decir, cuando algún usuario se encuentra actualizando un registro, éste se bloquea para evitar que algún otro usuario lo extraiga o intente actualizar.

En la actualidad el concepto tuvo una variación al concepro cliente-servidor en el que se mantiene la premisa de que lo más importante para crear una red es el sistema operativo.

Novell basó su investigación y desarrollo en la idea de que es el Software de la red y no el Hardware el que hace la diferencia en la operación de una red, situación que se ha podido constatar. En la actualidad Novell soporta más de 100 tipos de redes.

Durante los años entre 1985 y la actualidad, las redes lucharon por colocarse como una tecnología reconocida contra todo tipo de adversidades. En un principio IBM no reconocía a las redes basadas en microcomputadoras como equipo confiable.

Había inclusive gentes que llegaban a declarar que las microcomputadoras habían sido concebidas siempre como islas de información en las que el usuario debería tener al alcance de su escritorio todos los elementos para constituir un pequeño centro de cómputo autosuficiente. No es sino hasta la exhibición COMDEX de 1987 cuando IBM acepta esta tecnología como el reto del futuro y acuña el término "conectividad". Después de este evento empieza un crecimiento acelerado de la industria de las redes locales. Todos los fabricantes se lanzan a adaptar sus equipos y a proponer nuevas posibilidades de conectividad. Las tendencias actuales indican una definitiva orientación hacia la conectividad de datos. No sólo en el envío de información de una computadora a otra sino, sobre todo, en la distribución del procesamiento a lo largo de grandes redes en toda la empresa.

En la actualidad existe un gran interés por parte de todo tipo de usuarios en las redes locales. El reto importante para los desarrolladores de esta tecnología es el ofrecer productos confiables, de alto rendimiento que hagan uso de la base instalada ya en el usuario final.

A este último concepto se le denomina tecnología de protocolo abierto. Es decir, ofrecer a los usuarios soluciones de conectividad que sean compatibles con el hardware y el software ya adoptado por el usuario sin importar su marca, sistema operativo o protocolo de comunicación que utilicen.

Novell, por ejemplo, ofrece desde hace algún tiempo el concepto de Conectividad Universal bajo Netware, según el cual es posible integrar sistemas

operativos anteriormente incompatibles como VMS, Unix, DOS, Macintosh comunicándose por medio de una gran variedad posible de protocolos como TCP/IP, IPX, X25, Netbios, etc.

## 1.2 REDES DE ÁREA LOCAL.

### 1.2.1 Tipos de Redes.

Diferentes tipos de redes:

**ARCNET.** Esta red es muy popular en México y de bajo costo, auque debido al la tecnología imperante es viable que salga ya del mercado. Tiene componentes básicos, tarjetas de red y repetidores.

* Tarjeta Arcnet (8 bits, para PC, XT, AT, 386 y PS/2 25 y 30).
* Tarjeta Arcnet PS/2 (para PS/2 50 en adelante).
* Repetidor pasivo (4 nodos, 30 metros por nodo).
* Repetidor activo (8 nodos, 600 metros por nodo).
* Cable coaxial RG-62 (tipo videocassettera).

Reglas:

* Distancia máxima entre activo y pasivo: 30 metros.
* De 1 pasivo a cualquier dispositivo (PC, servidor de archivos o repetidor activo) la distancia máxima es de 30 metros.
* De 1 activo a todo es de 600 metros.

**ETHERNET.** Esta red se recomienda para trabajos pesados con mucho tráfico en el canal de comunicaciones y con acceso constante a disco duro. La velocidad de transferencia de los datos en el cable de comunicación es de 10 Mbps. Existen en el mercado nuevas tecnologías para la red Ethernet, es decir, mejoras en cuanto al rendimiento ya sea por medio de equipos de switcheo o bien por los cables de nivel 5 que permiten la transmisión de videoconferencias, voz, datos, etc.

Se prevé que se popularice una variante de esta red, el llamado Fast-Ethernet que utiliza velocidades de transmisión de 100 Mbps pero conserva los mismos problemas de Ethernet como son colisiones y saturación del canal de comunicación.

* La topología de este tipo de red es en bus lineal, las estaciones de trabajo se van anexando al troncal de cable coaxial con conectores tipo "T". El único componente son las tarjetas de red.
* Tarjeta Ethernet (servidor de archivos y estación de trabajo PC, XT, AT ó 386).
* Tarjeta Ethernet PS/2 (servidor de archivos y estación de trabajo PS/2).
* Tarjeta Ethernet Plus ( Servidor de archivos, AT y 386).
* Cable coaxial RG-58.
* Cable de par trenzado.
* Soporta 300 metros en el bus sin amplificador.
* Amplificador sencillo de un segmento para ampliar el bus 300 metros.

Existen nuevas tecnologías que se conocen como ATM (Modo de transmisión asíncrona), FastEthernet, 100VG, FDDI y alguna más que se prevé que se popularicen en un futuro muy cercano; pero por los costos que representa el cambiar a esas tecnologías probablemente se retracen, en especial ATM.

#### 1.2.1.1 Redes Jerárquicas.

Este tipo de redes se encuentran frecuentemente en las instalaciones de microcomputadoras principales o de minicomputadoras. Los usuarios acceden a la microcomputadora a través de terminales satélites (llamadas terminales "tontas", porque no pueden realizar ningún proceso por si mismas). El propósito básico de una terminal tonta es simplemente proporcionar una interfaz entre la microcomputadora anfitrión y los usuarios. Este es el tipo de red de las minicomputadoras y mainframes, es decir de redes tipo multiusuario.

Las redes jerárquicas proporcionan un proceso centralizado pero a la vez están limitadas en los siguientes puntos:

- Los usuarios del procesador central están limitados por las aplicaciones del anfitrión.

- La habilidad de los usuarios para realizar procesos de análisis está condicionada.

- Los cambios del servidor son muy costosos.

- Son grandes consumidores de tiempo.

- Los programas del servidor deben satisfacer a todos los usuarios de la red.

Con el abaratamiento de los procesadores, la capacidad de cálculo (en la forma de microcomputadoras personales) pudo colocarse en puestos de trabajo individuales y con esto surgieron: Las Redes Emparejadas.

### 1.2.1.2 Redes Emparejadas, tal como son las Redes de Área Local (LAN, Local Área Network).

Son microcomputadoras personales que permiten al usuario personalizar el logical y realizar los análisis de los datos que satisfagan sus necesidades concretas. Sin embargo, por separado, las microcomputadoras aisladas no ofrecen el acceso directo a los datos de la microcomputadora principal o servidor, no pueden compartir fácilmente la información ni los programas y la comunicación se basa en el sistema operativo.

Las redes de área local proporcionan una solución tanto a las limitaciones con microcomputadoras personales aisladas como a las centralizadas; son pares de redes, lo que significa que todos los dispositivos en la red pueden comunicarse entre ellos. En lugar de terminales tontas, también utilizan terminales inteligentes (porque tienen su propia unidad central de proceso). Las redes de área local proporcionan un puente no sólo entre las personas y la información, sino además entre los mismos ususrios individualmente.

### 1.2.2 Principales Atributos de una Red de Área Local.

Son muchos los atributos de una Red de Área Local, pero entre los de mayor importancia podemos mencionar los siguientes:

- Las conexiones entre las estaciones de trabajo suelen tener longitudes comprendidas entre algunos cientos de metros y varios kilómetros.

- Una red local transmite datos entre estaciones de usuario y computadoras (aunque algunas redes pueden transportar también imágenes y sonido).

- La capacidad de transmisión de una red local suele ser mayor que la de una red extensa o red de área ancha: las velocidades de transmisión suelen estar comprendidas entre 1 Mbit/seg y 20 Mbits/seg.

- El canal de la red suele ser propiedad de la misma organización que la utiliza.

- La tasa de errores de una red local suele ser considerablemente menor que la del canal telefónico orientado a redes extensas.

### 1.2.3 Ventajas de utilizar una Red de Área Local.

1. El costo del equipo físico, incluyendo la capacidad de compartir los dispositivos periféricos tales como las impresoras costosas, los discos de gran capacidad, los dispositivos especiales y los dispositivos de comunicaciones.

2. El Usuario, tienen la facilidad de comunicarse con distintas personas y grupos a través del empleo del correo electrónico y otros tipos de software.

3. Mantenimiento, éste incluye la capacidad de compartir los servicios de mantenimiento tales como los procesos de salvado de seguridad y todo el software de la instalación.

4. Las redes pueden resolver también un problema de especial importancia: la tolerancia ante fallas. En caso de que una terminal falle, otra puede asumir sus funciones y su carga de trabajo.

5. El empleo de redes confiere una gran flexibilidad a los entornos laborales. Los empleado pueden trabajar desde sus casas, utilizando terminales conectadas a la red de la oficina.

### 1.2.4 Construcción de una Red de Área Local.

Para construir una red de área local hay que considerar cinco puntos básicos:

- Seleccionar la topología y el equipo físico (hardware): Es diseñar la arquitectura física de la red. Trabajando con un instalador de redes, debe decidirse en cuales oficinas o locales deben tenderse los cables y los dispositivos claves (servidor).

- Instalar el equipo físico y el sistema operativo de la red: Es instalar el equipo físico y unir las microcomputadoras con los cables y las tarjetas de interfaz. Debe instalarse el Sistema Operativo adecuado en el disco duro de la máquina que se elege como servidor, configurándolo para reconocer los demás dispositivos.

- Configurar el sistema y cargar las aplicaciones: Esto es crear la estructura del subdirectorio y organizar el disco duro para preparar la carga de la aplicación y de otros datos.

- Crear el entorno del usuario: Esto es lo que se ve y se "siente" del sistema, a través de las pantallas que van apareciendo a partir de cuando el

usuario inicia la sesión y de los menús que ayudan y guían al usuario entre las muchas opciones disponibles.

- Establecer una administración de la red: en este paso se necesita establecer los procedimientos de soporte de la red.

- Actualmente el entorno de red para un usuario es de lo más amigable posible, el usuario tiene un drive lógico que pertenece a la red, pero el usuario lo "siente" como si estuviera físicamente en su máquina.

## 1.3 TOPOLOGÍAS MAS COMUNES.

La Topología de una red hace referencia a la ruta por la que discurren los datos a través de la red, el concepto "topología" es un concepto geométrico que alude al aspecto de una cosa. La topología es la forma (la conectividad física) de la red. A la hora de establecer la topología de una red, el diseñador ha de plantearse tres objetivos principales:

- Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico. Es decir, la capacidad que tiene una red para transportar datos correctamente.
- Encaminar el tráfico entre el ETD (equipo terminal de datos) transmisor y el receptor a través del camino más económico dentro de la red.
- Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo.

Las topologías más comunes que podemos encontrar en el desarrollo de redes de área local son cinco;

- Topología Jerárquica (árbol).
- Topología Horizontal (bus).
- Topología en Estrella.

- Topología en Anillo.
- Topología en Malla.

### 1.3.1 Topología Jerárquica.

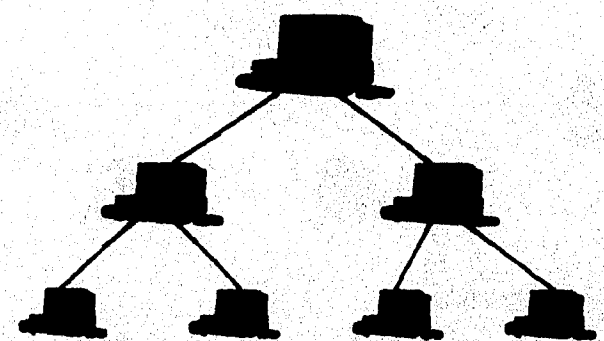
La estructura jerárquica es una de las más extendidas en la actualidad. El software que controla la red es relativamente simple, y la topología proporciona un punto de concentración de las tareas de control y resolución de errores. En la mayoría de los casos, la computadora situada en el nivel más elevado de la jerarquía es la que controla la red. Muchos fabricantes incorporan a esta topología un cierto carácter distributivo, dotando a las estaciones subordinadas de un control directo sobre las estaciones situadas en niveles inferiores dentro de la jerarquía, lo cual reduce la carga de trabajo al nodo que se encuentra en la parte superior.

Aunque la topología jerárquica resulta interesante por ser fácil de controlar, puede presentar ciertos problemas en cuanto a la posibilidad de aparición de cuellos de botella. En determinadas situaciones, la computadora del nivel más elevado, normalmente una gran computadorar central, ha de controlar todo el tráfico entre los distintos integrantes de la red. Este hecho no sólo puede crear saturaciones de datos, sino que además plantea ciertos problemas de fiabilidad. Si este computador falla, toda la red deja de funcionar, a no ser que exista otra computadora de reserva que sea capaz de hacerse cargo de todas las funciones de la computadora averiada. Pese a todo, las topologías jerárquicas han venido usándose ampliamente desde hace bastantes años, y seguirán usándose durante mucho tiempo, ya que permiten la evolución gradual hacia una red más compleja, puesto que la adición de las nuevas terminales subordinadas es relativamente sencilla.

Las redes con topología jerárquica se conocen también como redes verticales o en árbol. La palabra "árbol" alude al hecho de que su estructura se

parece bastante a un árbol cuyas ramas van abriéndose desde el nivel superior hasta el más bajo. Las ventajas y desventajas de una red vertical de comunicaciones son más o menos las mismas que las de una empresa estructurada jerárquicamente, líneas de autoridad muy claras con cuellos de botella frecuentes en los niveles superiores, y a menudo una insuficiente delegación de responsabilidad, cabe mencionar que este tipo de redes son básicamente para multiusuario.

**TOPOLOGÍA JERÁRQUICA**

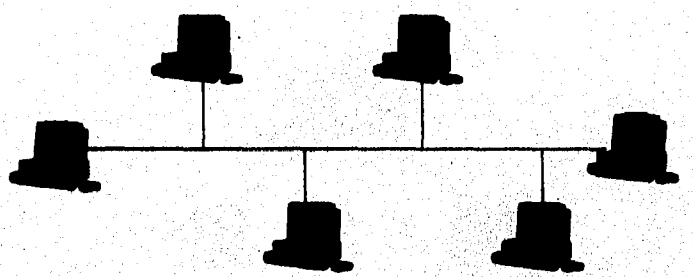


### 1.3.2 Topología Horizontal (BUS).

Esta topología es frecuente en las Redes de Área Local. Es relativamente fácil controlar el flujo de tráfico entre los distintos componentes, ya que el bus permite que todas las estaciones reciban todas las transmisiones, es decir, una estación puede difundir la información a todas las demás. La principal limitación de una topología horizontal es el hecho de que existe un sólo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si el canal de comunicaciones falla, toda la red deja de funcionar. Algunos fabricantes

proporcionan canales completamente redundantes por si falla el canal principal, y algunos ofrecen conmutadores que permiten rodear (by pass) un nodo en caso de que falle. Otro inconveniente de esta configuración estriba en la dificultad de aislar las averías de los componentes individuales conectados al bus. La falta de puntos de concentración complica la resolución de este tipo de problemas.

**TOPOLOGÍA HORIZONTAL (BUS)**



### 1.3.3 Topología en Estrella.

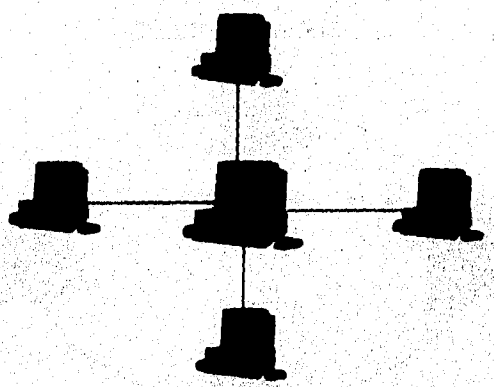
La topología en estrella es una de las más empleadas en los sistemas de comunicación de datos. Una de las principales razones de su empleo es histórica. Su software no es complicado y su flujo de tráfico es sencillo. Todo el tráfico emana del núcleo de la estrella, que es el nodo central, por lo general una microcomputadora, que posee el control total de las estaciones conectadas a él. La configuración en estrella es, por tanto, una estructura muy similar a la de la topología jerárquica, aunque su capacidad de procesamiento distribuido es limitada.

El nodo central es el encargado de encaminar el tráfico hacia el resto de los componentes; se encarga, además, de localizar las averías. Esta tarea es sencilla

en el caso de ésta topología, ya que es posible aislar las líneas para identificar el problema. Sin embargo, y al igual que en la estructura jerárquica, una red puede sufrir saturaciones y problemas en el caso de avería del nodo central. Algunas redes en estrella construidas en los años setenta experimentaron serios problemas de confiabilidad, debido a su carácter centralizado. En otros sistemas se estableció redundancia en el nodo central, como medida de seguridad, con lo cual la confiabilidad aumentó considerablemente.

En una red estrella todas las estaciones de trabajo están conectadas al servidor, pero no entre ellas.

**TOPOLOGÍA EN ESTRELLA**



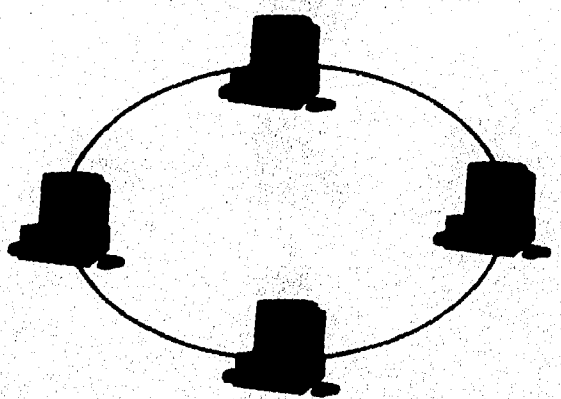
### 1.3.4 Topología en Anillo.

En una red de anillo el cableado va de estación en estación (y al servidor) sin que haya un principio ni un final.

Está topología es llamada así por el aspecto circular del flujo de datos. En la mayoría de los casos, los datos fluyen en una sola dirección, y cada estación recibe la señal y la retransmite a la siguiente del anillo. La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos, tan frecuentes en los sistemas en estrella o en árbol. Además la lógica necesaria para

poner en marcha una red de este tipo es relativamente simple. Cada componente sólo ha de llevar a cabo una serie de tareas muy sencillas: aceptar los datos, enviarlos al servidor de la red o retransmitirlos al siguiente componente del mismo. Sin embargo, como todas las redes, la red en anillo tiene algunos defectos. El problema más importante es que todos los componentes del anillo están unidos por un mismo canal. Si falla el canal entre dos nodos, toda la red se interrumpe. Por eso algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se pierde algún canal. Otros fabricantes construyen conmutadores que redirigen los datos automáticamente, saltándose el nodo averiado, hasta el siguiente nodo del anillo, con el fin de evitar que la falla afecte a toda la red.

**TOPOLOGÍA EN ANILLO**

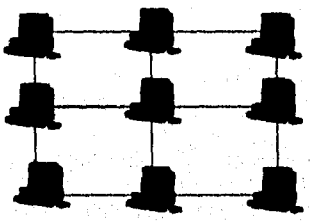


### 1.3.5 Topología en Malla.

La topología en malla se ha venido empleando en los últimos años. Lo que la hace atractiva es su relativa inmunidad a los problemas de embotellamiento y averías. Gracias a la multiplicidad de caminos que ofrece a través de los distintos componentes, es posible orientar el tráfico por trayectorias alternativas en caso de que algún nodo este averiado u ocupado. A pesar que la realización de este método es complejo y caro (para proporcionar estas funciones especiales, la lógica de control de los protocolos de una red en malla puede llegar a ser

sumamente complicada), muchos usuarios prefieren la fiabilidad de una red en malla a otras alternativas.

**TOPOLOGÍA EN MALLA**



## 1.4 DEFINICIÓN DE CONFIABILIDAD.

La Teoría de Confiabilidad es la ciencia que estudia las leyes de ocurrencia de fallas en equipo técnico.

**"Confiabilidad es la capacidad del equipo para preservar sus características de salida (parámetros) dentro de los límites establecidos bajo ciertas condiciones de operación dadas. "[1]**

**Existen muchas otras definiciones de confiabilidad que dependen de los conceptos fundamentales que se utilizan para ser formuladas. Todas las definiciones de confiabilidad pueden ser divididas en dos grupos esenciales diferentes; el primer grupo contiene definiciones cuantitativas, y el segundo grupo contiene definiciones cualitativas.**

**Una definición del primer grupo:**

[1] "Fundamentals of Reliability Theory", A.M. Polovko. Ed. Academic Press. pag.1

"Probabilidad de que determinado elemento desempeñará satisfactoriamente la función a la que se le destina, durante un período determinado y en condiciones especificadas".

Una definición del segundo grupo:

" Un producto confiable es aquel que desempeñará la función que tiene designada cuando se requiera que lo haga, durante su período de uso".

La medida de confiabilidad de un sistema es la frecuencia con que sus fallas ocurren en el tiempo.

La confiabilidad define estabilidad porque permite establecer la extensión en la cual un experimento, prueba o procedimiento de medición produce los mismos resultados en ensayos repetidos (muestreo repetido).

En general, el concepto de CONFIABILIDAD está definido como una probabilidad e implica la necesidad de enunciar con precisión qué constituye una falla.

### 1.4.1 Elementos del concepto confiabilidad.

De acuerdo con la International Electrotechnical Commission Standard 271-1974.

"La confiabilidad cuantitativa es la probabilidad de que una unidad desempeñe una función requerida bajo condiciones establecidas en un período establecido".

En el concepto de la confiabilidad existen cuatro elementos significativos:

**1. Probabilidad.** En este se toma en cuenta la variación que transforma la confiabilidad en una probabilidad. Es decir de unidad a unidad de un mismo producto se presentan variaciones lo que lleva a tomar el promedio de duración del producto.[2]

**2. Rendimiento.** La confiabilidad indica una característica de calidad de rendimiento, para que un producto ofrezca seguridad, debe satisfacer cierta función o desempeñar un trabajo en el momento que se le reclame.

**3. Tiempo.** La confiabilidad, establecida como una probabilidad de que el producto desempeñe una función, debe de identificarse con un determinado período de tiempo. (Ninguna unidad es eterna).

**4. Condiciones.** En estas se incluye la aplicación y las circunstancias de operación bajo las cuales se emplea el producto. Las condiciones de operación que "soporta" un producto o sistema pueden afectar en alto grado su margen de empleo y su rendimiento. (Ninguna unidad es para todo).

La falla de mecanismo se puede definir como la serie de acontecimientos cronológicos que lógicamente contribuyen a producir una falla.

### 1.4.2 Análisis de confiabilidad de un sistema.

El análisis de confiabilidad de un sistema consiste en:
1) Analizar el sistema y decidir si los eventos en consideración están conectados lógicamente mediante relaciones "y" u "o".

2) Si los eventos están relacionados por "y" el conjunto de interés está dado por:

[2] Por lo tanto, debe ser posible identificar distribuciones de frecuencia en las fallas del producto, que permitan predecir la duración de vida de las unidades del mismo.

$$\{A\} = \{A_1, A_2, A_3, \ldots A_n\}$$

$$P\{A\} = P\{A_1, A_2, A_3, \ldots A_n\}$$

Son estocásticamente independientes

$$P\{A\} = P\{A1\}P\{A2\}P\{A3\}\ldots P\{An\}$$

$$P\{A\} = \prod_{i=1}^{n} P\{Ai\}$$

3) Si los eventos están relacionados por "o" el conjunto de interés está dado por:

$$\{A\} = \{A_1 \cup A_2 \cup \ldots \cup A_n\}$$

Los eventos son mútuamente excluyentes

$$P\left\{\bigcup_{i=1}^{n} A_i\right\} = \sum_{i=1}^{n} P\{A_i\}$$

### 1.4.3 Cálculo elemental de la confiabilidad de un sistema.

Para mostrar el procedimiento que se sigue en la obtención de la confiabilidad de un sistema, consideremos los siguientes puntos:

-Sea un sistema representado por un diagrama de bloques.

-Cada bloque representa una componente o parte del sistema.

-Cada bloque está "bien" o está "mal"; es decir cada bloque es un dispositivo que está cerrado (bueno) o está abierto (malo).

-Todos los subexperimentos asociados con cada bloque son estocásticamente independientes.

Además consideremos:

- Que el sistema es un circuito.
- El propósito del sistema es pasar corriente.
- Cada bloque es un contacto de relevo.

Una vez que se hicieron las consideraciones pertinentes, podemos continuar con la representación de los diferentes eventos que intervienen en el cálculo de la confiabilidad, sean:

R: Confiabilidad del sistema.

F: Evento de que el sistema falle (circuito abierto).

F': Evento de que el sistema no falle (circuito cerrado).

$F_x$: Evento de que el bloque X esté mal (dispositivo abierto).

$F_x'$: Evento de que el bloque X esté bien (dispositivo cerrado).

Entonces:

$$p_x = P\{F_x'\} \; ; \; q_x = P\{F_x\} \; ; \; p_x + q_x = 1$$

$$R = P\{F'\} \; ; \; Q = P\{F\} = 1 - P\{F'\} = 1 - R$$

## 1.6 Sistemas en Serie y en Paralelo.

### 1.6.1 Circuitos en SERIE.

Un sistema en Serie es una configuración sencilla y común. La característica esencial de este tipo de sistema es que si alguno de sus componentes falla el sistema no funcionará. Esto es, todas las componentes tendrán que funcionar correctamente para que el sistema cumpla su función.

La estructura que presenta este tipo de sistemas es la siguiente:


Entonces la confiabilidad está dada por:

$$R = P\{\text{Circuito cerrado}\} = P\{F_1' F_2' F_3' F_4' F_5'\} = p_1 p_2 p_3 p_4 p_5$$

y la probabilidad de que el sistema falle

$$Q = P\{\text{Circuito abierto}\} = P\{F_1 F_2 F_3 F_4 F_5\}$$

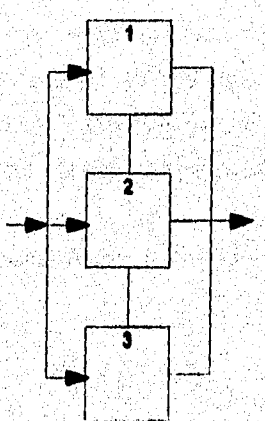
Alternativamente $Q = P\{F\} = 1 - P\{F'\} = 1 - p_1 p_2 p_3 p_4 p_5$

Aproximación para el cálculo de la probabilidad de falla del sistema:

$$P\left\{\bigcup_{i=1}^{n} F_i\right\} \cong \sum_{i=1}^{n} P\{F_i\}$$

**1.5.2 Circuitos en PARALELO.**

Un sistema en paralelo se define como un sistema que funcionará correctamente si al menos alguna de sus componentes funciona correctamente, en otras palabras, el sistema fallará únicamente si todas sus componentes fallan al mismo tiempo.




Entonces la confiabilidad está dada por:

$$R = P\{F_1' \cup F_2' \cup F_3'\}$$

la probabilidad de que el sistema falle es:

$$Q = P\{F_1F_2F_3\} = q_1q_2q_3$$

$$R + Q = 1 \Rightarrow R = 1 - q_1q_2q_3$$

El paralelismo o redundancia de los componentes cuando sólo uno es necesario puede parecer un desperdicio; sin embargo, en la práctica permite una mayor confianza en el sistema.

**1.5.3 Confiabilidad como función del tiempo.**
**Consideraciones:**

**- Una componente (o un conjunto completo de componentes armados en un sistema) se pone bajo un tiempo de tensión; por ejemplo:**

**i) Un instrumento electrónico puesto en servicio.**

**- Se puede definir un estado de "falla" para cualquier componente del sistema; esto es:**

**i) El instrumento puede dejar de funcionar.**

**- La componente se pone bajo condiciones de tensión a un tiempo determinado t=0 y se observa hasta que falla.**

**- Al tiempo para fallar o duración se le llamar T y se le puede considerar una v.a. continua con una función de probabilidad "f".**

**- El valor de T no se puede predecir mediante un modelo determinístico ya que componentes idénticos sometidos a esfuerzos idénticos fallan en tiempos diferentes e impredecibles.**

**- El modelo probabilístico con T como v.a. es el enfoque realista.**

Definición. La confiabilidad de una componente (o sistema) está definida como R(t) = P{T>t} donde T es la duración del componente y R es la función de confiabilidad.

Es decir, la confiabilidad de una componente es igual a la probabilidad de que la componente no falle durante el intervalo [0,t]. La confiabilidad es igual a la probabilidad de que la componente esté funcionando después del tiempo t.

Consideremos a la función de densidad de probabilidad de T, y sea:

$R(t) = \int_t^{\infty} f(s)ds$ y con la función de distribución acumulada de T

$$\Rightarrow R(t) = 1 - P(T \le t) = 1 - F(t) \ldots\ldots\ldots(1)$$

- Tasa de falla. Función de riesgo.

Definición. La tasa de falla Z (instantánea) o función de riesgo asociada con la v.a. T está dada por:

$$Z(t) = \frac{f(t)}{[1 - f(t)]}$$ utilizando la ec. (1) y sustituyendo tenemos:

$$= \frac{f(t)}{R(t)}$$

Interpretación de Z.

- Considerando la probabilidad condicional

$$P\{t < T < \Delta t + t / T > t\}$$

Probabilidad de que la componente falle durante las próximas Δt unidades de tiempo dado que la componente está funcionando en el instante t.

Aplicando la definición de probabilidad condicional

$$P\{t < T < t + \Delta t / T > t\} = \frac{\text{Probabilidad conjunta}}{\text{Probabilidad marginal}}$$

$$= P\{t<T<t+\Delta t/T>t\}$$

$$= \frac{\int_t^{t+\Delta t} f(s)ds}{R(t)}$$

$$= \frac{\Delta t f(\xi)}{R(t)} = \Delta t Z(t)$$

donde

$t \le \xi \le t+\Delta t$ para $\Delta t \to 0$ y $f$ continua

con la $\xi$ considerada como un valor muy pequeño

$\Delta t \cdot Z(t)$: proporción de componentes que estará entre $t+\Delta t$ de entre aquellas componentes que aún funcionan en el instante t.

**NOTA: La función de densidad de la duración (f.d.p. de T) determina unívocamente la tasa de falla (Z), la tasa de falla determina unívocamente la función de densidad de la duración.**

**Teorema. Si el tiempo para fallar es una v.a. continua con f.d.p. dada f y F(0) = 0 en donde F es la f.d.a. de T, entonces f puede expresarse mediante la tasa de falla Z como sigue:**

$$f(t) = Z(t) \cdot e^{-\int_0^t Z(s)ds}$$

**Demostración:**

**Puesto que**

$$R(t) = 1 - F(t)$$

$$R'(t) = -F'(t) = -f(t)$$

$$\Rightarrow Z(t) = \frac{f(t)}{R(t)} = \frac{-R'(t)}{R(t)}$$

**e integrando ambos miembros en el intervalo de 0 a t**

$$\int_0^t Z(s)ds = \int_0^t \frac{R'(s)}{R(s)}ds = -\ln\left[R(s)\right]_0^t$$
$$= -\ln\left[R(t)\right] + \ln\left[R(0)\right]$$
$$= -\ln\left[R(t)\right]$$

esto dado que $\ln\left[R(0)\right] = 0$ si y sólo si $R(0) = 1$, condición que se satisface si $F(0) = 0$, (probabilidad de falla inicial). En consecuencia

$$R(t) = e^{-\int_0^t z(s)ds}$$
$$\Rightarrow f(t) = F'(t) = \frac{d}{dt}\left[1 - R(t)\right]$$
$$= f(t) = Z(t)e^{-\int_0^t z(s)ds}$$

Relación entre la función de confiabilidad R y el tiempo promedio de falla E(T).

**Teorema.** Si E(t) es finito entonces:

$$E(t) = \int R(t)dt$$

La demostración de este teorema se obtiene a través de una integral doble la cual puede resolver utilizando integración por partes, y tomando en cuenta que se puede sustituir el valor de $R(t)$ *por* $\int_t^\infty f(s)ds$.

En otras palabras, el teorema significa que la duración promedio de una componente esta en función de la sobrevivencia que tenga después de un instante t.

## 1.6 DISTRIBUCIONES DE CONFIABILIDAD MAS COMUNES.

El tiempo entre fallas es una cantidad aleatoria continua. Esta cantidad aleatoria, desde el punto de vista probabilistico, puede ser bien determinada si su función de distribución es conocida. En Confiabilidad es más conveniente caracterizar este tiempo entre fallas por la derivada de la función de distribución.

Las funciones usadas para describir la falla son:

1) Función de densidad de probabilidad f(t)
2) Función acumulada de probabilidad F(t)
3) Función de tasa de falla R(t)

las cuales están relacionadas por:

$$F(t) = \int_0^t f(x)dx \; ; \; F(t) = e^{-\int_0^t R(x)dx}$$

$F(0) = 0$ ; $F(+\infty) = 1$ y continua por la derecha

Las funciones de distribución más usadas para las leyes de falla son :

- ***Distribución NORMAL.***

$$f(t) = \frac{1}{\sigma\sqrt{2\Pi}} e^{-\frac{1}{2}(\frac{t-\mu}{\sigma})^2} \; ; \; -\infty\langle\mu\langle\infty, \; \sigma\langle 0$$

- ***Distribución EXPONENCIAL NEGATIVA.***

$$f(t) = \lambda e^{-\lambda t} \quad ; \quad \lambda\rangle 0, t \geq 0$$

- ***Distribución GAMMA.***

$$\frac{\lambda(\lambda t)^{\alpha-1} e^{-\lambda t}}{\Gamma(\alpha)} \quad ; \quad \lambda,\alpha\rangle 0 \quad t \geq 0$$

### 1.6.1 LEY NORMAL DE FALLAS.

Una de las leyes que se utilizan para representar la distribución del tiempo para fallar es la ley normal, la f.d.p. asociada con el tiempo T para fallar es:

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}$$

esta ley implica que:

1.- La mayor parte de los componentes fallarán alrededor de un tiempo promedio de falla E(T).

2.- El número de fallas disminuye simétricamente cuando $|T-\mu|$ aumenta.

3.- La función de confiabilidad de la ley normal de fallas puede expresarse mediante la función de distribución normal acumulada tabulada (representada por $\phi$) para valores tipificados.

La distribución normal se observa en el caso de fallas graduales de componentes eléctricos y mecánicos; es muy utilizada en el análisis de la confiabilidad de sistemas complejos cuando las desviaciones de los parámetros, de los componentes, salen de los límites permitidos; es decir es un modelo apropiado para componentes en los cuales la falla se debe a algunos defectos de uso.

Propiedades de la ley NORMAL de fallas.

1) $E(t) = \mu$

2) $Var(t) = \sigma^2$

3) $F(t) = P\{T < t\} = 1 - \frac{1}{\sigma\sqrt{2\pi}} \int_0^{} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} = \varphi\left(\frac{t-\mu}{\sigma}\right)$

4) $R(t) = 1 - \varphi\left(\frac{t-\mu}{\sigma}\right)$

### 1.6.2 LEY EXPONENCIAL DE FALLAS.

La ley exponencial de fallas es aquella ley cuyo tiempo para fallar se describe mediante una distribución exponencial; la manera más sencilla de describirla es utilizando una tasa de fallas constante, esto es:

$$Z(t) = \lambda$$

La f.d.p. asociada con el tiempo para fallar T está dada por:

$$f(t) = \lambda e^{-\lambda t} \; ; \; t > 0$$

El complementario es $R(t) = 1 - F(t) = e^{-\lambda t}$

$$\Rightarrow \; Z(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

La tasa constante de fallas se puede interpretar como una indicación de que después de que la componente (artículo) ha sido usada, su probabilidad de fallar no ha cambiado. Es decir, no hay efecto de su uso.

También se puede interpretar de la siguiente forma:

$$P\left\{\frac{t < T + \Delta t}{T < t}\right\}$$

- Considere para $\Delta t > 0$ que $P\left\{\frac{t < T + \Delta t}{T > t}\right\}$ es la probabilidad de que la componente falle durante las próximas $\Delta t$ horas dado que no ha fallado en el instante t.

Entonces:

$$P\left\{t < \frac{T < t + \Delta t}{T > t}\right\} = \frac{P(t < T < t + \Delta t)}{P(T > t)}$$

$$= \frac{e^{-\lambda t} - e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}}$$

$$= 1 - e^{-\lambda \Delta t}$$

por lo tanto ésta probabilidad sólo depende de $\Delta t$

Para muchos tipos de componentes la hipótesis que conduce a la ley exponencial de fallas está sostenida por la evidencia empírica.

***Propiedades de la ley EXPONENCIAL de fallas.***

1) $E(t) = \frac{1}{\lambda}$

2) $Var(T) = \frac{1}{\lambda^2}$

3) $F(T) = P\{T < t\} = 1 - e^{-\lambda t}$

4) $R(t) = e^{-\lambda t}$

### 1.6.3 LEY GAMMA DE FALLAS.

Para el caso de la ley gamma, la función para hallar el tiempo para fallar es:

$$f(t) = \frac{\lambda \cdot (\lambda t)^{\alpha-1} \cdot e^{-\lambda t}}{\Gamma(\alpha)} \qquad \lambda, \alpha > 0, t > 0$$

donde $\lambda$ es el parámetro de la distribución y $\alpha$ es el parámetro que caracteriza la asimetría y exceso de la distribución. Dependiendo de este valor la forma de las características cuantitativas fundamentales de confiabilidad cambian de manera sustancial.

Cuando la redundancia en un sistema está conectada de acuerdo al método de reemplazo y bajo la condición de que el flujo de las fallas del sistema principal y de todas las redundancias es sencillo, entonces la distribución gamma representa acertadamente la distribución del tiempo para fallar de un sistema.

Esta distribución puede ser una característica de tiempos para fallar de sistemas electromecánicos si los componentes fallan instantáneamente durante la etapa inicial de operación y durante el período de desgaste del sistema.

***Propiedades de la ley GAMMA de fallas.***

1) $E(T) = \frac{\alpha}{\lambda}$

2) $F(T) = P\left\{T < t = 1 - \sum_{i=0}^{\alpha-1} \frac{e^{-\lambda}(\lambda t)^i}{i!}\right\}$

3) $R(t) = e^{-\lambda} \sum_{i=0}^{\alpha-1} \frac{(\lambda t)^i}{i!}$

Hasta ahora hemos visto partes fundamentales en el estudio de nuestro trabajo, mas adelante veremos la combinación de las dos teorías y lo importante de combinar diferentes técnicas de estudio de redes y confiabilidad.

# CAPITULO II

## ANÁLISIS DE CONFIABILIDAD DEL HARDWARE

## 2.1 COMPONENTES DE UNA RED Y COMO SE OPERAN

### *2.1.1 LOS SERVIDORES Y LAS ESTACIONES DE TRABAJO*

El Servidor, es el corazón de la Red de Área Local. Esta microcomputadora es de alta velocidad, corre el sistema operativo y gestiona el flujo de datos a través de la red. Las Estaciones de Trabajo individuales y los dispositivos periféricos compartidos (por ejemplo: las impresoras), están conectadas al servidor.

Cada estación de trabajo de la red es por lo general una computadora personal que corre su propio sistema operativo (por ejemplo: el DOS o el OS/DOS).

A diferencia de una microcomputadora aislada, la estación de trabajo contiene una tarjeta de interfaz y está físicamente conectada por medio de cables con el servidor. Además una estación de trabajo corre un programa especial, llamado Shell de la red, que permite la comunicación con el servidor, con las otras estaciones de trabajo y con los otros dispositivos de la red. Este Shell permite a la estación de trabajo utilizar archivos programas en el servidor tan fácilmente como lo pudiera hacer en sus propios discos. El software que se ejecuta en las estaciones de trabajo tambien es conocido como software de cliente.

**CARACTERÍSTICAS DE UNA COMPUTADORA PERSONAL:**

Como ya habiamos mencionado anteriormente, existen grandes cambios en el mundo de las computadoras personales, los cambios han contemplado el aumento en capacidad de cómputo y han disminuido considerablemente el tamaño físico.

La capacidad de cómputo se ha incrementado tanto que los términos de microcomputadora o computadora personal ya no hacen justicia a su poderío y utilización.

Podemos remontar el origen de estos cambios a las primera computadoras de 16 bits lanzadas al mercado en 1986, y a las subsiguientes que cuentan con procesadores de 32 bits y en un futuro a las computadoras de 64 bits.

En un principio el software ejecutado en estas computadoras no era capaz de aprovecharlas en su totalidad, el software de hoy en día, hace un uso completo de la capacidad de este procesador de 16 bits y de 32 bits.

Una de las ventajas de estas computadoras, no aprovechada adecuadamente hasta el momento, es la capacidad de direccionamiento de memoria RAM y de almacenamiento de disco duro.

Los procesadores actuales son de 32 bits, pero los procesadores de 16 bits son el equipo más popular, al menos en el mercado mexicano.

Existe en el mercado un número limitado de software que realmente utiliza al máximo la capacidad de los 32 bits. Dentro de las capacidades de las computadoras personales de 16 bits y 32 bits, encontramos los siguientes parámetros comunes:

1) Alto grado de capacidad en el manejo de memoria RAM para competir contra algunos equipos de computadoras.
2) Velocidad suficiente como para ser usados como servidores de redes, combinando diversos equipos de cómputo
3) Direccionamiento de discos, suficientemente grande como para almacenar grandes áreas de información, tal como una minicomputadora

Gracias a estas capacidades las PC compatibles se están integrando a las minicomputadoras con alguno de los siguientes dos esquemas de trabajo:

- Estación de trabajo inteligente de una minicomputadora

- Redes de minis y microcomputadoras, en las cuales los servidores de red se usan para llevar a cabo las comunicaciones necesarias con la minicomputadora, como un front-end.

**COMPARTIENDO RECURSOS:**

Las computadoras personales pueden compartir los siguientes recursos con otros usuarios:

Monitor, teclado, unidades de disco, memoria RAM, el CPU, el coprocesador y cualquier otro dispositivo presente.

La minicomputadora comparte:

Disco duro, memoria RAM, el CPU, unidades de cinta, impresora de alta velocidad, graficadores y grandes bases de datos.

Para poder ejemplificar mejor la ganancia de capacidad de cómputo al trabajar estos dos equipos en conjunto, partiremos de la forma como trabaja una terminal tonta:

**TERMINAL TONTA**

Cuando el usuario escribe un carácter en la terminal, ésta lo envía al CPU interrumpiendo el proceso ejecutado en ese momento. El CPU le responderá a la terminal, haciendo eco del carácter para comparar lo que el usuario escribió, en caso de ser iguales, se desplegará en la pantalla y en caso de ser distintos, se marcará un error y se repetirá el ciclo de envío. El CPU forma un buffer de memoria para los caracteres recibidos de cada una de las terminales hasta el momento en que reconoce el carácter RETURN (ASCII 13), en este instante interpretará a todos los caracteres como un comando, revisando la sintaxis del mismo.

Es obvio que la terminal se queda bloqueada o en un estado de espera hasta que el CPU le conteste sobre el éxito ó fracaso del comando del usuario.

En este caso, el trabajo del CPU se multiplica por cada terminal. Tienen que hacer el 100% de todas las validaciones y cambios en la pantalla necesarios para que el proceso funcione.

Si la terminal es una computadora personal con un programa de emulación de terminal su capacidad se desperdiciará en su totalidad, quedaría prácticamente reducida a teclado y monitor, el CPU no tiene ningún papel en este caso, salvo el de ejecutar la emulación de la terminal tonta. En una terminal inteligente el proceso es distinto:

**TERMINAL INTELIGENTE**

En esta terminal el usuario escribe todos los caracteres deseados sin ser enviados uno a uno al CPU, el envío al CPU de toda la cadena de caracteres se realiza hasta el momento en que se oprime RETURN.

La revisión de sintaxis se hace también en la terminal misma, asegurando todo el tiempo que los comandos enviados, son comandos válidos, sin posibilidad de errores de escritura.

Esta operación facilita mucho y acelera de sobremanera la comunicación entre CPU y terminal inteligente, pues únicamente espera respuesta de éxito o fracaso de su petición.

La terminal inteligente, queda liberada en su trabajo, el usuario queda en posibilidad de seguir trabajando con la computadora, porque la terminal realiza todas las validaciones posibles sobre los usuarios.

El trabajo en conjunto de ambas terminales ofrece una gran ventaja por no existir subutilización de las computadoras personales como terminales tontas, cada una de las computadoras realiza la tarea adecuada para su tipo.

### *2.1.2 MEDIOS DE TRANSMISIÓN*

Los cables más comúnmente utilizados como medio de transmisión son:

- Cable de Par Trenzado sin Apantallar.
- Cable de Par Trenzado Apantallado.

- Cable Coaxial.
- Cable de Fibra Óptica.

Los tres primeros conducen la señal eléctrica a través de hilo de cobre. Los cables de fibra óptica transportan la luz a través de hilos de vidrio.

### *2.1.2.1 CABLE DE PAR TRENZADO SIN APANTALLAR*

Los cables de par trenzado son dos hilos trenzados en seis vueltas por pulgada para compensar las interferencias de los pares de hilos. Otro nombre muy utilizado es el de "IBM tipo 3". Ya que en las instalaciones hay gran cantidad de este hilo, a menudo surge la tentación de ahorrar gastos y tiempo utilizándolos.

Este tipo de cables es utilizado normalmente en los hilos del teléfono. Sin embargo, utilizar el hilo del teléfono cuando hay tanto, puede conducir a problemas más graves.

El cable de par trenzado sin apantallar es muy sensible a las interferencias electromagnéticas.

El cable de par trenzado sin apantallar es barato, fácil de instalar y puede trabajar en redes reducidas. Pero se puede tener problemas en una red si no se elige correctamente el tipo de cable que se requiere para la instalación específica.

### *2.1.2.2 CABLE DE PAR TRENZADO APANTALLADO*

Los cables de par trenzado apantallado son similares a los de par trenzado sin apantallar, excepto en que utilizan hilos más gruesos y están protegidos de las interferencias por una capa aislante protectora. Y es más costoso que un cable de par trenzado sin apantallar. Cabe mencionar que este tipo de cables en realidad tiene 8 hilos, de los cuales solo utilizan 2 para transmisión y recepción de los datos.

### *2.1.2.3 CABLE COAXIAL*

El cable coaxial consta de dos conductores rodeados por dos capas aislantes. La primera capa aislante encierra un hilo central de cobre conductor, que se encarga de transportar la corriente. Esta tiene un blindaje trenzado exterior que la cubre y que impide que la señal radie al espacio. Su ventaja es que pueden instalarse casi en cualquier parte. Como el blindaje externo está puesto a masa, puede colocarse el cable al lado de objetos metálicos sin ningún problema.

### *2.1.2.4 CABLE DE FIBRA ÓPTICA*

El cable de fibra óptica trasmite los datos como impulsos de luz a través de cables de vidrio. Actualmente los grandes sistemas de redes van soportados por cables de fibra óptica. Los cables de fibra óptica tienen importantes ventajas sobre todos los tipos de cables de cobre. Proporcionan la transmisión más rápida y más fiable porque al no ser sensibles a las interferencias electromagnéticas no pueden perder ningún paquete. El cable de fibra óptica es más delgado y flexible, lo que hace que sea más fácil trabajar con él que con el más pesado de cobre. Y quizás lo más importante, el cable de fibra óptica tiene capacidad de transmisión de datos más rápidos que las redes del mañana requerirán.

El precio del cable de fibra óptica está bajando, pero es más caro que cualquiera de cobre. La colocación del cable de fibra óptica es más difícil que la del cable de cobre, porque los extremos deben estar especialmente pulidos y alineados para obtener una rápida conexión.

### *2.1.2.5 Especificaciones para los diferentes tipos de cableado en una red.*

Siguiendo con la especificaciones de cableado de las redes del tipo 10BASE-T y en adición al estándar IEEE 802.3.

Atenuación:

La atenuación debe ser baja o ecualizada de 10 dB o 5 Mhz a 10 Mhz. La máxima atenuación de la ruta de un cable entre el transmisor y su correspondiente receptor es de 11.5 dB para todas las frecuencias entre los 5 Mhz y los 10 Mhz. Esto consiste de un máximo de 10 dB atenuación para el cable.

La máxima atenuación de un cable completo es la ruta entre el transmisor y el correspondiente receptor, que es 11.5 dB en todas las frecuencias entre 5 Mhz y 10 Mhz.

Características de Impedancia

La impedancia característica diferencial de las frecuencias entre 5 y 10 Mhz tiene que estar entre 85 y 110 ohms.

**2.1.2.6 Lista de cables probados.**

Durante el desarrollo de la investigación se probaron cables de par trenzado para observar si son apropiados para redes Ethernet del tipo 10BASE-T. Los cables no probados pueden no funcionar correctamente dentro de la red debido a que, este tipo de cables pueden ocasionar un pobre rendimiento dentro de la red. El probador de cables HP 26687A puede ser usado para verificar la instalación de cables de par trenzado.

Estados Unidos.

| FABRICANTE | Número de Producto | Descripción | Longitud del cable |
|---|---|---|---|
| AT&T | 403101140 | 4 pares, 24indicadores, alambres dentro | 100 m |

| | | | |
|---|---|---|---|
| AT&T | 106371487 | 4 pares, 24indicadores, blindado | 185 m |
| Anixter | CM-00424BAG-3 | 25 pares, 24indicadores | 100m |
| Anixter | CM-02524BAG-3 | 25 pares, 24indicadores | 100m |
| Anixter | CMP-0024G-3 | 4 pares, 24indicadores, muy veloz | 100m |
| Anixter | CMP-025234G-3 | 25 pares, 24indicadores, muy veloz | 100m |
| Belden | 9566 | 6 pares, 24indicadores | 100m |
| Belden | 1154A | 4 pares, especificaciones de conexiones IBM del tipo 3 | 100m |
| HP | 92179D | cable terminal | 70m |
| HP | 92268A | 4 pares, 24 indicadores, cable y terminación recta con 8 pines 4 metros | - |

| | | | |
|---|---|---|---|
| HP | 92268B | 4 pares, 24 indicadores, cable y terminación recta con 8 pines 8 metros | - |
| HP | 92268C | 4 pares, 24 indicadores, cable y terminación recta con 8 pines 16 metros | - |
| HP | 92268D | 4 pares, 24 indicadores, cable y terminación recta con 8 pines 32 metros | - |
| HP | 92268M | 4 pares, 24indicadores, 100 metros | - |
| HP | 92268N | 4 pares, 24indicadores, soldado en secciones de 300 metros | 100m |
| HP | 92268S | 3 pares, 24indicadores, cable adaptado de 6 a 8 pines, 5 metros | - |

| | | | |
|---|---|---|---|
| IBM* | 4716748 | tipo 1, 2 pares, 22 indicadores, blindado | 340 m |
| IBM* | 4716739 | tipo 2, 2 pares, 22 indicadores, blindado | 340m |
| IBM* | 4716739 | tipo 2, 4 pares, 24indicadores | 200m |
| IBM | depende del distribuidor. | tipo 3, 4 pares, 24indicadores | 100m |
| IBM* | 4716743 | tipo 6, 2 pares, 26indicadores, blindado | 225m |
| IBM* | 6339583 | tipo 9, 2 pares, 26 indicadores, blindado | 235m |
| Northern Telecom | - | cable IBDN, 3 o 4 pares, 24 indicadores | 100m |

Los cables enunciados en la tabla anterior tienen una característica de impedancia de 150 ohms. La impedancia discontinua (conectando un cable de 150 ohms a un cable de 100 ohms) causa una reflexión de señales que pueden hacer decrecer la velocidad a la que transmite la red o igual incapacitar la red. Para reducir los efectos de la impedancia discontinua, nunca use cables de 150 ohms en distancias menores a 75 metros.

***Esquemas para el cableado del tipo de par trenzado para redes HP EtherTwist.***

*Requerimientos de instalación del cable del tipo de par trenzado.*

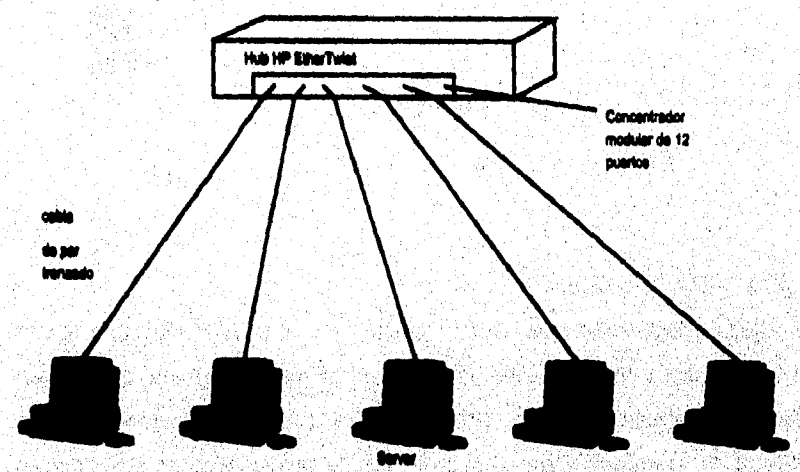
-Use cable apropiado , compatible con las especificaciones definidas en las redes del tipo 10BASE-T y en suma con los estándares IEEE 802.3

-El cable deberá ser de par trenzado.

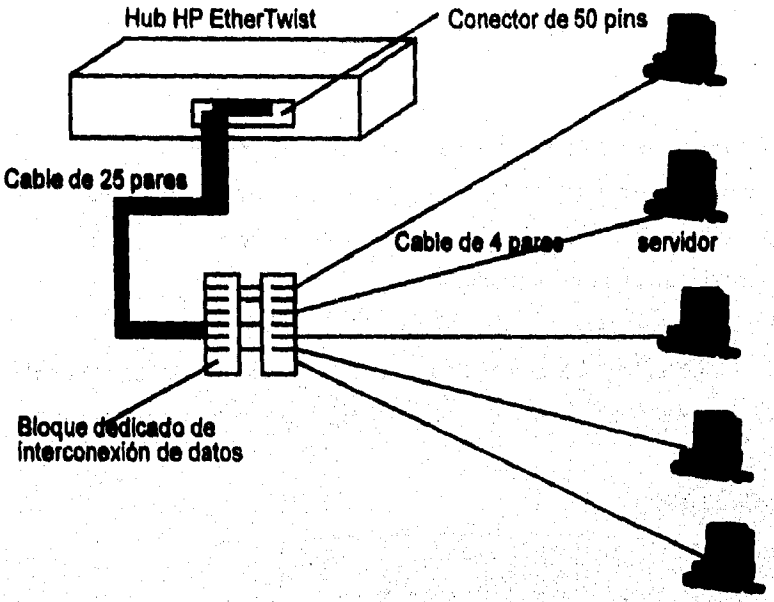
-El enchufe modular deberá ser de 8 pines.

-Si ya se cuenta con cable este podrá ser probado por el Probador de cables HP 28687A, este es un instrumento muy recomendable para usarse si se cuenta con una red.

Conexión de ejemplo:




Ejemplo 1




Ejemplo 2

### 2.1.3 TARJETAS DE RED.

Las tarjetas adaptadoras para red HP EtherTwist están diseñadas para operar con los productos estándares de hardware del mercado, basados en pruebas limitadas las tarjetas HP han sido probadas con un número cerrado de productos de hardware. Para cerciorarse que la tarjeta es compatible con el Sistema Operativo a utilizar hay que observar el manual de la misma.

| Tarjeta HP EtherTwist | Computadoras Personales |
|---|---|
| HP 27245A | Familia de HP Vectra PC |
| | IBM PC/XT/AT |
| | IBM PS/2 Modelo 25,30 |
| | Compaq Portátil |
| | Compaq de escritorio |

| | |
|---|---|
| | Epson PC |
| | Compuadd 325 (386/25) |
| | Olivetti M300 (386/16) |
| | Acer 1100/25 (386/25) |
| | AST 386/33 |
| | Toshiba T8500 Modelo 386/25 |
| | Hyundai 286C |
| HP 27248A | IBM PS/2 Modelos 50,60,70,80 |
| HP 27247A | Familia de la HP Vectra PC |
| | IBM PC AT |
| | Compaq Portátil |
| | Compaq de escritorio |
| | Epson |
| | 3Com 3S/40x |
| | Tandy 3000 y 4000 |
| | Honeywell 286,386 |
| | Zenith |
| | Wyse 3225 |
| HP 27248A | Familia de HP Vectra PC |
| | Compaq 386/33,386C,486C,Modelo 3000 |
| | Dell 425/E |

**Los siguientes productos son conocidos por su incompatibilidad con las tarjetas adaptadoras para red de HP EtherTwist:**

| Tarjeta HP EtherTwist | Computadoras Personales |
|---|---|
| HP 27247A | Epson 386/25,386/SX |
| | Hyundai 286C |
| | IBM PS/2 modelo 25,30 |

### 2.1.4 TRANSCEIVERS.

Los transceivers sirven para unir una o más computadoras personales u otros equipos a una red, en algunos casos sirven para convertir la señal luminosa de una fibra óptica a impulsos eléctricos que son con los que trabajan los cables de par trenzado. Se pueden usar como dispositivos standalone o incluidos con otros componentes de la red.

Todos los transceivers de Cabletron vienen con un interruptor de selección que le permite al usuario habilitar y desactivar el SQE (Prueba de Pulso). Este interruptor permite que los transceivers se conecten a un repetidor o a una computadora, según se requiera. Además, cada transceiver viene con indicadores de diagnóstico integrados, una serie de diodos emisores de luz que permiten detectar rápidamente los problemas de la red.

La familia de tranceivers provee una conexión para el puerto AUI (Atachment Unit Interface) Puerto de Unidad de Interconexión de Interface para cable coaxial, fibra óptica y par trenzado.

Los transceivers pueden conectarse directamente ó mediante un cable AUI de dispositivo de red ó cualquier sistema de tarjetas adaptadoras de red.

Los transceivers envían y reciben datos, detectan colisiones en una red y aumenta la confiabilidad de la misma mediante el monitoreo de malas funciones entre el puerto dispositivo de la red y el mismo transceiver. Soporta ambos protocolos el IEEE 802.3 y el Ethernet. Mediante leds proveen rápida visualización del status de la red.

#### 2.1.4.1 Características generales de los transceivers.

-Provee un conector AUI que conecta cualquier puerto periférico de AUI directamente o vía un cable AUI.
-Soporta dispositivos IEEE 802.3 y Ethernet (versión 1.0 y 2.0).
-Ocupa un pequeño espacio y es de fácil y rápida instalación para el usuario.

Opera transparentemente a cualquier sistema operativo de red.

### 2.1.4.2 Caracteristicas individuales de los Transceivers

*Transceiver EtherTwist.*

-Provee compatibilidad con redes del tipo 10BASE-T con protocolos IEEE 802.3 así como con redes HP StarLAN 10.

-Se conecta a cables de par trenzado de 8 pins modulares (RJ-45).

-Soporta los cables de par trenzado desprotegidos 22, 24 o 26 AWG, aunque el cable de par trenzado protegido pueds ser usado.

-Soporta 100 metros de cable de par trenzado para cualquier dispositivo AUI compatible. Son posibles distancias más largas usando cables de baja pérdida.

-Provee al usuario de switches con los cuales puede probar el acceso SQL.

-Contiene un LED que notifica al usuario que el transceiver esta en funcionamiento correcto.

- *Transceiver para cable de fibra óptica.*

-Provee compatibilidad con el IEEE 802.3 FOIRL estándar.

-Conecta a la fibra óptica por medio de dos conectores ST (TX y RX).

-Soporta ambos cables de fibra óptica 62.5/125-mm y 50/125-mm.

-Puede ser usada en configuraciones de red punto a punto usando fibra óptica con el puente HP 28673A 10:10 LAN y una configuración en estrella HP 28682A usando el Hub Plus de fibra óptica.

-Soporta un kilometro de fibra óptica en la configuración punto a punto.

-Provee de LEDs para una rápida visualización del funcionamiento del transceiver y además detecta colisiones, transmisión activa y un LED para saber el status del transceiver.

- *ThinLAN Transceiver.*

-Provee compatibilidad con las redes del tipo IEEE 802.3 del tipo 10BASE2.

-Se conecta a cable coaxial delgado por medio del puerto ThinLAN (BNC).

-Provee un switch de prueba usar-seleccionar SQE.
-Provee de un LED indicador de poder para una rápida notificación que el transceiver está funcionando.

### *2.1.4.3 ESPECIFICACIONES GENERALES..*

*Compatibilidad con hardware.*

El Transceiver HP 28685A EtherTwist, el Transceiver de fibra óptica HP 28683A y el Transceiver HP 28641B ThinLAN cada uno de ellos están diseñados para proveer una conexión AUI compatible para dispositivos LAN que son compatibles con el IEEE 802.3 o Ethernet versión 1.0 ó 2.0 estándar.

*Compatibilidad de Software.*

Los transceivers HP son transparentes para cualquier sistema operativo de red.

*Stándares.*

-IEEE 802.3 del tipo 10BASE-T
-IEEE 802.3 FOIRL
-IEEE 802.3 del tipo 10BASE2

*Emisiones.*

VCCI clase 1, FTZ 1046/84 (VDE nivel B), FCC parte 15 clase A, CISPR-22 nivel A CISPR-22 nivel B (HP 28683A solamente).

El tamaño de los transceivers es casi como el de una tarjeta de crédito, esto los hace sumamente manejables, los transceivers pueden conectarse directamente a la tarjeta de red, al puerto AUI o bien al puerto AUI del hub EtherTwist.

**TABLA DE ESPECIFICACIONES.**

| | 28685A | HP 28693A | HP 28641B |
|---|---|---|---|
| **Medio Ambiente** | | | |
| Temperatura de Operación | 0°C a +55°C<br>+32°Fa +131°F | | |
| Humedad Relativa | 5% a 95%<br>@ 40°C no se condensa | | |
| **Características Eléctricas** | | | |
| Requerimientos de Voltaje | 9.0-15.75 V | 10.5-15.75 V | 10.2-15.75 V |
| Consumo de Energía | 1.0 W típicos<br>2.6 W máximo | 1.8 W típicos<br>2.4 W máximos | 2.0 W típicos<br>2.6 W máximo |
| **Características Físicas** | | | |
| Conectores | -Estándar IEEE 802.3 AUI 15 pins<br>-Modular 8 pins | -Estándar IEEE 802.3 AUI 15 pins<br>-ST fibra óptica (Tx/Rx) | -Estándar IEEE 802.3 AUI 15 pins<br>-BNC |
| Switches *habilitado/inhabilitado* | -Prueba SQE<br>-Tiempo de Ligado | -Prueba SQE<br>-Prueba Loopback | -Prueba SQE |
| Dimensiones | 9.62 cm X 4.34cm X 2.41 cm<br>3.75 in X 1.71 in X0.95 in | | |
| Peso | 85 grms (3.0 oz) | 75 grms (2.6 oz) | 85 grms (3.0 oz) |

**ESPECIFICACIONES ÓPTICAS PARA LOS TRANSCEIVERS DE FIBRA ÓPTICA HP 28683A**

| | 62.5/125 μm fibra | 50/125 μm fibra |
|---|---|---|
| Receptor Óptico | -32 dBm típicos<br>-27 dBm mínimos | -30 dBm típicos<br>-27 dBm mínimos |
| Transmisor Óptico | -12 dBm típicos<br>-17 dBm mínimos | -12 dBm típicos<br>-17 dBm mínimos |
| Intensidad Óptica | 10 dB | 6 dB |
| Intensidad de onda | 820 nm | 820 nm |

### 2.1.5 CONCENTRADORES

Los concentradores para grupos de trabajo permiten crear pequeños grupos de trabajo independientes que se pueden interconectar fácilmente con otros grupos de trabajo para crear una red más grande.

Los concentradores, en general, presentan las siguientes características:

- El soporte de MIB de monitoreo remoto (RMON), significa que los concentradores se pueden configurar para aplicar umbrales de alarmas a los datos obtenidos por medio del DLM.
- Proporciona una eficiente conectividad de nivel físico para todos los dispositivos y subredes interconectadas, sin necesidad de utilizar un puente externo o un ruteador.
- Los concentradores se pueden administrar mediante un sistema de administración de redes que cumple con el SNMP.
- La variada línea de concentradores proporciona diversos niveles de conectividad para pequeños grupos de trabajo independientes.
- Reduce los costos y facilita la instalación utilizando tramos cortos de UTP.

- Contiene indicadores LEDS de diagnóstico para un monitoreo de redes a primera vista.
- Están diseñados para ser el centro de grandes infraestructuras de redes, responden a las demandas para una mayor confiabilidad.
- Tienen también una arquitectura abierta para soportar nuevas tecnologías de Redes de Área Local

### 2.1.7 Pruebas a equipo

Para realizar las pruebas de los equipos se contó con la valiosa colaboración del Centro de Cómputo de la ENEP Acatlán y de algunos de sus proveedores que intervinieron en la construcción de la red del plantel. Cabe mencionar que algunos de los equpos probados ya no existen hoy en el mercado pero sirven para definir tal vez no todos los problemas con que se enfrentan los instaladores de redes, pero si al menos darán la pauta para pruebas con nuevos equipos.

**Tipo de controladora de disco duro para Net Ware ELS I y ELS II.**

En este tipo de software no es posible seleccionar el tipo de controladora de disco duro al momento de hacer la generación de NetWare. El NetWare ELS únicamente soporta determinados controladores de disco duro.

El NetWare ELS I únicamente soporta los siguientes controladores de disco duro:

* Para servidor IBM AT compatible, controlador Western Digital MFM.
* Para servidor IBM PS/2 modelos 50 y 60, controlador de disco duro MFM.
* Para servidores PS/2 modelo 60 y 80, controladores ESDI.

Mientras que el NetWare ELS II soporta:

* Para servidor IBM AT compatible controlador Western Digital MFM, y en casos especiales, controladores de tipo RLL o ESDI, siempre y cuando en el BIOS del servidor estén dadas de alta las características del disco duro (cabezas, cilindros, SEC/TRAC, precompensación) que se quieran instalar.
* Para servidores de tipo PS/2 modelos 50, 50Z y 60 controladores de disco duro MFM para PS/2.
* Para servidores de tipo PS/2 modelos 60, 70 y 80 controladores ESDI para PS/2.

**Pruebas con tarjeta Ethernet NE/2-32.**

Requerimientos:
1 Servidor PS/2 modelo 80 386
1 Tarjeta EtherNet NE/ 2-32
1 Tarjeta EtherNet NE/ 2
1 NetWare 386
1 diequete de drivers
1 Estación de trabajo IBM AT compatible
1 Tarjeta NE1000

Pruebas Realizadas:

Se instaló una red Advanced NetWare 386 en servidor PS/2 modelo 80 386, con tarjeta de red, primero NE/ 2 y después NE/ 2-32.

Como estación de trabajo se utilizó una PC IBM AT compatible con tarjeta NE1000. Se corrió la prueba de *performance*.

Comentarios:

Fue necesario cargar el *driver* de la tarjeta NE/ 2-32 (NE232.LAN) en el *diskette* de System del NetWare 386, y así poderlo llamar en la instalación de la red.

En la siguiente tabla se muestran los resultados que se obtienen con el *performance*.

**Prueba de disco duro Priam.**

**Características:**
**Marca: Priam**
**Modelo: ID330-FC**
**Interfase Tipo: ESDI/RLL**
**Capacidad: 330 MB**
**Número de Cilindros: 1225**
**Número de Cabezas: 15**
**Velocidad de Acceso: 10 Mb/s**
**SEC/TRAC: 36**

**Pruebas Realizadas:**

**Se realizaron instalaciones de sistema operativo NetWare: SFT NetWare 286 V2.12, Advanced NetWare 286 V2.12 y V2.15 dedicado y no dedicado en el servidor PC-AT IBM compatible.**

**Comentarios:**

**Se dio de alta el disco duro en el Setup de la PC-AT con el archivo SETUP que viene con el software del disco duro. Se configuró como tipo 9, no fue necesario correr el COMPSURF.**

**En el proceso de generación de NetWare, es necesario generar un directorio llamado DSK_DRV_PRI y en él cargar los archivos *.OBJ, además en el directorio AUXGEN cargar los archivos *.DSK.**

Al momento de seleccionar el tipo de controladora de disco duro, se selecciona el tipo ESDI/RLL, y se sigue el proceso de instalación normal.

**Pruebas de disco duro Control Data.**

**Características:**

**Marca:** Control Data

**Modelo:** 94161-155

**Interfase:** Futuro Domain TMC-855

**Capacidad:** 150 MB

**Número dè Cilindros:** 969

**Número de Cabezas:** 9

**SEC/TRAC:** 34

**Instalación del disco:**

Para poder instalar el disco duro en la PC-AT es necesario declarar en el *setup* de la AT que no hay discos duros instalados. A continuación se instala el disco duro y la controladora y con el *diskette* etiquetado como "*Master Diskette*" corre la utilería llamada "DM" y selecciona la opción "*Initialize Scsi Drive tables*" que permite que la AT reconozca el disco duro y la controladora.

**Comentarios:**

Para la generación de NetWare es necesario generar un directorio llamado "DSK_DRV_.FUT" y en él cargar todos los archivos del *diskette* llamado "*Novell NetWare 286 Scsi Disk Drivers*".

También en el directorio de AUXGEN se deben cargar los archivos con extensión *.DSK

Se realiza la generación normal y en el momento de seleccionar el tipo de controladora de disco duro se escoge "*Future Domain (830/840/850)*" y se continua con la generación e instalación normal.

**Pruebas con el disco duro Maxtor.**

**Características:**

**Marca: Maxtor**

**Modelo: XT-4380E**

**Interfase: Adaptec 2322B**

**Capacidad: 335 MB**

**Número de Cilindros: 1222**

**Número de Cabezas: 15**

**SEC/TRAC: 38**

**Pruebas Realizadas:**

**Instalación de Red Advanced NetWare 286 V2.15 dedicado. El disco presenta algunos problemas al instalarse con el tipo de controlador que utiliza el sistema operativo Netware, pero se pretende que el fabricante proporcione proximamente un controlador que sea 100% compatible con Netware.**

**Comentarios:**

**Se instaló la red en un servidor AT 386 Acer de 20/16 Mhz. con ROM BIOS *Award Software* V3.03A con tarjeta ArcNet Novell.**

**Se dio de alta el disco duro en el setup del servidor con el Software Lanstor que viene junto con el disco. Se corre la instalación automática, tecleando "*Lanstor/instal*" y el disco duro queda automáticamente dado de alta en el *setup* del servidor. A continuación se indica si se desea bajar los *drivers* necesarios para la generación de NetWare a disquetes. Se responde que si y se piden los siguientes disquetes: DSK_DRV_001 y AUXGEN.**

**A continuación se realiza el proceso de generación normal y se selecciona como tipo de controladora la siguiente: *Storage Dimensions*.**

**Se recomienda no correr el COMPSURF, ya que el disco viene preparado. Se realiza la instalación normal de NetWare.**

Un punto importante con respecto a la controladora de disco duro Adaptec 2322B que se utilizó en esta prueba, es que fue necesario habilitar un estado de espera, poniendo *Jumper* en la posición "J2-3", debido a que presentaba problemas con el servidor 386.

**Sistema Operativo NetWare ELS I de Novell trabajando con Ethernet y/o Arcnet al utilizar como servidor una IBM PS/2.**

Comentarios:

Se realizaron pruebas para instalar tarjetas Ethernet microcanal con el sistema operativo ELS I. Las tarjetas que se utilizaron fueron:

**NE/2 de Novell**
**Tiara LanCard E/AT**

Estas tarjetas NO funcionaron con el sistema operativo, puesto que ya vienen configuradas con la opción de default (IRQ=3, I/OBase 300H) y no se pueden configurar con estas características.

Con tarjetas Arcnet microcanal se probaron:

**LanCard Tiara Arcnet**
**Novellco MNC**

Las anteriores y cualquier tarjeta compatible con el estándar MicroSystems funcionaron correctamente con los parámetros por default (IRQ=2, I/OBase=2EOH).

**Pruebas con tarjetas Proteon P1347.**

**Características:**

**Marca: PROTEON**

**Modelo: P1347**

**Velocidad: 4MB/s**

**Protocolo: Token Ring**

**Bus: 16 bits**

**Buffer: 16 Kbytes**

**Tipo de Cable:** ***Shielder Twisted Pair,*** **conector DB-9**

***shielded Twisted Pair,*** **conector RJ-45, RJ-11**

***Socket Prom:*** **disponible (2)**

**Pruebas Realizadas:**

**Se instaló la tarjeta en una PC-AT compatible y una red Advanced NetWare 286 V2.15**

**Comentarios:**

**Se probó la tarjeta con diferentes configuraciones, como servidor y como estación de trabajo.**

**Cuando exista un problema entre la tarjeta P1347 con la configuración de default (IRQ=12, I/O=A20, DMA=5, BOOT ROM=D800) y en la PC donde se esté instalando este modelo de tarjeta se recomienda cambiar a las siguientes opciones:**

**IRQ= 4, I/O=1A20, DMA=5, BOOT ROM=DOOO**
**IRQ= 3, I/O=2A20, DMA=6, BOOT ROM=C800**

**Estas opciones también son válidas cuando se utilice *prom* de autoencendido. Este modelo de tarjeta utiliza dos *promps* de autoencendido, el**

primero, marcado como "MSB", se instala en el *socket* U24; el marcado como "LSB", en U30.

Es necesario configurar los siguientes jumpers:

| | |
|---|---|
| JP12 | 2-3 |
| JP18 | 2-3 |
| JP19 | 1-2, 3-4 |

Cuando se ha configurado el archivo de prom de autoencendido "Net$DOS.SYS" se debe renombrar a "PRO4$AT.SYS", para que las estaciones con este modelo de tarjeta puedan leerlo.

**Pruebas con tarjetas Proteon P1840 y servidor PS/2 modelo 80.**

**Características:**
**Servidor: PS/2 Mod. 80**
**Memoria RAM: 4 Mb.**
**Disco Duro: Maxtor 330 Mb.**
**Controladora: ESD I**
**Tarjeta: Proteon P1840**
**Diskette de Drivers**

**Pruebas Realizadas:**

Se instaló una red Advanced NetWare 286 V2.15 en un servidor PS/2 modelo 80 y con tarjeta Proteon modelo P1840.

**Comentarios:**

La instalación de la red se realizó con drivers Proteon V2.3 y presentó problemas en la PS/2 modelo 80 como servidor.

Al momento de tratar de accesar a la red desde cualquier estación de trabajo, manda el siguiente mensaje "*Packet File Corrupted*", o también en ocasiones, la estación de trabajo queda bloqueada cargando el *login*.

Estos mismos drivers se probaron en PS/2 modelo 50Z como servidor sin presentar ningún problema. Para la PS/2 modelo 80 fue necesario cambiar los *drivers* de Proteon versión 3.0 sin presentar problema alguno.

**Pruebas con NetWare 5250 Twinax Gateway (local).**

Comentarios:

Se probó un *prerelease* de *gateway* local vía cable Twinax, para conectarse a un sistema de IBM ya sea S/36/34/38, que consiste de *software* y *hardware*.

***Software.***

Los programas permiten a cualquier estación de trabajo de una red local (NetWare), emular una gran variedad de dispositivos compatibles con los sistemas minis de IBM. El juego de programas se corren de la siguiente forma:

***Gateway Server:*** Se recomienda que la máquina que realizará las funciones de *gateway* sea una 386 para mejor respuesta en tiempo. Se ha probado en IBM XT 4.7 MHz (conectado a un S/38), y en Olivetti M24 de 8 MHz (conectado a un AS/400).

Esta máquina puede funcionar como no-dedicada, es decir puede emular y ser el gateway, aunque esto no es recomendable.

***LAN WorkStation:*** Se corre en las estaciones de trabajo que requieran entrar en emulación con el *Host*.

***Hardware.***

Consta de una tarjeta instalada en la máquina que funciona como gateway. Esta tarjeta puede ser:

*Novell Twinax Adapter* (Bus tipo AT)

*Micro Integration Stwinax Adapter* (Microcanal)

Se puede emular y soportar lo siguiente:

* Terminales modelos 5251, 5291, 3180 y 3196.

* Impresoras modelo 3810, 5219, 5224, 5256.

* Acceso a la mayoría de las aplicaciones de los sistemas S/3X o AS/400.

*Soportar APIs V2.1

* Transferencia de archivos.

* Permite hasta siete sesiones concurrentes y cinco sesiones por estación de trabajo.

La conexión al Host se puede hacer de dos maneras:

1. Directamente con un cable Twinax (véase la figura 1). [4]

2. Indirectamente por medio de los controladores 5251 Mod.12, 5294 ó 5293 (véase la figura 2).

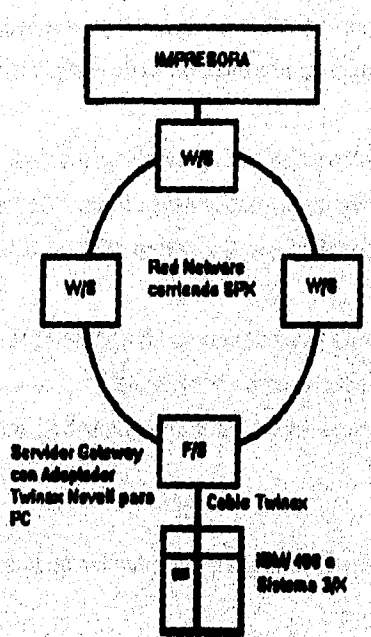


Figura 1.1 Gateway Twinax enlazado al host a través del cable Twinax.

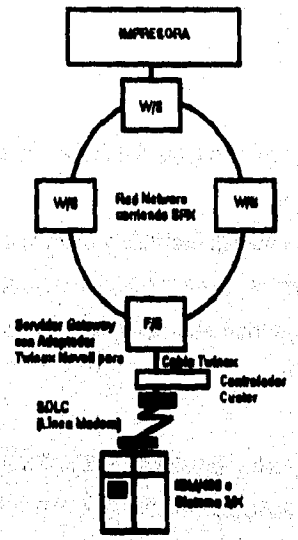



Figura 1.2 Gateway Twinax enlazado al host a través de un controlador.

**Pruebas con tarjeta Proteon P1342.**

**Características:**

**Marca: PROTEON**

**Modelo: P1342**

**Velocidad: 4 Mbps.**

**Protocolo: Token Ring**

**Bus: 8 Bits**

**Buffer: 1792 Bytes**

**Tipo de cable: Shielded Twisted Pair Connector Tipo D-9 pin.**

**Unshielded Twisted Pair Connector RJ-45 ó RJ-11**

**Socket Prom: Disponible.**

**Pruebas:**

Se instaló la tarjeta en una PC-XT compatible y PC-AT compatible y se probó como estación de trabajo.

**Comentarios:**

Este modelo de tarjeta sólo puede funcionar en estaciones de trabajo y nunca en servidores de archivo.

Se probó con diferentes configuraciones y cuando exista un problema entre la tarjeta con la configuración de default (IRQ=3 I/O=A20 DATA BLOCK=A000 BOTT PROM=D800) y la PC donde se está instalando la tarjeta, se recomienda probar las siguientes opciones:

IRQ=3, I/O=1A20, DATA BLOCK=A000, BOOT PROM=D000
IRQ=4, I/O=2A20, DATA BLOCK=A800, BOOT PROM=C800

Estas opciones son válidas también para cuando se utiliza prom de autoencendido. Es necesario renombrar el archivo NET$DOS.SYS que se genera para el prom de autoencendido en el servidor como "PRO4$PC.SYS" para que las estaciones de trabajo con este modelo de tarjeta puedan funcionar.

**Conexión de Token Ring Proteon con HP RS/25C.**

**Características:**
**Servidor de Archivos Modelo: HP RS/25C**
**Velocidad: 25 MHz**
**Disco duro: HP 300 Mb**
**Memoria base: 640 Kb**
**Memoria extendida: 3.5 Mb**
**NetWare: Advanced NetWare 2.15 Rev C Dedicado.**
**MS-DOS: Ver 3.3**

Tarjeta de Red: PROTEON
Modelo: P1347
Velocidad: 4 Mbps
Topología: Token Ring
Drivers: Ver. 3.0

Descripción:

Cuando se enviaba a guardar en el servidor con SYSCON en la opción de Supervisor Options o de WordStar se almacenaba basura en los archivos accesados.

Solución:

Fue necesario deshabilitar el Jumper marcado como SA (SAEN) en la tarjeta Token Ring del servidor de archivos.

Comentarios:

Se recomienda deshabilitar este Jumper en la tarjeta Token Ring del servidor de archivos en PC-AT que no sea completamente compatible con IBM y que puede presentar los siguientes problemas:

Errores de DMA
Respuestas incorrectas
Fallas de la instalación.

**Enlace de estaciones Acer y Unisys utilizando tarjetas Tiara Arcnet con prom de autoencendido Novell.**

Características:
Marca: ACER
Modelo: AcerStation

Bios: Award 3.01B
Video: Monocromático
Velocidad: 12 MHz
Memoria: 512 Kb
Marca: UNISYS
Modelo: PW 825
Bios: Phoenix 8386 V1.10
Video: VGA/EGA
Velocidad: 20 MHz
Memoria: 640/1024 Kb

Tarjetas ARCNET
Marca: Tiara
Modelo: Tiara Lancard/A
Driver: RX-NET Novell
Boot Prom: ARCNET V2.1
MS-DOS: V3.30
Configuración de default: (IRQ=2, I/O=260, Mem Buffer=D000)

Pruebas:

Se probaron las estaciones de trabajo en dos redes Advanced NetWare 286 V2.15 REV A y SFT 286 V2.15 EV C. Se generó el *Shell* para ambas redes y se generó el archivo NET$O.SYS en cada servidor.

Cuando se trató de enlazar con prom de autoencendido, las estaciones mandaron el mensaje de error *"File Server Could Not be Found"*, aleatoriamente.

Comentarios:

Reducir la velocidad a menos de 12 MHz. Substituir el circuito integrado PCF1508/011 marca Phillips que se localiza en posición U6, por el circuito

integrado LINCO11. Substituir el prom de autoencendido de Novell por el prom de autoencendido marca Tiara.

Las estaciones de trabajo sin prom de autoencendido funcionan bien sin hacer cambio alguno.

**Especificaciones de cable y restricciones de longitud para línea de productos Synoptics.**

Cable blindado de par trenzado (*Shielded Twisted Pair*, STP).

El cable STP se ha diseñado para trabajar en sistemas de cableado IBM de 150 Ohms de impedancia. La utilización de cables STP que no satisfaga las especificaciones eléctricas de un cableado IBM puede producir un pobre comportamiento de la red LattisNet. Existen cinco tipos de cables STP que pueden utilizarse con LattisNet. En la siguiente tabla se muestran las especificaciones eléctricas del cable STP.

| Par de Hilos | Tipo 1 | Tipo 2 | Tipo 6 | Tipo 8 | Tipo 9 |
|---|---|---|---|---|---|
| cobre calibre | 22AWG | 22AWG | 22AWG | 22AWG | 22AWG |
| Imped. 3-30 Mhz | 150 Ohm | 150 Ohm | 150 Ohm | 150 Ohm | 150 Ohm |
| Aten. @ 10 Mhz | 36 db/Km | 36 db/Km | 53 db/Km | 70 db/Km | 53 db/Km |
| Resis. CD | 87 ohm/Km | 87 ohm/Km | 87 ohm/Km | 87ohm/Km | 87ohm/Km |
| Diafon. 3-5 Mhz | -58 db | -58 db | - 58 db | - 58 db | - 58 db |

**Restricciones de longitud para STP**

| | | |
|---|---|---|
| Tipo 1 y 2 | 100 mts. máx. | Concentrador- Concentrador/PC |
| Tipo 6 y 9 | 68 mts. máx . | Concentrador- Concentrador/PC |
| Tipo 8 | 50 mts. máx. | Concentrador- Concentrador/PC |

Cable sin blindar de par trenzado (*Unshielded Twisted Pair*, UTP).

El cable UTP se ha diseñado para operar en instalaciones con cableado DIW (D-inside wire). Este tipo de cable se fabrica en diferentes tamaños: 2, 3, 6, 12,16, 25, 50, 75 y 100 pares de cables. En la siguiente tabla se muestran las especificaciones eléctricas para cable UTP.

| | | |
|---|---|---|
| Calibre | . 24 AWG | |
| Imped. | @10 Mhz | 85-100 Ohms |
| Aten. | @ 10 Mhz | 3 db/ 33 m. |

Restricciones de longitud para UTP

100 mts. máximo en concentradores de concentrador/PC. El cable telefónico plano, al que se conoce como *silver stain* puede utilizarse como cable de extensión *patch cable* con una longitud máxima de 9 m. Este tipo de cable tiene características de di afonía muy altas (10MHz), lo cual crea falsas colisiones en el medio de transmisión. Por lo tanto no debe utilizarse para la configuración total de una red.

*Fibra Óptica.*

LattisNet puede operar con los tipos A, B y C de fibra óptica multimodo. El tipo de cable 5 de las normas de IBM es equivalente al tipo B. En la tabla se muestran las especificaciones eléctricas de la fibra óptica para LattisNet.

*Restricciones de longitud para fibra óptica*

Longitud máxima de 2000 mts. entre concentradores. Dos tipos de concentradores ópticos pueden ser utilizados: FMSA ó ST. El conector FMSA fue el primero en implantarse y por lo tanto está ampliamente distribuido en redes

locales. Tiene una pérdida por acoplamiento de 2 db y puede utilizarse con fibra tipo B ó tipo 5 de IBM.

El conector ST se ha diseñado especialmente para aplicaciones de red con una pérdida por acoplamiento máxima de 1 db y se utiliza con fibras de tipo A ó C.

Tipo ATipo BTipo C

| | | | |
|---|---|---|---|
| Diámetro exterior | 125 um. | 140 um. | 125 um. |
| Diámetro interior | 62.5 um. | 100 um. | 125 um. |
| Apertura | 0.29 | 0.29 | 0.29 |
| Pérdidas de acoplamiento | 1 db | 2 db | 1 db |

**NetWare Access Server (NAS).**

Comentarios:

Los siguientes puntos son recomendaciones que se dan para un mejor funcionamiento del NAS. El NAS se ha diseñado para trabajar en forma dedicada en máquinas con procesador 80386 exclusivamente, con BUS tipo AT. Debe contener drives de "5.25" de alta capacidad con opción de disco duro, tener por lo menos 4 MB en RAM (con 2 MB funciona para una estación remota). La cantidad de memoria depende de las estaciones remotas que se quieran conectar. Al utilizar la siguiente fórmula es posible calcular la cantidad de memoria RAM necesaria de acuerdo con el número de estaciones remotas que se deseen conectar.

$$1000 + (N * 750) = RAM$$

En donde N es la cantidad de estaciones remotas a conectar.

La memoria extra (mayor de 640) debe configurarse como memoria "extendida" no como expandida (EMS ó EEMS).

Un solo NAS puede soportar hasta 15 usuarios remotos simultáneamente. Para esto es necesario instalar por lo menos una tarjeta de comunicaciones (WNIM+) y una tarjeta de red (ArcNet, EtherNet, etc.). En la máquina en donde se va a correr el NAS se pueden instalar hasta 4 WNIM+. Existen máquinas que por cuestiones de direccionamiento sólo soportan 3 WNIM+. Esto se puede checar con un paquete de software que viene en un diskette de verificación.

El NAS no soporta los puertos seriales propios de las máquinas en donde se instala para conectar estaciones remotas. Para esto son indispensables las tarjetas WNIM+.

Las tarjetas de video que puede tener la máquina en donde se corre el NAS son: MDA, CGA, FGA, VGA, HGA, HTC. Novell recomienda utilizar CGA para su mejor funcionamiento. El NAS es soportado por las versiones de NetWare V2.1 ó mayores. Funciona con MS-DOS V3.X, soporta velocidades hasta de 19.2 Kbits/s y usa modems del tipo Hayes SmartModem y compatibles con la norma V.32.2.

También soporta multiplexores de la marca: AT&T, RACAL-VADIC.

Las estaciones remotas pueden ser máquinas del tipo: IBM PC, XT, AT, PS/2 ó compatibles, las cuales deben tener un puerto serial RS232C y, por lo menos, 256 KB de acuerdo con el paquete de aplicación que se utilice. Apple Macintosh Plus, Macintosh SE ó Macintosh II con 512 KB de RAM.

Terminales ASCII tales como DEC-VT-100, IBM 3101 ó cualquier máquina que pueda emular terminales tipo ASCII.

Los usuarios remotos pueden enviar trabajos de impresión a impresoras que se hayan conectado al servidor de archivos o a una impresora local, pero no soporta impresoras que se conecten directamente al NAS. También, pueden tener acceso a un Mainframe IBM (SNA) Gateway mediante el NetWare 3270 LAN WorkStation V1.1 ó mayor, lo que les permite emular 8 sesiones concurrentes y sólo terminales 3270 modelo 2. Además soporta el software de File Tranafer Send-Receive.

**Irregularidades en comportamiento de IBM PS/2 de diversos modelos utilizados como servidores de red bajo topología Arcnet.**

**Características:**
**File Server: IBM**
**Modelo: 80 y otros**
**Lan: Arcnet Novellco PS/2**
**NetWare: Adv. NetWare 2.15 Rev C**
**Estación de trabajo: IBM**
**Modelo: 50Z**
**Lan: Arcnet Novellco**

**Pruebas Realizadas:**

Se instaló el sistema operativo de red en el servidor PS/2 bajo Arcnet y se detectaron comportamientos extraños aleatorios; en ocasiones se cala el servidor o en algunas otras ocasiones se desplegaba basura en la estación de trabajo. Por otro lado, algunos usuarios reportaron otros síntomas como pérdida de comunicación de la estación de trabajo o comportamiento anormal del servidor.

**Comentarios:**

Se detectó incompatibilidad aleatoria con algunos modelos de IBM PS/2 utilizados como servidores. Las fallas quedaron solucionadas definitivamente con el cambio del circuito RAM (6116) en las tarjetas Arcnet PS/2 Novellco.

**Pruebas con concentrador Synoptica 2530.**

**Características:**
**Marca: Synoptics**
**Modelo: 2530 AUI/UTP**

Velocidad: 10 MB/s

Puertos: 8 RJ-45

1 AUI (Conector DB15)

Distancia: 100 metros RG/45

50 metros AUI

Requerimientos:

1 PC-AT compatible

1 Tarjeta EtherNet Twisted Pair

1 Diskette de drivers

1 PC-XT compatible

1 Tarjeta EtherNet Twisted Pair

1 Diskette de drivers

1 PS/2 50Z

1 Tarjeta EtherNet MC

1 Diskette de drivers

1 Concentrador

1 *Transceiver*

300 metros de cable RG/58

50 metros de cable grueso

2 Terminadores de 50 Ohms

Pruebas Realizadas:

Se montó una red con Advanced NetWare 286 V2.15 con las siguientes características:

Servidor de Archivos AT IBM Compatible

Tarjeta Twisted Pair EtherNet

Drivers Tiara

Estación de Trabajo PC-XT Compatible

Tarjeta Twisted Pair EtherNet

Drivers NE1000

Estación de Trabajo PS/2 50-7
**Tarjeta EtherNet Tiara MC**
**Drivers Tiara**

Se realizaron pruebas de comunicación con el concentrador, estaciones de trabajo, servidor de archivos y las máximas distancias permitidas con los cables grueso y RG/58 sin problema alguno.
Para cable grueso 50 m
Para cable RG/58 300 m

Comentarios:

Se recomienda deshabilitar la señal de SQE de los *transceivers* que estén conectados al concentrador, debido a que el *transceiver* genera una prueba de detección de colisión al final de cada paquete de datos transmitidos si la señal SQE está habilitada. El concentrador modelo 2530 AUI/UTP realiza las siguientes funciones:

* Amplifica y re sincroniza las señales recibidas y las transmite a los dispositivos conectados a él (computadoras, *transceivers*, concentradores).
* Realiza las funciones de un repetidor multipuerto de acuerdo con la norma *IEEE 802.3*. Detecta colisiones en la red e informa a los dispositivos conectados con él sobre la presencia de éstas.
* Tiene la función de *Jabber* que aísla al concentrador de la red cuando un paquete de datos recibidos sobre algún puerto excede en su longitud a la norma 802.3 (1518 Bytes).

La función de partición se implantó en el puerto AUI para desconectarlo ante un número excesivo de colisiones consecutivas, o si la colisión que se presenta es de gran tamaño. Contiene una serie de *leds* que indican el estado del concentrador:

*Power*. Led verde alimentación.

*Faul Status.* Led rojo cuando se activa la función de Jabber.
*Data.* Led verde cuando la información está presente dentro del concentrador.
*<Data>.* Led verde se enciende 350 ms después de que el dato está presente en el concentrador.
*Col.* Led ámbar cuando se detecta una colisión en el concentrador.
*Segment Fault.* Led rojo indica que el puerto AUI se ha separado automáticamente de la red debido a excesivas colisiones o a que el tamaño de la colisión fue grande.

**Pruebas con concentrador Synoptica 1010.**

**Características:**
**Marca: Synoptics**
**Modelo: Concentrador 1010**
**Módulos: 1 Módulo 405 UTP**
**Puertos por Módulo: 8 puertos RG**

**Requerimientos:**
**PC-AT IBM Compatible**
**1 Tarjeta EtherNet Twisted Pair**
**1 diskette de drivers**
**1 PC-XT IBM compatible**
**1 Tarjeta EtherNet Twisted Pair**
**1 Diskette de drivers**
**1 Transceiver**
**1 Concentrador 2350 Synoptics**
**1 Concentrador 1010 Synoptics**
**50 m de cable grueso**

**Pruebas Realizadas:**

A continuación se armó una red con las características mencionadas para probar la comunicación del servidor de archivos, estación de trabajo y los concentradores.

* Servidor de Archivos.
PC-AT IBM compatible
Tarjeta EtherNet Twisted Pair Tiara
Drivers Tiara

* Estación de trabajo.
PC-XT IBM compatible
Tarjeta EtherNet Twisted Pair Accton
Drivers NE-1000
NetWare Advanced NetWare 286 V2.15

Comentarios:

Durante las pruebas realizadas de comunicación se encontró que cuando se está utilizando el cable grueso de 50 m, la estación de trabajo no entra en la red, y utilizando un cable de menor tamaño (12 m), la estación entra sin problemas.

A continuación se mencionan las características más importantes del concentrador modelo 1010:

El concentrador contiene tres ranuras libres en las cuales se les puede instalar módulos LattisNet Host, que son de cuatro tipos, que permite la conexión de dispositivos (concentradores, computadoras, transceivers) con tres tipos de cables como son *Unshielded Twisted Pair* (UTP), *Shielded Twisted Pair* (STP) y *fibra óptica*.

El concentrador 1010 además contiene, en su parte superior izquierda, un módulo que se puede configurar de las siguientes formas de acuerdo con el tipo de módulo que se le instale:

* **Concentrador STAND ALONE.-** Viene configurado con un módulo de diagnóstico modelo 1201-D, que nos informa de la actividad de la red con *Leds* indicadores.

*Data Led.* Led verde indica que el dato está dentro del concentrador.

*<Data> Led.* Se enciende temporalmente cuando el dato entra al concentrador.

*Collision Led.* Led ámbar se enciende cuando se detecta una colisión en el concentrador.

Además en sus tres ranuras libres se le pueden instalar hasta 3 módulos LattisNet Host.

*** Concentrador LOCAL.- Este concentrador debe de configurarse con el módulo de la serie 1200 de canal de interconexión simple, que permite conectarse a cualquier otro concentrador local o central. Además en sus tres ranuras libres se le pueden instalar hasta tres módulos LattisNet Host.**

*** Concentrador CENTRAL.- Está configurado con un módulo de la serie 1200 de canal de interconexión simple en su parte superior izquierda, y deberá configurarse con el módulo 204 Retiming instalado en una de las ranuras libres. Además se pueden instalar hasta dos módulos de interconexión de la serie 201 en sus ranuras restantes.**

**Pruebas con disco duro removible y disco duro fijo en un servidor de archivos PC-AT compatible.**

**Características:**
**Servidor de Archivos: AT IBM Compatible**
**Vel: 8 MHz**
**Tarjeta: NE1000**
**Disco duro (fijo): Rodime**

**Modelo: RO203E**

**Capacidad: 30 Mb**

**Tarjeta Controladora: AT Western Digital**

**Disco duro (removible): Tandon**

**Modelo: AD-PAC**

**Capacidad: 40 Mb**

**Tarjeta Controladora: Tandon**

**Modelo: PCA RLL Controller**

**Receptáculo: Tandon AD-PAC**

**Diskette de drivers: Tandon**

**Diskette de utilerías: Tandon**

**Pruebas:**

**Se instaló una red Advanced NetWare 286 V2.15 Rev C dedicado, en el servidor de archivos PC-AT compatible.**

**1.- Se verificó el funcionamiento del disco Tandon con su propia controladora como disco fijo.**

**2.- Se verificó el funcionamiento con un disco duro Tandon removible y un disco duro Rodime como fijo de la controladora de Tandon.**

**3.- Se verificó el funcionamiento del disco Tandon como removible con su propia controladora y el disco Rodime como fijo con la controladora Western Digital a la vez.**

**Comentarios:**

**La tarjeta controladora Tandon se configuró con la siguiente opción:**

**IRQ = 12**

**Dirección = C8000**

Este modelo de tarjeta soporta hasta dos discos duros fijos RLL y hasta dos discos duros removibles Tandon AD-PAC. No soporta *floppies*. Fue necesario utilizar la tarjeta Western Digital como controladora de *floppies*.

Una vez instalada la controladora con el disco duro Tandon que se da de alta en la PC-AT con el archivo llamado "RLLSETUP" que está en el diskette de utilerías de Tandon, debe mandar el siguiente mensaje: Tandon Overlay Rom, Rom Installation Complete.

Para la generación de NetWare es necesario cargar el archivo "Tandon.OBJ" al directorio de DSK_DRV_001, estos archivos están en el diskette de drivers de Tandon.

Se selecciona como controladora de disco duro una *"Tandon RLL Driver"*.

* Para la primera prueba, el sistema operativo se configuró así:
- Controladora Tandon RLL Driver
- Canal 0
- Configuración 7: Todas las unidades fijas
IRQ=12, I/O=38XH, NO DMA
- Disco duro Tandon configurado como:
"booteable"
Directorio Cache SI

* Para la segunda prueba, de la siguiente forma:
- Controladora Tandon RLL Driver
- Canal 0
- Configuración 3: Data-PAC removible (NETW2.15)
IRQ=12, I/O=38XH, NO DMA
- Disco duro Rodime configurado como:
Fijo "booteable"
Directorio Cache SI
- Disco duro Tandon configurado como:

Removible no "booteable"
Directorio Cache NO

* Para la tercer prueba:
- Controladora Western Digital
- Industry Standard ISA ó AT Comp
- Canal 0
- Configuración 0: ISA-DISK Primary Verify=ON
IRQ=14, I/O=1F0
- Disco duro Rodime configurado como:
Fijo "booteable"
Directorio Cache SI
- Controladora Tandon
- Tandon RLL Driver
- Canal 1
- Configuración 3: Data-PAC removible (NetW2.15)
IRQ=12, I/O=38XH, NO DMA
- Disco duro Tandon configurado como:
Removible no "booteable"
Dirección Cache NO

La instalación de NetWare se realiza con el procedimiento acostumbrado. Se recomienda el disco duro Tandon AD-PAC al momento de realizar la instalación.

Al momento de "bootear" la PC-AT (servidor), el siguiente mensaje aparece en la pantalla:

F3 "Bootear" de la partición activa

F7 "Bootear" de floppy

Se teclea F3 para levantar la red.

En la prueba 1, la red levanta de disco duro Tandon.

En las 2 y 3, la red levanta de disco duro Rodime y para montar el volumen removible (Tandon) se inserta el disco duro Tandon Data-PAc de 40 Mb en el receptáculo Tandon AD-PAC, y se teclea en la consola del servidor lo siguiente: *Mount 0.*

Para desmontar el volumen removible en la consola del servidor se teclea lo siguiente: *Dismount 0.*

**Pruebas de funcionamiento de disco duro Maxtor XT-8760E con sistema operativo NetWare instalado.**

**Características:**
**Marca: Maxtor**
**Modelo: XT-8760E**
**Capacidad: 600 Mb**
**Cabezas: 15**
**Cilindros: 1224**
**SEC/Track: 34**
**Interfase: ESDI**
**Marca: Adaptec**
**Modelo: 2322 REV C**
**Drivers: Lanstor V1.4.2 (ADV NET y SFT)**
**Drivers: Lanstor /386 ESDI V1.0 (NetWare 386 V3.0)**

**Pruebas:**

**Se instaló el disco duro Maxtor y la controladora Adaptec en un servidor modelo IBM AT compatible, se cargó Advanced NetWare V2.15 dedicado, NetWare SFT V2.15.**

Se instaló el disco duro Maxtor y la controladora Adaptec en un servidor modelo ACER386, se cargó Advanced NetWare 286 V2.15, NetWare 386 V3.0 con partición "booteable" de DOS V3.3 y sin partición.

Comentarios:

El disco duro ya viene preparado para la instalación de NetWare. Se recomienda no correr CompSurf.

En setup de AT IBM compatible y Acer386, el disco duro Maxtor XT-8760E se declara como tipo 1 (615 cilindros, 4 cabezas, 17 SEC/TRA).

Para la generación del sistema operativo NetWare Advanced y SFT es necesario cargar los drivers del diskette etiquetado como "Lanstor V1.4.2" a los siguientes diaquetes:

_Lanstor.OBJ DSK_DRV_001

_Lanstor.DSK Auxgen

En la generación del sistema operativo NetWare se selecciona como tipo de controladora: *Storage Dimensions Lanstor.*

Se continúa con el proceso acostumbrado de generación e instalación. Para la instalación de NetWare 386 el driver de la controladora se encuentra en el diskette etiquetado como "Lanstor/386 ESDI V1.0" y solamente funciona con NetWare 386 V3.0

**Pruebas de funcionamiento de tarjeta Proteon modelo P1390.**

Características:

Marca: PROTEON

Modelo: P1390

Vel: 4 Mb/s, 16 Mb/s

Buffer: 128 Kb

Compatible: IBM PC/XT, PC AT, PS/2 (2530-286) Microcanal

Instalable: Servidor de Archivos, puente de estación de trabajo.

Drivers: NetWare 386

NetWare 286 V2.15

NetWare 286 V2.0a

Cable tipo: UTP/STP

Conector tipo: RJ-45 para UTP

DB-9 para STP

Pruebas:

Se instaló una red Advanced NetWare 286 V2.15 en el servidor de archivos IBM AT compatible, una estación de trabajo Acer Station. Se probó el funcionamiento de tarjetas Proteon P1390 en el servidor de archivos y en la estación de trabajo, con cable tipo UTP y STP se corrió la prueba Performance.

Comentarios:

Para la generación del sistema operativo NetWare es necesario cargar los drivers de la tarjeta P1390:

| | |
|---|---|
| ANW-139X.OBJ | |
| BNW-139X.OBJ | |
| CNW-139X.OBJ | LAN_DRV_201 |
| DNW-139X.OBJ | |
| SHL-139X.OBJ | |
| NW-139X.LAN | Auxgen |
| SHL-139.LAN | SHGEN-1 |
| Promac.Out | System |

Al momento de seleccionar el tipo de controlador de red se selecciona: ProNet-4/16 P139X.

Para el servidor de archivos y el puente se pueden seleccionar hasta 14 configuraciones posibles (UTP/STP), (4 Mbps, 16 Mbps). Para la estación de trabajo existen 18 configuraciones posibles (UTP/STP), (4 Mbps, 16 Mbps). La tarjeta se configura como UTP ó STP, 4 Mb ó 16 Mb por software al momento de seleccionar el tipo de configuración.

Si la tarjeta se instala en una ranura de 16 bits se deberá seleccionar una configuración que use DMA (5, 6, 7). Si se instala en una ranura de 8 bits se deberá seleccionar una configuración que use pseudo DMA (PSDMA) que es una forma de controlar al DMA por medio del software. El pseudo DMA no es tan rápido como el DMA que proporciona el hardware.

Cuando la PC en donde se instale la tarjeta P1390 no es ISA compatible puede presentar algunos problemas:

Errores de DMA.

Errores de inicialización de tarjeta.

Existen las siguientes alternativas para poder solucionarlos:

Deshabilitar el Jumper Seen (Adress Enable).

Cambiar el DMA Clock del de *default* (8 MHz).

### 2.1.8 Distribuciones de confiabilidad para los componentes de hardware

Una vez realizadas las pruebas anteriores se llega a las siguientes conjeturas.

La confiabilidad de un componente electrónico se define como la probabilidad de que funcione de forma continua y satisfactoria durante un intervalo de tiempo estipulado T. Si los componentes que tienen algún defecto de fabricación de antemano son eliminados por la inspección que se hace en la fábrica de las piezas terminadas, y si las fallas producidas por el uso se evitan mediante la revisión y el mantenimiento por parte del usuario, en caso de las redes por el administrador de la red, las demás causas de falla en el funcionamiento se pueden considerar como fenómenos aleatorios. Bajo estas condiciones, las fallas por unidad de tiempo que se producen en un número grande de componentes semejantes expuestos a condiciones comparables están distribuidos típicamente según la **distribución Poisson**. En consecuencia el tiempo que transcurre entre las fallas tendrá una **distribución exponencial**.

La ley exponencial de fallas indica que cuando un componente ha sido utilizado durante un tiempo específico, al ocuparlo nuevamente no existe ningún efecto de uso por la utilización anterior; esto sucede de manera específica en los componentes electrónicos.

Considerando que los componentes del hardware de una red están básicamente constituidos por componentes electrónicos, se puede utilizar la distribución exponencial de fallas.

Una vez expuesto lo anterior, se procederá a definir la función de confiabilidad de algunos elementos que están involucrados en la estructura de las redes.

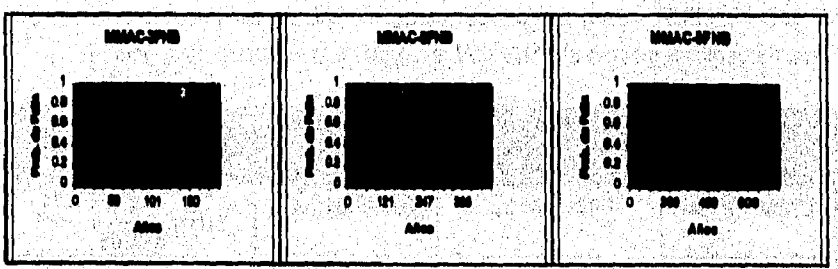
De acuerdo a datos que se obtuvieron de estos componentes, expresados en Tiempo Promedio de Recurrencia, y de acuerdo a la igualdad $E(t)=\frac{1}{\lambda}$, se

puede obtener el valor de lambda despejándolo de la igualdad anterior. Por lo tanto, tenemos que $\lambda = \frac{1}{E(t)}$.

**CONCENTRADORES**

Concentrador MMAC - 3FNB. Concentrador de tres ranuras y bus de red flexible.
Concentrador MMAC - 5FNB. Concentrador de cinco ranuras y bus de red flexible.
Concentrador MMAC - 8FNB. Concentrador de cableado que contiene ocho ranuras, con bus de red flexible.

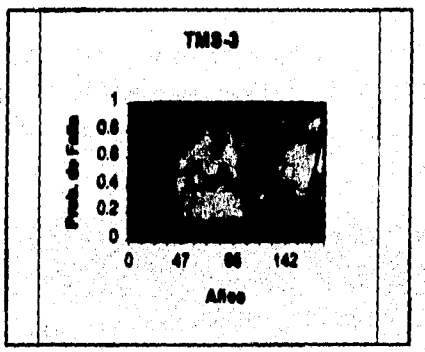
| | | | |
|---|---|---|---|
| MMAC-3FNB | 1'851,984 Hrs. | 0.0000005399 | $f(t) = \frac{1}{1851984} e^{-\frac{t}{1851984}}$ |
| MMAC-5FNB | 4'267,368 Hrs. | 0.0000002343 | $f(t) = \frac{1}{4267368} e^{-\frac{t}{4267368}}$ |
| MMAC-8FNB | 7'028,252 Hrs. | 0.0000001422 | $f(t) = \frac{1}{7028252} e^{-\frac{t}{7028252}}$ |




**TRANSCEIVERS**

El transceiver TMS-3 es una liviana unidad de bajo costo diseñada especificamente para complementar las aplicaciones de cableado Ethernet delgado. Este tiene dos diodos indicadores de luz (LED) que indican el estado de alimentación y de la prueba de pulso (SQE).

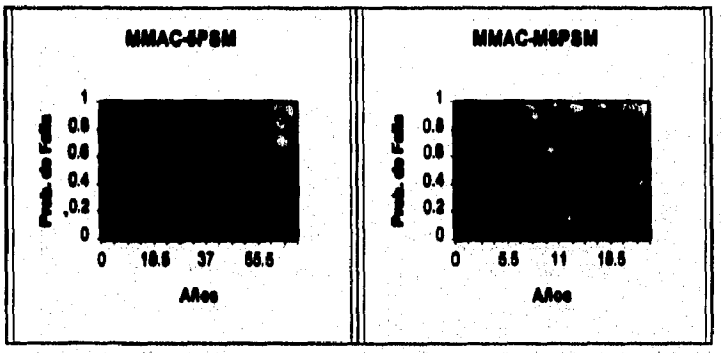
| | | | |
|---|---|---|---|
| TMS-3 | 1'664,440 Hrs. | 0.0000060082 | $f(t)=\frac{1}{1664440}e^{-\frac{t}{1664440}}$ |




**FUENTES DE ALIMENTACIÓN REDUNDANTES**

MMAC - 5PSM. Fuente de alimentación para concentradores de la serie MMAC-5.
MMAC - M8PSM. Este módulo se puede reemplazar sin desactivar el equipo permite verificar, gracias al LANVIEW, *a simple vista* el estado de la unidad.

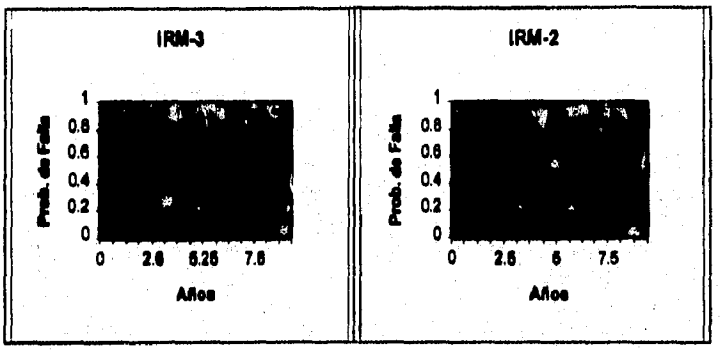
| | | | |
|---|---|---|---|
| MMAC-5PSM | 648,165 Hrs. | 0.0000015428 | $f(t)=\frac{1}{648165}e^{-\frac{t}{648165}}$ |
| MMAC-M8PSM | 200,000 Hrs. | 0.000005 | $f(t)=\frac{1}{200000}e^{-\frac{t}{200000}}$ |




## MÓDULOS DE ADMINISTRACIÓN PARA ETHERNET

**Módulo Repetidor Inteligente IRM - 3. Separa automáticamente los puertos con problemas y los vuelve a conectar cuando éstos se solucionan.**
**Módulo Repetidor Inteligente IRM - 2. Este módulo además de las funciones del IRM-3, incluye capacidades de administración más sofisticadas, tales como desglosar errores de puerto, bloqueo de puertos y análisis completo del rendimiento en forma gráfica.**

| | | | |
|---|---|---|---|
| IRM - 3 | 92,425 Hrs. | 0.000010819 | $f(t)=\frac{1}{92425}e^{-\frac{t}{92425}}$ |
| IRM - 2 | 87,603 Hrs. | 0.000011415 | $f(t)=\frac{1}{87603}e^{-\frac{t}{87603}}$ |



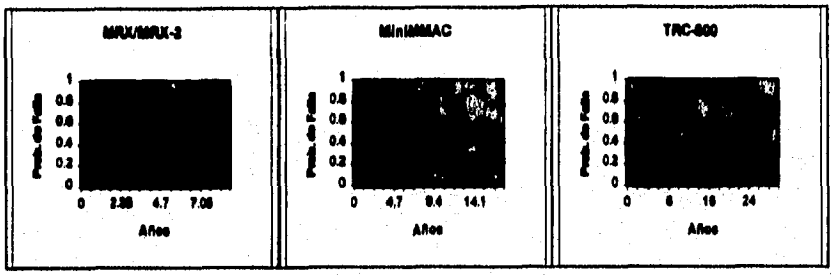

**CONCENTRADORES DE GRUPOS DE TRABAJO.**

MRX / MRX - 2. Concentradores que cumplen con el estándar 10BASE-T e IEEE 802.3 cuyo diseño repetidor asegura una transmisión de datos confiable al regular y a generar, repentinamente, los paquetes de datos. Están equipados con LED's LANVIEW que proporcionan un diagnóstico de nivel físico para la rápida detección de errores en la red.

MiniMMAC. Diseñado para necesidades de redes más pequeñas.

Concentrador Pasivo TRC - 800. Altamente confiable y de bajo costo.

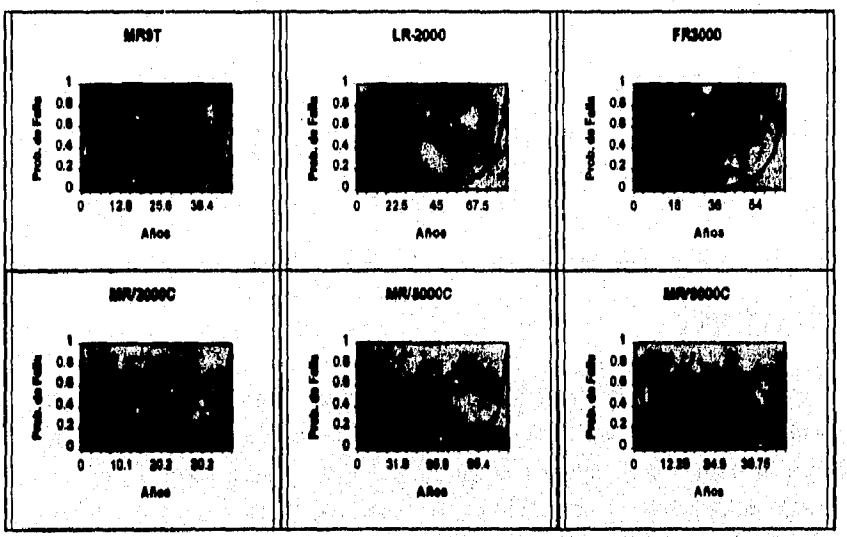
| | | | |
|---|---|---|---|
| MRX / MRX-2 | 83,133 Hrs. | 0.000012028 | $f(t)=\frac{1}{83133}e^{-\frac{t}{83133}}$ |
| MiniMMAC | 165,251 Hrs. | 0.0000060514 | $f(t)=\frac{1}{165251}e^{-\frac{t}{165251}}$ |
| TRC - 800 | 286,368 Hrs. | 0.000003492 | $f(t)=\frac{1}{286368}e^{-\frac{t}{286368}}$ |




**REPETIDORES**

Repetidor Multipuertos Serie MR9T. Dentro de las funciones que desempeña están la separación automática y reconexión y extensión de fragmentos. Gracias a estas funciones se asegura una transmisión de datos confiable y protege la integridad de la red en general al separar cualquier enlace con complicaciones.
Repetidor Ethernet LR - 2000.
Repetidor de fibra óptica FR3000.
Repetidores multipuerto MR/2000C MR/5000C y MR/9000C. Extienden fragmentos de colisión, separan los segmentos con problemas y vuelven a conectar los segmentos sin problemas.

| | | | |
|---|---|---|---|
| MR9T | 453,103 Hrs. | 0.0000022070 | $f(t)=\frac{1}{453103}e^{-\frac{t}{453103}}$ |
| LR-2000 | 788,172 Hrs. | 0.0000012687 | $f(t)=\frac{1}{788172}e^{-\frac{t}{788172}}$ |
| FR3000 | 653,016 Hrs. | 0.0000015313 | $f(t)=\frac{1}{653016}e^{-\frac{t}{653016}}$ |
| MR/2000C | 353,967 Hrs. | 0.0000028251 | $f(t)=\frac{1}{353967}e^{-\frac{t}{353967}}$ |
| MR/5000C | 1'112,294 Hrs. | 0.0000008990 | $f(t)=\frac{1}{1112294}e^{-\frac{t}{1112294}}$ |
| MR/9000C | 426,636 Hrs. | 0.0000023439 | $f(t)=\frac{1}{426636}e^{-\frac{t}{426636}}$ |




**PUENTES**

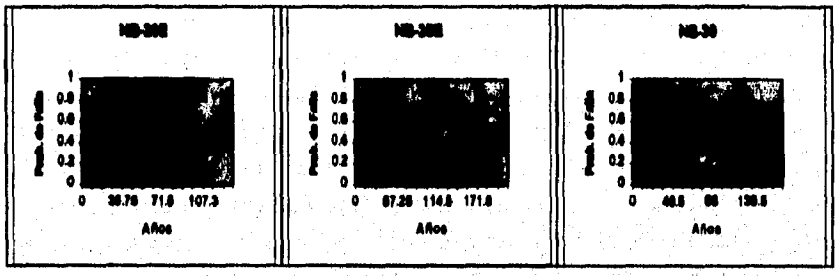
**Puente local Ethernet-a-Ethernet NB - 20E. Puente de bajo costo de desempeño medio. Incluye un sistema de software de filtración que determina los paquetes que pueden pasar por él.**

**Puente local Ethernet-a-Ethernet administrado NB - 25E. Incluye un sistema de hardware de filtración que determina los paquetes que pueden pasar por él sin recargar la CPU anfitriona.**

**Puente Remoto NB - 30. Puente remoto independiente del protocolo, el cual conecta dos redes de área local Ethernet.**

| | | | |
|---|---|---|---|
| NB-20E | 1'250,781 Hrs. | 0.0000007995 | $f(t) = \frac{1}{1250781} e^{-\frac{t}{1250781}}$ |
| NB-25E | 2'008,032 Hrs. | 0.0000004980 | $f(t) = \frac{1}{2008032} e^{-\frac{t}{2008032}}$ |

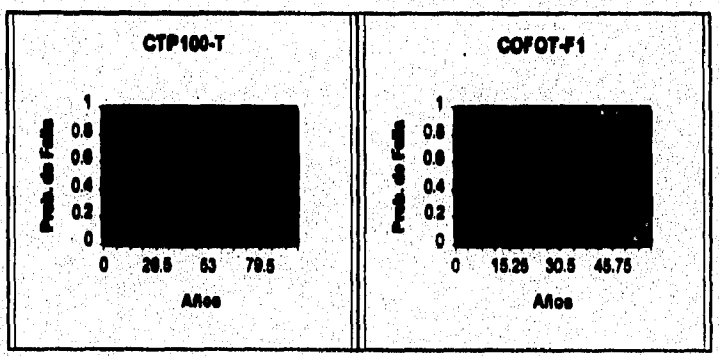
| | | | |
|---|---|---|---|
| NB-30 | 1'627,869 Hrs. | 0.0000006143 | $f(t)=\frac{1}{1627869}e^{-\frac{t}{1627869}}$ |




**ADAPTADORES**

**CTP100 - T. Adaptador de cable de par trenzado-a-cable coaxial. Contiene la correción y detección automática de polaridad que detecta si se ha invertido la polaridad del par de entrada.**
**COFOT - F1. Adaptador de cable coaxial-a-fibra óptica.**

| | | | |
|---|---|---|---|
| CTP100-T | 931,098 Hrs. | 0.0000010740 | $f(t)=\frac{1}{931098}e^{-\frac{t}{931098}}$ |
| COFOT-F1 | 539,956 Hrs. | 0.0000018520 | $f(t)=\frac{1}{539956}e^{-\frac{t}{539956}}$ |



Como se puede observar en las tablas, el tiempo mínimo requerido para que un componente falle es de 9.49 años, correspondiente al concentrador MRX/MRX-2. Este dato puede darnos una clara idea de que la confiabilidad, en cada uno de los componentes de hardware que colaboran dentro de la red de área local, es bastante alta; el único inconveniente de estos niveles de confiabilidad radica en que el equipo utilizado no estará a la vanguardia dentro de 10 años ó menos, pero lo que si podemos asegurar es que si las necesidades de los usuarios de una red no se incrementan (que lo vemos poco probable) las redes actuales seguirán funcionando. La única restricción es que los avances del software van ligados al hardware y viceversa, y cada día se aprecia que esta industria seguirá avanzando a pasos agigantados y sin que nadie quiera quedarse rezagado por lo cual al adquirir nuevo software tendrán por ende que invertir en hardware.

# CAPITULO III

## ANÁLISIS DE CONFIABILIDAD DEL SOFTWARE.

## 3.1 Confiabilidad del Software.

El amplio uso de computadoras y microprocesadores en los productos actuales, en los procesos y en los sistemas administrativos ha provocado un énfasis creciente sobre la medición cuantitativa de la confiabilidad de la lógica programada - o software -, que es tan importante en muchas aplicaciones como la confiabilidad del mismo hardware.

La confiabilidad del software se puede definir como:

"La probabilidad de que un sistema o componente software opere sin falla durante un periodo especificado de tiempo en un ambiente específico".

**En este contexto, una "falla del software" puede considerarse como una separación inaceptable de la operación del programa de los requisitos.**

En la confiabilidad del software la fuente de fallas es primordialmente el diseño, mientras que las fuentes de fallas en el hardware pueden ser también físicas, de manufactura, servicio u otras degradaciones.

Para poder desarrollar una función de densidad que pueda representar de forma significativa el nivel de confiabilidad del software -utilizado en una LAN-, es necesario aplicar conceptos de métrica de programación así como ingeniería de software. Estas materias pueden ayudar a obtener parámetros de acuerdo a la lógica de programación, lenguaje utilizado, procesadores utilizados, etc., es decir, todos aquellos elementos que intervienen para que un programa de computadora funcione en una máquina específica.

Consideramos que un gran porcentaje de los problemas que se pueden presentar en el software provienen desde el análisis del sistema, ya que en esta parte es donde se deben involucrar todos aquellos elementos necesarios para el funcionamiento del software final. Este porcentaje es seguido por los errores en la

programación, considerando que es muy frecuente el paso de parámetros entre funciones internas del software.

La minoría de los problemas que se presentan con el software se enfocan al grado de utilización de un paquete, ya que se pueden tener licencias para una cantidad específica de usuarios dentro de la red.

Otro aspecto que se debe tomar en cuenta al momento de probar el software, es que se debe evaluar en procesos de cálculo forzados, ya que de esta forma es posible localizar errores (bugs) dentro del sistema.

Un ejemplo claro de fallas en el software es el de la calculadora de Windows, utilizando la calculadora de forma "normal" no existe ningún problema; pero se ha descubierto que existe un error de programación ya que al cambiar al código binario presenta fallas al transformar y sumar números. Este es un error poco perceptible pero fácil de comprobar.

De tal forma podemos afirmar que para cada software realizado este presenta posibles fallas en las etapas de su desarrollo que se enuncian a continuación:

- Análisis.
- Desarrollo.
- Implantación.
- Uso frecuente.

Pero sería materialmente imposible definir la confiabilidad del software en general ya que cada uno es diferente y presenta diferentes problemas dentro del uso frecuente para el que fue creado cada uno.

Considerando los elementos significativos del concepto de confiabilidad y aplicándola al concepto de sistema de software, podemos enunciar las siguientes definiciones. Dentro de este capítulo se ofrecen las bases para que el lector pueda tener parámetros para definir los factores que influyen en el trabajo del software en una red y analice que es lo que eventualmente podría llegar a fallar en su trabajo diario.

Confiabilidad inherente. Identifica la confiabilidad potencial que es capaz de crear un diseñador en su proyecto. Este puede ser el más alto valor que un diseño puede proporcionar. Cuando se pasa del proyecto a su transformación en un "artículo" se lograr un valor de confiabilidad inherente. A este valor se le denomina : confiabilidad lograda.

Confiabilidad lograda. Es el valor de la confiabilidad demostrada por el producto (sistema). Por lo tanto, se incluyen los efectos de manufactura o desarrollo sobre esta confiabilidad.

Si se desean obtener mejoras en la confiabilidad de un producto o sistema real se debe medir y analizar dicho sistema, a fin de determinar los efectos que dan lugar a que la confiabilidad lograda sea menor a la inherente. Esto obliga a un estudio sobre las fallas de mecanismo del producto (Sistema en cuestión).

## 3.2 PROTOCOLOS DE COMUNICACIÓN

Los protocolos de comunicación son una serie de reglas que permiten que dos ó más sistemas se comuniquen.

La palabra *protocolo* pasó a formar parte de la terminología de computación alrededor de los años 70's, cuando el Departamento de Proyectos Avanzados de la Defensa de los Estados Unidos decidió construir una red de computadoras heterogéneas distribuidas geográficamente.

Hasta ese entonces, la comunicación entre los programas o procesos de computadoras estaba limitada a los procesos que estaban localizados dentro de la misma máquina. La comunicación interprocesos era realizada a través del uso de memoria compartida y señales especiales intercambiadas por mediación del sistema operativo. Esta técnica representaba la analogía de una charla "cara-a-cara" entre los procesos. La comunicación entre procesos entre sistemas distantes geográficamente, habría dejado a los procesos con diversas limitaciones puesto que tendrían que interactuar a través de un medio ambiente hostil con un ancho de banda limitado, retrasos y transmisiones poco fiables. Además, los

procesos existentes en los diversos sistemas de cómputo no "hablan" la misma lengua nativa, habiendo sido creados por diferentes fabricantes.

"Los protocolos son herramientas comunes diseñadas para controlar la transferencia de información entre sistemas de computadoras"[1]. Están elaborados de secuencias de mensajes con formatos y significados específicos. Estos mensajes equivalen a las instrucciones de un lenguaje de programación.

### 3.2.1 Elementos de un protocolo.

Los protocolos serían incompletos o impropios si no manejaran correctamente un número de funciones básicas:

a) ***Nomenclatura de un protocolo.*** Los protocolos involucran comunicación y por tanto, transferencia de información. Cuando una sección de información debe transferirse de un dominio a otro, hay que especificar algunas indicaciones no ambiguas del destino. En la mayoría de las circunstancias, el emisor no ejecuta la trasferencia física de la información por sí mismo. Generalmente, el emisor invoca a algún mecanismo común inferior además de un conjunto de parámetros, incluyendo nombres o direcciones.

b) ***Control de errores.*** Cuando la información es transladada una cierta distancia, debe de utilizarse un medio de transmisión como cables, fibras ópticas, microondas o satélites. Ocasionalmente, el ruido, la sintonización impropia, el daño físico, o la interferencia humana, corrompen o interrumpen las señales usadas para conducir los mensajes. Por ello se requiere de mecanismos que detecten y tal vez puedan recuperar los errores en la transmisión. El mismo conceptos se aplica cuando se efectúa una transmisión en sistemas más complejos, como las redes de paquetes, que intentan llevar a cabo su propio control interno de errores. La calidad de la transmisión puede ser considerablemente mejorada mediante un sistema que controle los errores, pero a veces se encuentran errores residuales que pueden señalarse como problemas

[1] Redes de Telecomunicaciones, Mischa Schwartz
Addison-Wesley Iberoamericana

de interferencia, cambios de instalación, operación, administración, fallas de hardware y software, etc.

La información intercambiada entre dos entidades aparece como cadenas de bits, enviadas y recibidas en bloques de un byte de longitud. La integridad de los bits puede asumirse con una probabilidad de $10^{10}$ a $10^{11}$ bits, lo cual es considerado como satisfactorio. Esto resulta de las propiedades de los códigos de detección de errores que acompañan a la información. En la actualidad, estos formatos podrían hacerse tan específicos como se requiriese, utilizando cualquiera de las técnicas de detección y corrección de errores. Sin embargo, pueden existir aún pérdidas o duplicación de bloques, que no son observados por los códigos de detección de error.

Para asegurar la integridad de los bloques, éstos se etiquetan con identificadores únicos. Tan pronto como el receptor registra los identificadores recibidos correctamente, puede descartar duplicados. Los bloques recibidos son reconocidos restituyendo sus identificadores. Después de un *retraso* previamente establecido denominado tiempo fuera (time out), el emisor retransmite los bloques no reconocidos. Este sencillo esquema, llamado Solicitud de Respuesta Automático (ARQ), es uno de los más utilizados en los protocolos de comunicación.

c) ***Control de flujo***. La cantidad de información transmitida por una fuente en particular puede exceder la capacidad del receptor o la capacidad de un sistema intermedio de transmisión. Una solución cruda podría ser descartar tráfico cuando éste no puede ser absorbido. Esta forma de control de flujo puede utilizarse como último recurso para prevenir detenciones, pero no se considera como una herramienta eficiente.

Un objetivo del control de flujo es mantener el flujo dentro de los límites compatibles con la cantidad de recursos disponibles. En la práctica, el control de flujo es un conjunto de políticas que tratan de optimizar la utilización de los

recursos del sistema, a la vez que cuidan que las tasas de información se mantengan cercanas a sus valores nominales.

Cuando dos entidades intercambian información, deben ser aptas para regular el flujo de la otra. Para ello, se utilizan dos mecanismos básicos: detención y avance (stop and go) y créditos (credit).

± Detención y Avance.

El receptor acepta o rechaza todo el tráfico excepto algunos mensajes cortos de señalización. El receptor tiene que tomar en cuenta el retraso de tránsito necesario para transportar señales de "alto" y "avance" al emisor. Cuando este retraso es grande, comparado con el retraso de transmisión de un bloque, una cierta cantidad de tráfico puede seguir fluyendo durante un momento. Además, cuando el receptor puede resumir tráfico, el retraso de tránsito de una señal de "avance" se convierte en un tiempo ocioso. En resumen, esta técnica es de simple implementación, y trabaja satisfactoriamente en enlaces terrestres.

± Créditos.

Se asume que al emisor no se le permite transmitir a menos que haya recibido una indicación del receptor con la cantidad de tráfico que éste puede aceptar. Esto se conoce como créditos. El uso de créditos asegura completamente al receptor de que puede asignar los recursos suficientes para el tráfico acreditado. Sin embargo, el receptor puede decidir dar más créditos que sus recursos disponibles, en el caso en que los retrasos de tránsito o los tiempos de respuesta del emisor son lo suficientemente grandes para otorgar recursos adicionales entretanto.

Un esquema de control de flujo puede fallar si los mensajes de señalización no están protegidos contra pérdida y duplicación. Diversas técnicas son utilizadas para proteger los mensajes de señalización:

1) Pueden reconocerse mensajes de señalización individuales.

2) La información de señalización puede ser encerrada (piggybacked) en el campo de control de los bloques enviados en dirección inversa, cuando el tráfico es bidireccional.

3) Puede utilizarse señalización redundante: las pérdidas son recuperadas automáticamente por un mensaje subsecuente y los duplicados no son perjudiciales.

d) ***Sincronización***. Las entidades involucradas en comunicaciones deben recordar un cierto número de parámetros, o variables de estado, esto es, asociaciones, números de mensaje, créditos, retrasos, etc. En conjunto, esta información es llamada contexto del protocolo. La información del contexto es creada por generación del sistema o como resultado de comandos explícitos de situación del contexto, o sobre una base incremetal durante el intercambio de tráfico. Debido a los retrasos de transmisión y el tiempo de respuesta de la maquinaria en cada extremo de una comunicación, los contextos se desarrollan asincrónicamente. No obstante, ocasionalmente es necesario asegurarse de que ambos lados de un contexto de protocolo se encuentren simultáneamente en un estado bien definido, esto es, en la inicialización, el recolocar el punto de chequeo, etc. Esto se denomina sincronización. La sincronización intenta garantizar la consistencia del contexto, o también reportar un error.

### 3.2.2 PROTOCOLOS PARA REDES LOCALES.

Como en cualquier sistema de comunicación, el conjunto completo de las funciones necesarias para la comunicación en redes locales está estructurado en una jerarquía de capas con sus respectivos protocolos. En las redes locales, esta jerarquía está simplificada debido a la naturaleza difusora de la transmisión. En términos del modelo ISO/OSI, los niveles de enlace (link) y de red (network) están fusionados ya que no se necesitan las funciones adicionales de ruteo ejecutadas en la capa de la red.

Sin embargo, el compartir el canal se convierte en un problema en un sistema de difusión, por lo que se deben utilizar mecanismos para protocolos que

eviten la contención, como el de paso de señal (token passing) o el de detección de portadora (carrier sense).

Aprovechando las ventajas de las propiedades mencionadas, los protocolos de las capas de red/enlace se han implementado en varias redes locales con las siguientes características: conmutación de mensajes; carencia de mensajes explícitos de reconocimiento debido a las bajas tasas de error, difusión y/o multidifusión.

Los protocolos de las redes locales, pueden dividirse en dos niveles básicos: **protocolos de bajo nivel y protocolos de alto nivel.** En cada nivel, las características de las redes locales producen efectos en el diseño y funcionalidad de los protocolos.

### 3.2.3 Protocolos de bajo nivel.

El término "protocolo de bajo nivel" identifica a los protocolos básicos utilizados para transportar grupos de bits a lo largo de la red con la oportunidad y la veracidad apropiadas. Los protocolos de bajo nivel no conocen el significado de los bits transportados. Dos aspectos de las redes locales tienen un fuerte impacto en el diseño de los protocolos de bajo nivel: primero, el alto rendimiento realizado puramente mediante tecnología de hardware que proporciona la simplificación de los protocolos; y segundo, los protocolos de bajo nivel deben diseñarse para aprovechar las ventajas y preservar las capacidades especiales de las redes locales, de manera que estas capacidades puedan utilizarse, a su vez, por los protocolos de alto nivel.

* Simplificación. Las redes locales deben soportar una amplia variedad de hosts ( computadoras que procesan las aplicaciones de los usuarios), desde procesadores dedicados hasta grandes sistemas de tiempo compartido. La existencia de hosts extremadamente simples conducen al requerimiento de

protocolos de bajo nivel simples y flexibles que puedan ser implementados económicamente en pequeños hosts, no comprometiendo el rendimiento de hosts mayores.

Dos factores intervienen en la simplicidad de los protocolos de bajo nivel de redes locales:

a) Uso limitado de bits de control (overhead)

b) Control de flujo simplificado

* Capacidades especiales. Los protocolos convencionales de bajo nivel han provisto una función mejor caracterizada como un flujo bidireccional de bits entre dos entidades comunicándose: un circuito virtual.

El circuito virtual es implementado por un proceso que otorga una entrega secuencial de paquetes a su destino. Además de que un circuito virtual es una forma importante de comunicación, las redes locales proporcionan otras dos que son muy útiles en una gran variedad de contextos:

a) Comunicación por intercambio de mensajes.

b) Comunicación por difusión.

### 3.2.4 Protocolos de alto nivel.

Los protocolos de bajo nivel de una red local, existen para apoyar a los protocolos de alto nivel, los cuales a su vez, refuerzan las aplicaciones del usuario.

* Acceso a recursos comunes. El modelo de cómputo más común es el de una gran computadora centralizada, con componentes remotos como terminales y, tal vez algunos otros dispositivos de entrada/salida.

Una aplicación simple, pero muy importante de una red local es generalizar esta idea ligeramente para incluir más de una computadora central. A medida que crece la carga de trabajo excediendo la capacidad de una sola máquina, una solución común es procurar una segunda máquina, y dividir las aplicaciones y la carga de trabajo entre las dos máquinas. El problema de comunicación a resolver

es simple pero crítico, permitir a una terminal individual tener acceso a ambas máquinas centrales.

### 3.2.5 Especificación de Protocolos.

Se asume que la arquitectura de comunicación de un sistema distribuido está estructurada como una jerarquía de diferentes capas de protocolo, cada capa provee un conjunto particular de servicios a sus usuarios superiores. Desde este punto de vista, la capa puede ser vista como una caja negra o máquina que permite una cierta interacción con otros usuarios.

Un usuario está involucrado con la naturaleza del servicio provisto, pero no así con la forma en que el protocolo se arregla para proveerlo.

La descripción de la conducta de entrada/salida de la capa de protocolo constituye una especificación de servicio del protocolo. Debe ser abstracta en el sentido de que describe los tipos de comandos y sus efectos, pero deja abierto el formato exacto y los mecanismos para conducirlos. Estos formatos y mecanismos pueden ser diferentes para los usuarios en distintas partes del sistema y están definidas por una especificación de interface.

Una especificación de protocolo es un refinamiento o implementación distribuida de su especificación de servicio, de forma tal que define parcialmente cómo se proporciona el servicio. Esta implementación del servicio es lo que usualmente se conoce por diseño de una capa de protocolo. La especificación del protocolo debe definir cada entidad al grado necesario de asegurar la compatibilidad con las otras entidades de la capa.

Un protocolo no puede ser definido sin describir su contexto. El contexto está dado por la capa de la arquitectura del sistema distribuido en donde se utiliza el protocolo. Una descripción de una capa debe incluir los siguientes elementos:
1) Una descripción general del propósito de la capa y de los servicios que proporciona.

2) Una especificación exacta del servicio que será proporcionada por la capa.
3) Una especificación exacta del servicio provisto por la capa inferior, y requerida para la operación correcta y eficiente del protocolo.

4) La estructura interna de la capa en términos de entidades y sus relaciones.

5) Una descripción del o de los protocolos utilizados entre las entidades, incluyendo:

*a*) Una descripción informal que abarque toda la operación de las entidades.
*b*) Una especificación del protocolo que incluye, primero una lista de los tipos y formatos de los mensajes intercambiados entre las entidades; y segundo, reglas que gobiernan la reacción de cada entidad a los comandos del usuario, mensajes de otras entidades y eventos internos.
*c*) Cualquier detalle adicional, como por ejemplo, consideraciones para perfeccionar la eficiencia, sugestiones para opciones de implementación, o una descripción detallada que puede aproximarse a una implementación.

### 3.2.6 Verificación de Protocolos.

En su interpretación más general, la validación de sistemas tiene el propósito de asegurar que un sistema satisfaga sus especificaciones de diseño y opera a satisfacción de sus usuarios. La actividad de validación es importante durante todas las fases de diseño, y puede incluir, la prueba de la implantación final del sistema, estudios de simulación, predicciones de rendimiento y verificación.

La verificación está basada en la especificación del sistema e incluye razonamiento lógico. Puede también utilizarse durante la fase de diseño antes de que exista cualquier implementación del sistema, para evitar posibles errores de

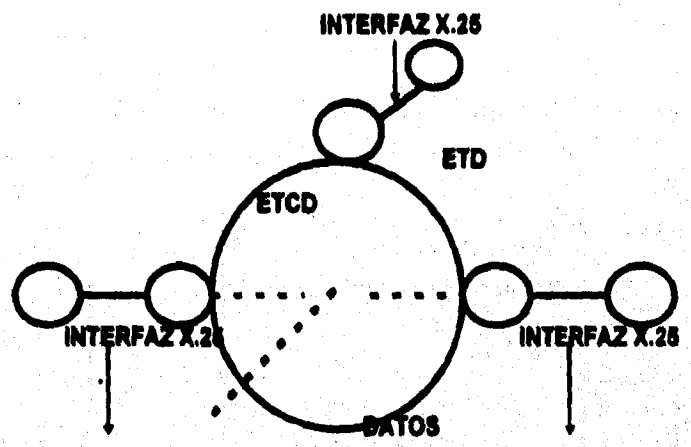
diseño.. Mientras que las pruebas y la simulación sólo validan el sistema para ciertas situaciones, la verificación permite, en un principio, la consideración de todas las posibles situaciones que el sistema puede encontrar durante la operación actual.

La verificación es esencialmente una demostración de que un objeto responde de manera satisfactoria a sus especificaciones.

## 3.3 PROTOCOLO X.25

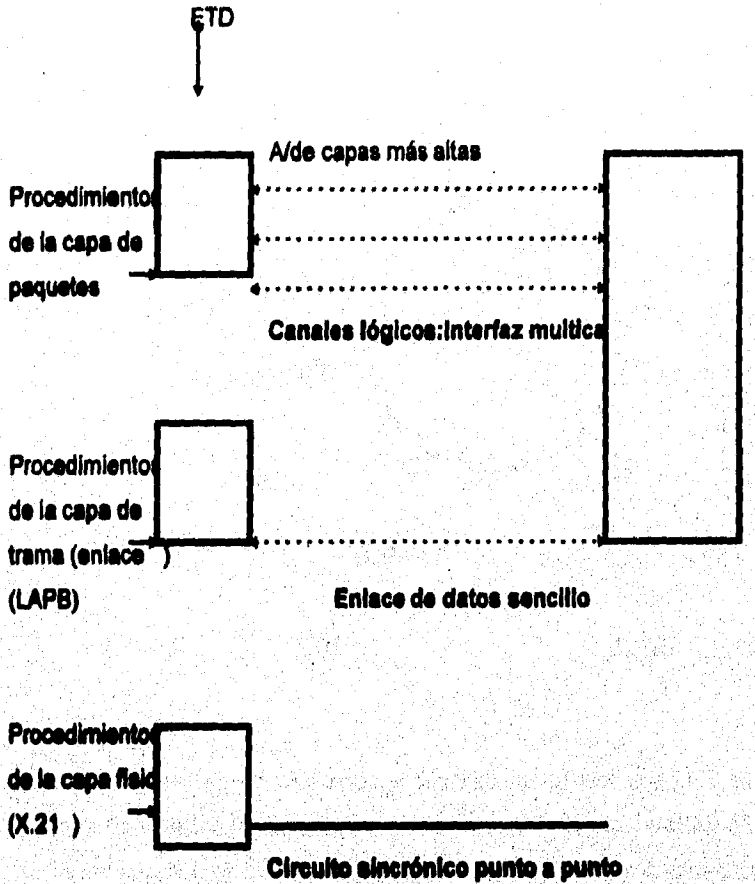
El protocolo X.25, aunque en sentido estricto no es una arquitectura de red, constituye un protocolo por capaa que presenta varias de las propiedades de las arquitecturas de redes. X.25 es una recomendación de interfaz, esto es, describe los protocolos de interfaz que se requieren para permitir a un equipo terminal de datos (ETD) comunicarse con un equipo terminal de circuitos de datos (ETDC), que se supone proporcionará acceso a una red de conmutación de paquetes.

La idea básica de este protocolo se muestra en la figura siguiente:




Los ETD que desean comunicarse a través de una red de datos lo hace estableciendo interfaces X.25 con la red. La red maneja entonces la entrega de los datos necesarios entre los ETCD. La arquitectura X.25 supone que la red de datos es del tipo de conmutación de paquetes, aunque esto no es necesario, ya que solo se prescriben protocolos de interfaz entre la red y los usuarios (ETD). Los ETD pueden ser cualquier clase de terminal inteligente o computador equipado para manejar le protocolo X.25. Se dispone para ello de los llamados PAD (ensambladores-desensambladores de paquetes) que se pueden conectar a terminales comunes para que estas funcionen como ETD.

Se prescriben tres capas para el protocolo X.25. Estas capas se muestran esquemáticamente en la figura siguiente:




La capa más baja es, por supuesto, la capa física. La recomendación X.21 de CCITT (BERT), (FOLT1980a) es el procedimiento de capa física adoptada por X.25. El protocolo de capa de enlace o trama que usa el circuito síncrónico de punto a punto establecido por X.21 consiste en un conjunto de procedimientos llamado LAPB (*balanced link access procedures*, procedimientos balanceados de acceso al enlace). Los procedimientos LAPB forman un subconjunto de HDLC y ADCCP y son compatibles con ellos. La capa de enlace usa una estructura de trama para llevar de manera confiable los datos (paquetes) entre los dos extremos

del enlace. Es la tercera capa, la capa de paquetes, la que está totalmente prescrita en X.25. Esta capa corresponde a la capa de red en las arquitecturas de redes.

## 3.4 ALGORITMOS DE ACCESO.

### 3.4.1 MÉTODOS DE ACCESO

Los métodos de acceso definen a quién se le va a otorgar el canal para transmitir en un momento dado.

Método de acceso.

La necesidad de los protocolos multi-acceso aparece siempre que un recurso es compartido ( y por tanto accesado) por un número de usuarios independientes.

Dos razones principales que contribuyen a esta situación son: el requerimiento de los usuarios para compartir recursos caros y además escasos aunado a la necesidad de comunicación entre las distintas entidades. El problema radica en como controlar el acceso a un canal común para asignar de forma eficiente el ancho de banda disponible para los usuarios. Las soluciones a estos problemas forman un conjunto de protocolos conocidos como métodos de multi-acceso. Estos protocolos y su rendimiento difieren de acuerdo al medio ambiente en cuestión y los requerimientos que el sistema debe satisfacer.

Para cuestiones de confiabilidad, los métodos de acceso son evaluados de acuerdo a varios criterios. Las características de ejecución que deseables son, primeramente, alta utilización del ancho de banda y bajos retrasos de mensaje. Pero un número de otros atributos son de igual importancia. La habilidad de un protocolo de acceso de soportar simultáneamente tráficos de diferentes tipos, diferentes prioridades, con longitud variable de los mensajes, y diferentes causas de retraso, es esencial a medida que la alta utilización del ancho de banda es otorgada por el multiplexaje de todos los tipos de tráfico. También, para garantizar

la operación propia de esquemas con control distribuido, es deseable tener un sistema insensible a los errores que resultan de información errónea.

### 3.4.2 Relación de los métodos de acceso con los protocolos de comunicación.

Los protocolos de comunicación, como se ha mencionado, son herramientas utilizadas para el control de la transferencia de información entre sistemas de computadoras.

Los métodos de acceso, son en sí, un conjunto de protocolos de comunicación a nivel de enlace, que sirven para controlar el acceso a recursos comunes compartidos por varios usuarios.

Estos protocolos de acceso son protocolos de bajo nivel puesto que son utilizados para transportar grupos de bits a través de la red. Los métodos de acceso sirven de base a los protocolos de aplicación de alto nivel.

Los métodos de acceso son muy importantes en el contexto de las redes locales, ya que requiere de un mecanismo que determine qué usuario puede utilizar el canal de transmisión y en que momento debe hacerlo. En este ambiente, el rendimiento de un protocolo de acceso para una red de difusión, depende principalmente de qué tan rápido puede identificarse uno de los usuarios listos para transmitir , dándole un acceso único al canal compartido.

### 3.4.3 Clasificación general de los métodos de acceso.

Los métodos de acceso difieren en la naturaleza estática o dinámica del algoritmo de asignación del canal (esto es , si al usuario se le asigna un tiempo fijo de transmisión, o por el contrario, este tiempo varía según las necesidades del sistema ), la naturaleza centralizada o distribuida del proceso de toma de decisiones, y el grado de adaptabilidad del algoritmo a las necesidades cambiantes. De acuerdo a esto, los métodos de acceso pueden agruparse en cinco clases principales:

-Técnicas de asignación fija.

-Técnicas de acceso aleatorio
-Asignación de demanda controlada centralmente.
-Asignación de demanda con control distribuido.
-Estrategias adaptables y modos mixtos.

**a)Técnicas de asignación fija.**

Estas técnicas consisten en asignar el canal al usuario, independientemente de su actividad, particionando el espacio en tiempo del ancho de banda en divisiones (slots) que son asignados en una forma estática predeterminada.

Las técnicas de asignación fija toman dos formas comunes:

-ortogonal: como por ejemplo el acceso múltiple por división de frecuencia (FDMA) o el acceso múltiple por división de tiempo (TDMA).

-quasi-ortogonal: como en el acceso múltiple por división de código (CDMA).

**b)Técnicas de acceso aleatorio.**

En la comunicación de computadoras, gran parte del tráfico de información es caracterizado como "explosivo" (bursty), esto es, tráfico interactivo de terminal. La explosividad es un resultado del alto grado de aleatoriedad observado en el tiempo y tamaño de los mensajes y del relativo retraso requerido por el usuario. Si alguien observara la conducta de un usuario a través de un período de tiempo, vería que el usuario requiere de los recursos de comunicación mas bien infrecuentemente, pero cuando lo hace, requiere de una respuesta rápida. Esto es, existe una gran relación pico promedio en la tasa requerida de transmisión de datos. Si se utilizan esquemas de asignación fijos de subcanal, entonces debe otorgársele suficiente capacidad a cada subscriptor para encontrar sus tasas pico de transmisión con la consecuencia de que la utilización del canal resultante es baja. Un enfoque más ventajoso es el de proporcionar un solo canal compartible de alta velocidad al gran número de usuarios.

La existencia de algún esquema positivo de reconocimiento permite al transmisor determinar si su transmisión es exitosa o no. El problema es como controlar el acceso al canal común de una forma que produzca, bajo las limitaciones físicas de simplicidad e implementación de hardware un nivel aceptable de rendimiento. La dificultad de controlar un canal que debe llevar su propio control de información ha dado lugar a los protocolos de acceso aleatorio.

Algunos ejemplos de esta técnica:

-Aloha: para la red desarrollada en 1970 en la Universidad de Hawai, permite al usuario transmitir en el momento que desee. Si ocurre una colisión el usuario retransmite su información.

-Acceso múltiple por detección de portadora (CSMA): Es efectivo en comunicaciones de área local. Los usuarios pueden detectar el canal para saber si alguien más está transmitiendo.

-Acceso múltiple por extensión de espectro (SSMA): Aplicaciones en comunicación vía satélite y redes de computadoras, permite que el receptor capture en paquete, en lugar de que el usuario capture el canal.

c) Asignación de demanda controlada centralmente.

Las técnicas de asignación de demanda requieren que se intercambie información explícita de acuerdo a las necesidades del recurso de comunicación. En este caso, la asignación de demanda es controlada por un organizador (scheduler) central. Como ejemplos se tienen:

-Sistemas orientados al circuito: en estos sistemas, el ancho de banda es dividido en canales, ya sea en frecuencia o en tiempo, que son asignados en demanda. Estos sistemas sólo son atractivos cuando las aplicaciones tienen un tráfico tipo stream (chorro o corriente).

-Sistemas de sondeo (polling): Son utilizados principalmente en una topología de estrella en las redes locales. Un controlador central envía mensajes a

las terminales, preguntándoles, una a una, si tienen alguna información que transmitir.

-Acceso múltiple por reservación de canal dividido (SRMA): el ancho de banda disponible es dividido en dos canales: uno utilizado para transmitir información de control, y el segundo usado para los mensajes de información mismos.

-Acceso múltiple por controlador global (GSMA): es un esquema multi-acceso adecuado para una línea o bus de alta velocidad, que está basado en el concepto de división del tiempo para reservación. Un controlador revisa todas las tareas de los usuarios conectados a la misma línea, los cuales transmiten cuando se les asigna un subcanal (slot) durante una cierta cantidad de tiempo.

d)Asignación de demanda con control distribuido.

Existen dos razones por las que el control distribuido es deseable. La primera es la confiabilidad; con el control distribuido el sistema no es dependiente de la operación de un controlador central. La segunda, es una mejora en el rendimiento, especialmente cuando se trata de sistemas con grandes retrasos de propagación, como los satélites.

El elemento básico que caracteriza a los algoritmos distribuidos es la necesidad de intercambio de información entre los usuarios, ya sea explícita o implícitamente.

Algunos ejemplos de estos esquemas pueden ser:

-Aloha con reservación: Se utiliza en canales de satélite y se basa en un eje de tiempo dividido en subcanales, los que están organizados en estructuras (frames) de igual tamaño. La duración de una estructura debe ser mayor que el retraso de propagación del satélite.

-Esquema de reservación primero-en-entrar, primero-en-salir (FIFO): En este esquema, las reservaciones se hacen explícitamente. La división de tiempo se utiliza para proporcionar un subcanal de reservación, otorgado mediante la disciplina FIFO.

-Esquema de reservación circular (RR): La base de este esquema es la asignación fija en tiempo, pero con la diferencia de que los subcanales libres son asignados a las estaciones activas en una forma round-robin (circular). Es utilizado en canales de satélite.

-Algoritmos de control distribuido en redes locales: Se utilizan con una topología de anillo (ring), en donde los mensajes no son difundidos, sino que son pasados de nodo a nodo a lo largo de enlaces unidireccionales, hasta que regresan al nodo origen.

a) Estrategias adaptables y modos mixtos.

Cada uno de los esquemas anteriores tiene sus ventajas y limitaciones. Ningún esquema actúa mejor que los otros sobre el rango completo de la capacidad de canal del sistema. A pesar de que algunas características de un sistema (como el retraso de la propagación, la velocidad del canal, etc.) probablemente no varían durante la operación, el peso del sistema estará sobre la variación en el tiempo.

Actualmente lo que se necesita es una estrategia para elegir un método de acceso que sea adaptable a las necesidades variables de manera que la optimización se mantenga todo el tiempo. El tipo y la cantidad de información requeridos por una estrategia aceptable, así como la implementación del mecanismo de adquisición de información, están entre los factores cruciales al determinar el rendimiento y fortaleza de la estrategia.

Algunos ejemplos de estas técnicas son:

-Esquema de urna (urn): Es un esquema simple y elegante en el que el eje de tiempo está dividido en subcanales y todos los usuarios están sincronizados. Asumiendo que todos los usuarios conocen el número exacto de usuarios ocupados, el esquema consiste en dar acceso completo (esto es, transmitir con probabilidad igual a uno) a un número k de usuarios.

-Esquemas de reservación sobre colisión (RUC): En estos esquemas, el canal es dividido en subcanales de longitud fija, en el eje de tiempo, los que a su

vez están divididos en dos partes: un subcanal de datos para la transmisión de paquetes de información y un subcanal de datos para la transmisión de paquetes de información y un subcanal de datos para la transmisión de información concerniente a los usuarios. El subcanal de información puede estar en uno de dos estados, el estado de contención o el estado reservado. Es normalmente en el estado de contención donde los usuarios pueden accesar los subcanales mientras no ocurra una colisión. Si una colisión es detectada, el subcanal cambia al estado reservado y permanece así hasta que es despejada la cola de reservaciones.

-Aloha con detección de portadora (MACS): Este esquema consiste en permitir a un usuario "atrapar" , por detección de portadora, subcanales que no están siendo utilizados por una gran población de pequeños usuarios accesando el canal en un modo de Alohas con subdivisión de canal.

-Acceso aleatorio de grupo (GRA): Estos procedimientos consisten en utilizar ciertos períodos de tiempo para permitir que algunas terminales de la red transmitan su información mediante una base de acceso aleatorio de grupo, procedimientos de reservación o de asignación fija.

### 3.4.4 MÉTODOS DE ACCESO EN REDES DE ÁREA LOCAL.

**Métodos de sondeo (polling).**

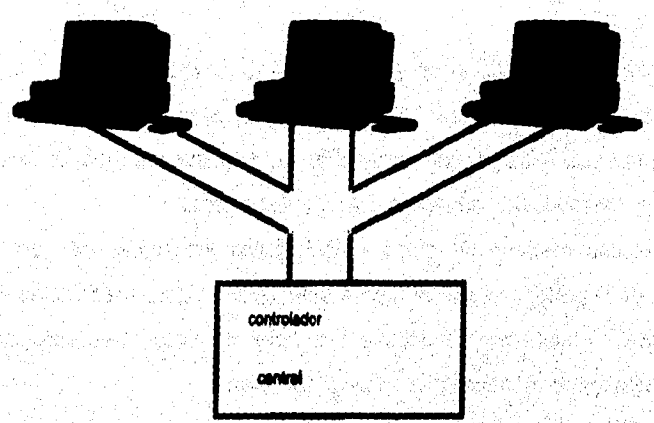
El sondeo es un método de acceso al medio de transmisión con un control central, utilizado generalmente en una topología de estrella.

Existen tres métodos principales de sondeo:

- Sondeo de llamada por turno (roll-calling).
- Sondeo por eje (hub).
- Sondeo adaptable o de prueba (probing).

**a) Sondeo de llamada por turno (roll-calling).**

En este método, un controlador central envía mensajes de sondeo a las terminales, una por una, preguntando a la terminal sondeada si tiene alguna información que transmitir. Para esto, la estación central puede tener una lista conteniendo el orden en que las terminales serán sondeadas. Si la terminal interrogada tiene algo que transmitir, prosigue; si no, una respuesta negativa (o ausencia de respuesta) es recibida por el controlador, el cual sondea a la siguiente terminal en la secuencia. El siguiente esquema muestra este tipo de sondeo:




El sondeo requiere de un constante intercambio de mensajes. Estos contienen una dirección que identifica la terminal que está siendo sondeada. Cada terminal conoce su propia dirección y solo responde a sus propios sondeos, a pesar que recibe todas las preguntas. Por lo general, cada terminal se sondea una vez por ciclo, pero en algunas circunstancias, las terminales que se consideren más importantes pueden ser sondeadas varias veces en un ciclo.

Una vez que una terminal envía la respuesta de que tiene información para enviar, gana el control de la línea y el sondeo no continúa hasta después que la terminal ha enviado su mensaje. Entonces, existe el problema de que en el momento en que la terminal accesa el canal, puede mantenerlo durante mucho tiempo. Para evitar esta condición, algunos sistemas incluyen un "tiempo fuera" programable que permite a la terminal controlar la línea por un periodo específico

de tiempo y entonces rompe la conexión, de manera que a otras terminales no se les excluya de utilizar el canal. De tal forma que el sondeo de llamada por turno es eficiente solo si:

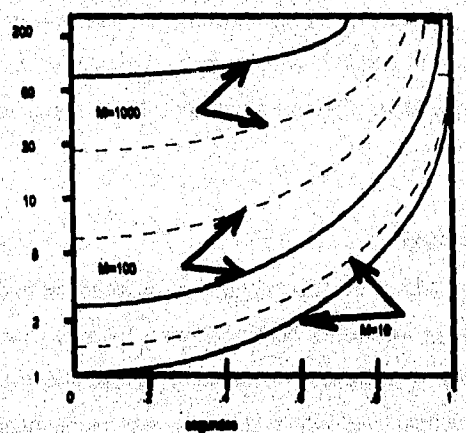
-el retraso de propagación es pequeño,

-la sobreinformación (overhead) debida a los mensajes de sondeo es baja, y

-la población de usuarios no es excesivamente grande.

Análisis detallado:

Para la realización de este análisis se considera a una población de M usuarios compartiendo el canal. Se denota por L la razón entre la longitud del mensaje de información y la longitud del mensaje de sondeo, y "a" será la razón entre el retraso de propagación y el tiempo de transmisión de mensajes. En la siguiente figura que se muestra se observan algunos resultados numéricos correspondientes a los valores típicos de "L" y "a".




Estas curvas muestran que a medida que el tamaño de la población se incrementa, y por tanto se tiene un número más y más grande de usuarios, el rendimiento del sondeo se degrada significativamente. La utilización del canal puede alcanzar un 100% del ancho de banda del canal si a las terminales se les permite vaciar sus buffers (espacio de almacenaje) cuando son sondeadas. Pero

como resultado la variación del retraso de los paquetes puede volverse intolerablemente grande.

b)Sondeo de eje (hub).

En líneas half-duplex (transmisión emisor-receptor y viceversa, no simultáneo) cada sondeo requiere de dos turnos en línea, uno que permite al controlador enviar, y otro para que la terminal envíe información. Ya que el tiempo de turnaround (tiempo que tarda la información en propagarse del origen al destino y viceversa) es del orden de unos cientos de milisegundos, puede llevarse mucho tiempo completar un ciclo en la línea con muchas terminales más aún si éstas permanecen ociosas la mayor parte del tiempo.

El método de sondeo de eje fue diseñado para solucionar este problema. Aquí, el controlador sondea la terminal más alejada de él. La terminal direccionada invierte el sentido de la línea. Si tiene información que enviar, la manda hacia el controlador. De lo contrario, manda un mensaje de sondeo direccionado a su vecina en la línea. Si ésta terminal tampoco tiene nada que enviar, transmite un sondeo a su vecina. El sondeo se propaga de terminal en terminal hasta que encuentre alguna que tenga algo que transmitir o hasta que el sondeo regrese al controlador.

## 3.5 NOVELL NETWARE®.

Dentro de la gama de sistemas operativos para red, existe uno que llama la atención por encima de los demás, Novell Netware. Este sistema operativo por su arquitectura cliente/servidor ha sido el que en el mercado de sistemas operativos para redes se ha popularizado en el mundo y más propiamente en México, a pesar de competir con otros como LAN Manager de Microsoft, Lantastic de Artisoft y más recientemente de NT Advanced Server también de Microsoft ó el próximo a salir OS/2 Warp Server; Netware domina casi el 80% en el mercado mexicano y su filosofía de redes radica en el enfoque de que el sistema operativo se encuentra en el software y no tanto en el hardware de la red.

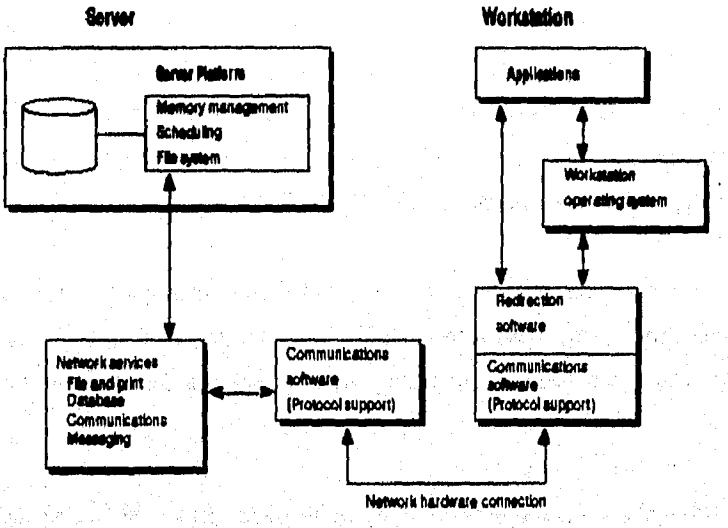
El sistema operativo del servidor de Novell provee un alto rendimiento en la red; también como reside el sistema operativo en el servidor y provee la conectividad que completa el sistema computacional, creando el ambiente en el cual opera la red. Archivo y respaldos, seguridad, impresión e interproceso de comunicación son algunos ejemplos, de las funciones y aplicaciones, que el sistema operativo Novell permite se ejecuten dentro de la red.

Los sistemas operativos de red están diseñados para optimizar la funcionalidad de las aplicaciones de la red, incluyendo la arquitectura, el rendimiento, la confiabilidad, seguridad y soportes estándar del sistema operativo de red.

El sistema operativo de red puede dividirse dentro de los siguientes componentes:

**Sistema Operativo del servidor (Server Operating System)**
**Aplicaciones Cliente/Servidor (Client-Server Applications)**

Estos componentes se combinan para permitir el sistema de comunicación sobre el cual los servicios de red son distribuidos a los usuarios. Esta combinación se muestra en la siguiente figura:




El sistema operativo de red es el corazón de la red, proporcionando la funcionalidad esencial que se necesita para soportar las operaciones más básicas de la red.

El enlace entre el sistema operativo de la estación de trabajo y el sistema operativo de la red en el servidor es proporcionado por el software de comunicaciones de la red, el cual utiliza el hardware de la red para establecer comunicación con otros nodos y servidores de la red. El software de comunicaciones concede los protocolos de comunicaciones que facilita los requerimientos y respuestas que serán enviadas dentro de la red.

Los productos de red contiene una variedad de perfiles que dan al sistema confiabilidad e integridad de los datos. Los siguientes perfiles protegen desde el almacenaje medio hasta archivos de aplicaciones criticas, permitiendo a Novell proporcionar los más altos niveles de confiabilidad red en la industria.

- Verificación de Lectura después de leer (*Read-After-Write Verification.*) Cada escritura en el disco es repasada y verificada para ser leída.

- Duplicación de Directorios (*Duplication of Directories*). Netware mantiene un duplicado de la estructura del directorio raíz. Si la estructura del directorio es dañado, el respaldo permite al usuario tener acceso a los datos de la red.

- Duplicación de FATs (*Duplication of FATs*). Netware mantiene un duplicado de las Tablas de Localización de Archivos, (*File Allocation Tables*), previniendo la contaminación de las FAT por ejecutar un disco inutilizable.

*Hot Fix*. El Hot Fix ofrece la detección de defectos y corrección, durante la ejecución, del disco.

*Tolerancia de Fallas del Sistema (System Fault Tolerance) (SFT)*. La Tolerancia de Falla del Sistema da diversas facetas de confiabilidad, incluyendo discos espejo, disco duplicado y la Transacción de Rastreo del Sistema.

**Sistemas Operativos Novell.**

El servidor de sistemas operativos Novell dota de soluciones para una gran variedad de necesidades.

**Sistema Netware V3.12**

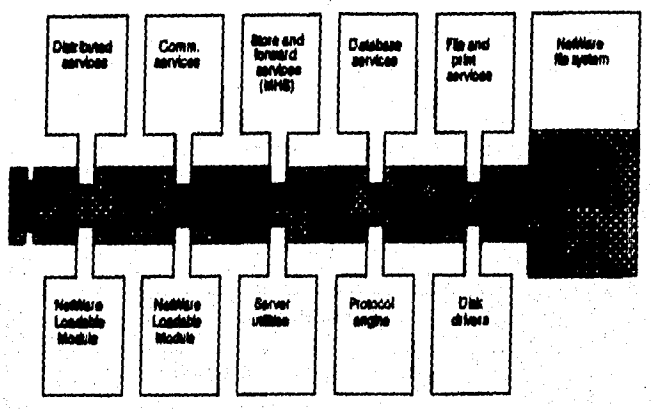
El sistema Netware V3.12 suministra una ruta de migración entre el trabajo en grupo y redes departamentales. Esta diseñado para compañías extensas con redes que soportan cientos de usuarios en un sólo servidor, el sistema Netware V3.12 ha redefinido las capacidades de la tecnología de red; provee para la integración de minicomputadoras, PC's basadas como servidores de red, soporta todos los comandos DOS, Windows, OS/2, UNIX y Macintosh así como el ambiente de IBM SAA.

**Overview.**

El sistema Netware V3.12 proporciona la libertad para diseñar una red con los recursos de computación para el mejor ajuste a las necesidades de organización.

El componente central del Netware V3.12 es el tiempo real de sistema operativo. El tiempo real es la fundación para la rapidez y confiabilidad de la red.

Todos los servicios de red, aplicaciones basadas en el servidor y utilidades del servidor son módulos que pueden ser llamados o vaciados en cualquier momento sin causar baja en el servidor. Estos componentes del sistema son conocidos como Módulos Cargables de Red (*Netware Loadable Modules*, NLMs). La arquitectura modular del Netware V3.12 se muestra en la siguiente figura.




**Estratificación.**

El sistema Netware V3.12 tiene disponibles varias configuraciones útiles. Todas las configuraciones ofrecen la misma funcionalidad; la única diferencia es el número de usuarios que cada una de las versiones soporta.

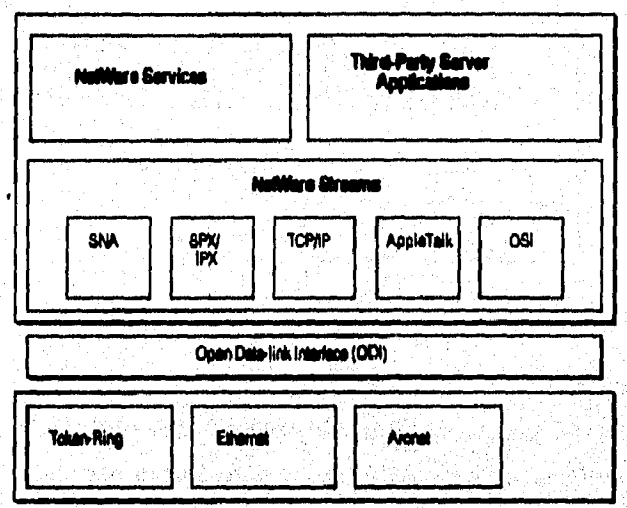
**Soporte para clientes (Client Support).**

El Netware V3.12 soporta una gran variedad de clientes, capacitando a las organizaciones para seleccionar los sistemas operativos que son mejores para ellos.

**Soporte de protocolos (Protocol Support).**

El Netware V3.12 incluye el transporte TCP/IP, una colección de NLMs (*Netware Loadable Modules*), que ofrecen al Netware V3.12 con protocolos de transporte TCP/IP, interfases de Aplicaciones Programadas (APIs) y herramientas para manejar esos protocolos. El protocolo Internet (IP, Internet Protocol) rutea a fin de que el transporte TCP/IP de facilidades al TCP/IP para empaquetar lo que

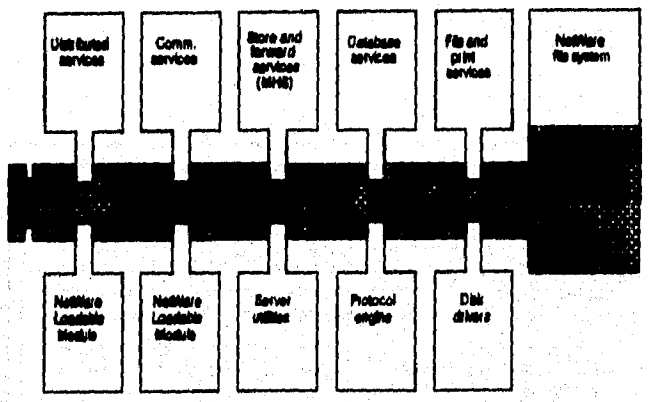
va a ser enviado de una red con sistema Netware V3.12 a otra. "Tunneling" IPX a través de IP facilita al servidor Netware V3.12 el ser conectado entre un TCP/IP Internet. La arquitectura abierta de la ingeniería del Protocolo Netware V3.12 se muestra en la siguiente figura.




Ejemplos de Protocolos que operan con Netware V3.12 son SPX/IPX, TCP/IP, SNA, AppleTalk y OSI TP4.

**Alto rendimiento y capacidad (High Performance and Capacity).**

Netware V3.12 es un sistema operativo multitareas diseñado específicamente para dotar del rendimiento a la red. Existen diferentes sistemas operativos de red que corren por encima de un sistema operativo de propósito general, el Netware accesa al CPU del servidor directamente, operando rápida y más eficientemente. Para aumentar el rendimiento, los adaptadores de red 32-bit NE3200 y NE/2-32 de Novell pueden ser utilizados para incrementar la cantidad




**Estratificación.**

El sistema Netware V3.12 tiene disponibles varias configuraciones útiles. Todas las configuraciones ofrecen la misma funcionalidad; la única diferencia es el número de usuarios que cada una de las versiones soporta.

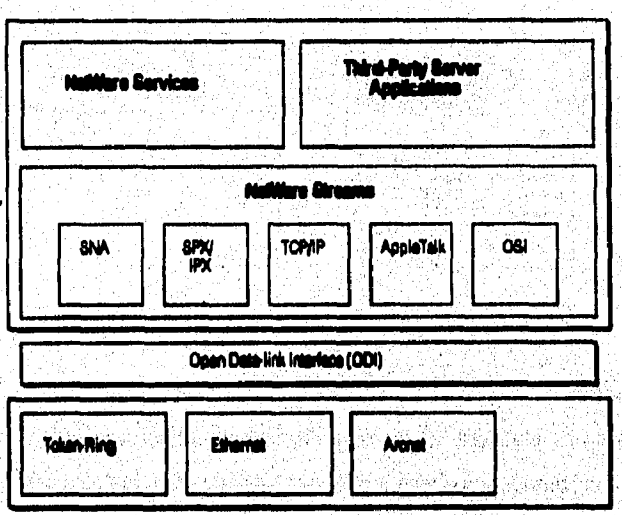
**Soporte para clientes (Client Support).**

El Netware V3.12 soporta una gran variedad de clientes, capacitando a las organizaciones para seleccionar los sistemas operativos que son mejores para ellos.

**Soporte de protocolos (Protocol Support).**

El Netware V3.12 incluye el transporte TCP/IP, una colección de NLMs (*Netware Loadable Modules*), que ofrecen al Netware V3.12 con protocolos de transporte TCP/IP, Interfases de Aplicaciones Programadas (APIs) y herramientas para manejar esos protocolos. El protocolo Internet (IP, Internet Protocol) rutea a fin de que el transporte TCP/IP de facilidades al TCP/IP para empaquetar lo que

va a ser enviado de una red con sistema Netware V3.12 a otra. "Tunneling" IPX a través de IP facilita al servidor Netware V3.12 el ser conectado entre un TCP/IP Internet. La arquitectura abierta de la ingeniería del Protocolo Netware V3.12 se muestra en la siguiente figura.




Ejemplos de Protocolos que operan con Netware V3.12 son SPX/IPX, TCP/IP, SNA, AppleTalk y OSI TP4.

**Alto rendimiento y capacidad (High Performance and Capacity).**

Netware V3.12 es un sistema operativo multitareas diseñado especificamente para dotar del rendimiento a la red. Existen diferentes sistemas operativos de red que corren por encima de un sistema operativo de propósito general, el Netware accesa al CPU del servidor directamente, operando rápida y más eficientemente. Para aumentar el rendimiento, los adaptadores de red 32-bit NE3200 y NE/2-32 de Novell pueden ser utilizados para incrementar la cantidad

de datos que pueden ser movidos dentro y fuera de la red así como dentro de la memoria del servidor.

El Sistema Universal de Archivos del Netware V3.12 proporciona una variedad de perfiles que mejoran el rendimiento. Las Turbo FATs (*File Allocation Tables*) permiten archivar tablas de localización (FATs) en grandes archivos para buscar rápidamente, substancialmente mejorar la rapidez en la lectura del disco.

**Gran capacidad en el sistema de manejo de archivos (High-Capacity File System).**

El Netware V3.12 soporta el máximo almacenaje y memoria requerida posibles bajo la actual tecnología de PC's y esta listo para aprovechar la nueva tecnología que esté disponible. El Netware esta diseñado para soportar hasta 32 TB (*Terabytes*) en disco de almacenaje y hasta 4 GB (*Gigabytes*) en memoria RAM. Con la tecnología actual el Netware V3.12 puede soportar hasta 2048 Mbytes en disco de almacenaje y 256 Gbytes en memoria RAM.

El Sistema Universal de Archivos del Netware V3.12 permite manejar grandes archivos y volúmenes permitiendo al Netware soportar los grandes archivos de Bases de Datos usualmente asociados con minicomputadoras o mainframes.

**Seguridad (Security).**

La seguridad del Netware es proporcionada en capas que sobreenvuelven para proteger los recursos de la red. Estas capas inician en los niveles de archivo y movidos dentro de los directorios de la red, usuarios y passwords y grupos de usuarios.

Los supervisores de la red pueden mantener la seguridad de la red tan simple o complejo como se requiera en la instalación. Un usuario puede ser limitado a utilizar determinados archivos, determinados directorios, o ser restringido a usar una única estación de trabajo o un determinado número de horas al día.

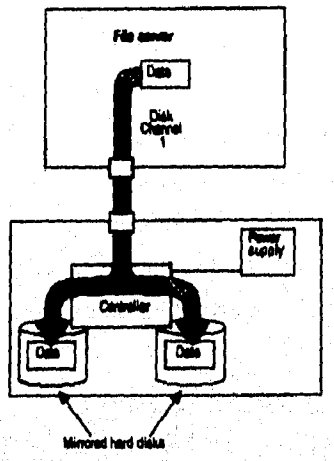
Antes de solicitar los servicios o que los datos sean concedidos, el Netware V3.12 confirma el derecho del usuario a utilizar esos recursos a través de un proceso de autorización. Una vez que la identificación del usuario ha sido confirmada, Netware checa el perfil del usuario para hacer seguro que el usuario esta autorizado para ejecutar la tarea que el o ella esta intentando.

**Confiabilidad (Syatem Reliability).**

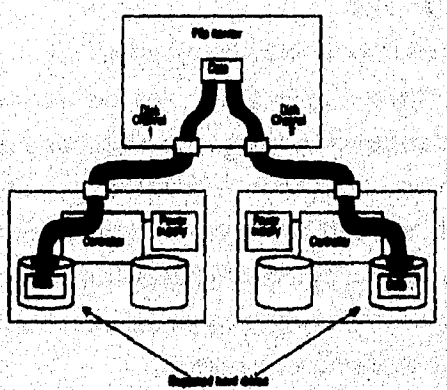
El Sistema de Confiabilidad en la estructura interna del Netware V3.12 incrementa en la red la seguridad por resguardar contra fallas en partes criticas del hardware de la red. Esas tolerancias de falla muestran estas estructuras dentro de la corrida sistema no operativo como procesos el sistema operativo permitiendo al Netware V3.12 el librar la tolerancia de fallas sin sacrificar el rendimiento.

Cada vez que los datos son escritos en el disco de la red, el Netware V3.12 automáticamente ejecuta la verificación read-after-write (Leer después de Escribir). Este proceso garantiza que los datos podrán ser leidos una vez que fueron escritos. Con el Hot-Fix, las áreas defectuosas del disco son etiquetadas como "malas" y listadas en una tabla de bloques malos. Los datos son relocalizados en un área buena conocida sin afectar la operación normal de la red.

Los Discos Espejo permiten al Netware V3.12 proteger el sistema contra pérdida de datos debido a los drives defectuosos en el disco. El Netware V3.12 duplica un volumen fisico entero en un segundo disco duro. Si el disco original falla, el duplicado toma, automáticamente, por otro lado la escritura para no perder información. Para el realce en el proceso de disco el Netware v3.12 soporta hasta ocho discos espejo.




Disk Duplexing proporciona un alto nivel de protección debido a la duplicación entera del canal del disco. Esta protege al sistema contra la pérdida de datos por drives defectuosos en el disco, controladores de disco, interfases y suministro de energía. Fallas en los controladores y canales de disco son detectadas automáticamente, corregidas y LOGGED. Si cualquier componente en el canal del disco falla, el canal redundante entra en funcionamiento automáticamente para no perder la operación o algún dato.



Una función estructurada de monitoreo UPS en el Netware V3.12 monitorea el Suministro Ininterrumpible de Energía (*Uninterruptible Power Supply*, UPS) asignado al servidor y abastecimiento automático, salvaguardar el parar el trabajo de la red si ocurre una falla en la energía. El Sistema de Rastreo de Trámites (*Transaction Tracking System*, TTS) protege los archivos de aplicaciones multiusuarios de contaminación debido a transacciones incompletas. Si un sistema de fallas ocurre durante tal transacción, Netware V3.12 podría salir de la transacción y dejar el archivo como era antes de que la transacción iniciara.

**Manejo de recursos (Resource Management).**

Las facetas del Manejo de Recursos en el Netware V3.12 facilita a los supervisores de la red, checar el estado de cada NLM (*Netware Loadable Module*) corriendo en la red y determinando cuales recursos de los NLM en la red se están utilizando.

Para incrementar la confiabilidad de los NLMs , el sistema operativo realiza consistentemente el chequeo de todos los NLMs, detectando procesos que no han dejado el control frecuentemente y protegiendo contra los NLMs que han guardado recursos. Un NLM autollamado facilita llamar NLMs dependientes si éstos no están ya llamados.

**Servicio de nombres Netware (Netware Name Service).**

El Netware Name Service (NNS), está disponible separadamente del Netware V3.12, es un servicio nombrado que habilita a los usuarios del Netware para accesar recursos en múltiples servidores con un sólo LOGIN. Para los supervisores de la red el NNS simplifica la tarea de mantener un ambiente consistente para el usuario. Para los usuarios de la red, el NNa ofrece un acceso transparente a los recursos computacionales que ellos necesitan, sin importar en cual de las redes se encuentran esos recursos.

**Servicios de Impresión (Printer Services).**

Los servicios de impresión en el sistema Netware V3.12 están proporcionados a través de una aplicación de servidor de impresión que está unido con el sistema operativo. El Netware Print Server V1.21 puede soportar hasta 16 impresoras en la red por cada servidor de impresión, y múltiples servidores de impresión pueden ser instalados en una sola red.

**Requerimientos de Hardware (Required Hardware).**

El Netware V3.12 requiere un servidor de red, estaciones trabajo y adaptadores de red que han sido instalados y conectados correctamente. En el servidor se requiere un mínimo de 4 MB en RAM. Más memoria puede ser requerida dependiendo del número de usuarios, el número de NLMs llamados y el tamaño del disco duro de la red. Para llamar el software, el servidor puede ser equipado con drives de disquetes de alta capacidad.

IBM PCs, XTs, ATs y compatibles, todos los modelos de la familia de computadoras IBM PS/2, el Macintosh SE, Plus y 512Ke, y todos los modelos de la familia de computadoras Macintosh II pueden ser usados como estaciones de trabajo en la red.

El tipo de adaptador de la red a usar depende del tipo de computadoras utilizadas como servidor o como estaciones de trabajo. En servidores de 32bit Micro Canal en redes Ethernet Novell recomienda usar el NE/2-32. El bus de 32-bit del NE/2-32 permite a los usuarios ganar el mayor rendimiento potencial del Netware V3.12 para incrementar la cantidad de datos que pueden ser movidos dentro y fuera de la red y dentro de la memoria del servidor.

Para los servidores Extended Industry Standard Architecture (EISA) de redes Ethernet, Novell recomienda el NE3200, un adaptador maestro de bus de 32-bit.

### 3.6 Spectrum 3.0

En la actualidad, la complejidad de las redes y la creación continua de diferentes productos de software que operan con diferentes protocolos, los cuales se encuentran a la vanta, pueden hacer que las tareas de dirección de la red lleguen a ser incomprensibles. Afortunadamente para los administradores de redes, las plataformas de administración de redes están arribando al ambiente con una mayor apertura e interoperabilidad que las plataformas anteriores.

Estos altos niveles en las plataformas y aplicaciones proporcionan al administrador de la red un gran control y una gran penentración en los variados recursos de red. Los resultados que se pueden obtener son: una asombrosa reducción en el tiempo de respuesta de la red, incremento en la eficiencia de la red y una considerable pérdida en el esfuerzo para la administración personal de la red.

Spectrum 3.0 es una plataforma de administración de redes que proporciona una independencia entre el protocolo y el programa administrador para obtener una mayor integración del sistema; proporciona información de la red al momento de realizar algún cambio en la misma, corrección de problemas y localización de puntos que presentan problemas.

Además presenta de manera gráfica el modelo de la red para localizar múltiples perspectivas de manera visual en una red compleja.

- Proporciona una avanzada capacidad de administración para todos los ambientes de redes: LAN, WAN, SNA, PBX y ATM.

- Aisla automáticamente errores ya sean grandes o pequeños.

- Proporciona acciones correctivas para asistir al personal de la red en la solución de problemas.

- Provee una alarma inteligente "filtrante", que ayuda a minimizar el tiempo requerido para localizar fallas.

El SPECTRUM 3.0 contiene 8 pantallas básicas que son:

- Topologías
- Localización
- Rendimiento
- Organización
- Alarma
- Eventos
- Pérdida y Origen
- Búsqueda

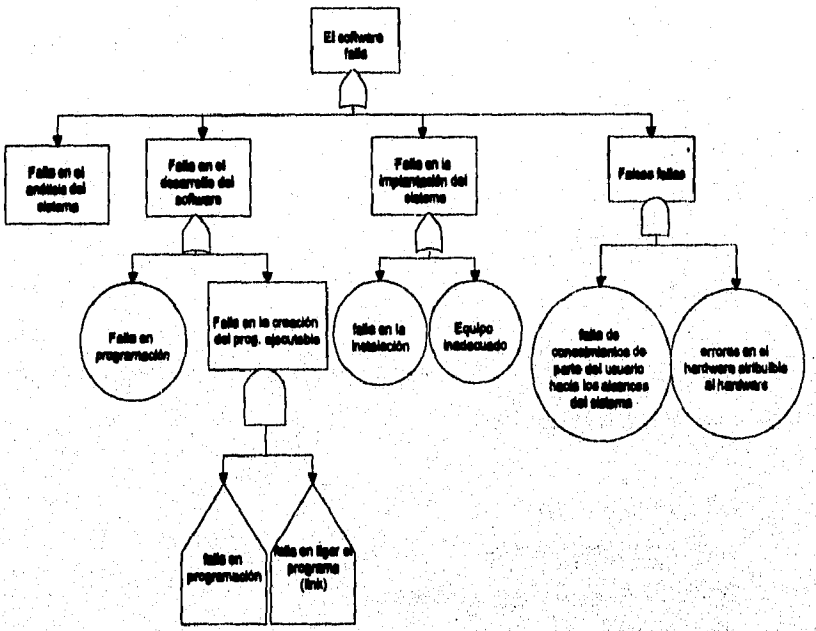
Dentro de las diferencias que contiene esta plataforma con respecto a otras podemos considerar las siguientes:

- Aislamiento de fallas
- Soporte de Multiprotocolos
- Verdaderas arquitecturas cliente/servidor
- Operación en Múltiples plataformas UNIX
- Facilidad para acostumbrarse a cajas de herramientas

Aunque en esta tésis se maneja principalmente el sistema operativo Novell Netware es importante resaltar que existen otros que quizas sean mejores dependiendo de el uso y equipo instalado dentro de una empresa, como es el caso de Windows NT de Microsoft, OS/2 Lan Server de IBM, Bines de Banyan, Lantastic de Artisoft, etc. y que valdria la pena evaluarlos unos contra otros en otra investigación.

Finalmente podemos concretizar que el árbol de falla del software se podría definir como el siguiente, ya que como vimos al principio del capítulo no podríamos definir una función de densidad para el software ya que cada uno presenta sus diferentes problemas en las fases de desarrollo del mismo, a

continuación se presenta un árbol de fallas del software que puede ser una buena base para el estudio en quizás otra investigación más profunda.



# CAPITULO IV

## CONFIABILIDAD DE UNA RED DE ACUERDO A LAS TOPOLOGÍAS MAS USUALES

***LA RED DE LA ENEP ACATLÁN.***

La Red de Área Local de la ENEP esta conformada por seis servidores que trabajan bajo el sistema operativo Novell Netware ver. 3.12 con capacidad para 175 usuarios sumando el número de licencias. Dentro del plantel se puede hacer uso de los seis en línea, es decir acceder a los seis al mismo tiempo, pero con la restricción de tener un usuario creado en cada uno de ellos. Lo importante de esta red es que se pueden utilizar recursos diversos que contiene cada servidor.

Uno de los servidores mencionados tiene capacidad para 50 usuarios y es parte fundamental del Depto. de Sistemas de Información (DSI). Dentro de éste se maneja una buena parte administrativa de la escuela y se desarrollan en él los sistemas en red que funcionan en las divisiones y en otros órganos.

Otro servidor tiene capacidad para 25 usuarios y esta destinado a la utilización por parte de los alumnos para desarrollo académico. Este contiene además, una gran cantidad de software para diversos propósitos, cabe mencionar que dicho software puede ser accesado desde cualquier nodo de la red de la escuela.

Un tercer servidor pertenece al Centro de Idiomas Extranjeros y tiene también una capacidad de 25 usuarios. La finalidad de este servidor es almacenar los programas que se desarrollan en el DSI para la administración del CIE.

Los otros tres servidores pertenecen al la Unidad de Administración Escolar y la Secretaría Administrativa, los cuales se manejan de manera autónoma sin estar directamente bajo la supervisión del Centro de Cómputo.

El estudio de esta red represento un reto, desde el punto de vista técnico y la planeación que existe para poder llevar a cabo un proyecto de tal magnitud. Desde la planeación de esta red se contó con la asesoría de empresas como Adder, Ossys y Neeps, las cuales fueron las encargadas de la planeación e

instalación. Cabe mencionar que mientras se desarrolló el trabajo de investigación se encontraron deficiencias en las instalaciones y por ende falta de confiabilidad.

Los mayores puntos de conflicto se generaron al crear la red, es decir, al momento de diseñarla sobre papel no existía una planeación cuidadosa con estrategias bien establecidas pensando en cuanto podría crecer la red. De ahí que los mismos proveedores no pensaran en función de una red global y realizaran trabajos que no eran adecuados para una red de esta forma.

A continuación se describirán algunos aspectos importantes de la red de la ENEP Acatlán que sin llegar a ser un estudio exhaustivo si presenta un panorama global de la red, sus problemas y finalmente la solución de los mismos.

***DESCRIPCIÓN TÉCNICA DE LA RED DE LA ENEP ACATLÁN:***

En esta parte se describen los aspectos fundamentales en materia de hardware y software, es decir las características de los equipos y el software que se utiliza para la comunicación y el intercambio de información.

| [redacted] | [redacted] |
|---|---|
| **Servidor DSI:**<br>Servidor HP 486 DX2-66 Mhz<br>24 Mb de RAM<br>HD SCSI de 511 Mb<br>Tarjeta de interfase HP Ethertwist de 16 bits modelo AM2100<br>Monitor VGA de 13'' monocromático (B/N) | Partición primaria MS-DOS ver. 6.0<br>Partición no primaria Novell Netware ver. 3.12 50 usuarios<br>Netshield de Mcafee Associates México, S.A de C.V. |
| **Servidor COMPUTO:**<br>Hp 486DX2<br>NetServer Serie LE<br>24 Mb RAM<br>Monitor monocromático VGA de 13". | Partición primaria MS-DOS ver. 6.0<br>Partición no primaria Novell Netware ver. 3.12 para 25 usuarios |
| **Servidor CIES:**<br>Servidor HP 486 DX2-66 Mhz<br>24 Mb de RAM<br>HD IDE de 240 Mb<br>Tarjeta de interfase HP Ethertwist de 16 bits modelo NE2100<br>Monitor VGA de 13'' monocromático (B/N) | Partición primaria MS-DOS ver. 6.0<br>Partición no primaria Novell Netware ver. 3.12 25 usuarios<br>Netshield de Mcafee Associates México, S.A de C.V. |
| **Servidor SRIAADMVA_A7:**<br>Servidor HP 486 dx2 a 66 Mhz<br>32 Mb de RAM | Partición primaria MS-DOS ver. 6.0<br>Partición no primaria Novell Netware 25 usuarios |

| | |
|---|---|
| HD IDE de 410 Mb<br>Tarjeta de interfase 3 Com de 16 bits modelo 3c5x9<br>Monitor monocromático de 14" | |
| Servidor ACAUAE1:<br>Servidor 486 66 Mhz<br>24 Mb de RAM<br>HD IDE de 410 Mb<br>Tarjeta de interfase 3COM de 16 bits modelo 3C5X9<br>Monitor 14" de Monocromático de 14" | Partición primaria MS-DOS ver. 6.2<br>Partición no primaria Novell Netware ver 3.11 para 25 usuarios |
| Servidor UAE2006:<br>Servidor Pentium 75 Mhz<br>24 Mb de RAM<br>HD IDE de 410 Mb<br>Tarjeta de interfase 3COM de 16 bits modelo 3C5X9<br>Monitor 14" de Monocromático de 14" | Partición primaria MS-DOS ver. 6.2<br>Partición no primaria Novell Netware ver 3.12 para 25 usuarios |

Como se revisó en capítulos anteriores las tarjetas y los equipos son parte primordial de la red de la escuela, de tal forma que es importante verificar cada uno de estos para conocer más a detalle el funcionamiento de la red en su conjunto, aquí se describe cada uno de los equipo administrados por el Departamento de Sistemas de Información y del cual se tiene un control estricto para asegurar que la confiabilidad de la red se mantenga en un buen nivel.

| | | | | |
|---|---|---|---|---|
| **Centro de Idiomas Extranjeros** | | | | |
| ACER | 286 | Cabletron 8 bits | C.I.E. | Español |
| ACER | 286 | Cabletron 8 bits | C.I.E. | Alemán |
| ACER | 286 | 3Com 16 bits | C.I.E. | Francés |
| ACER | 286 | Cabletron 8 bits | C.I.E. | Ingles |
| ACER | 286 | 3Com 16 bits | C.I.E. | Ingles |
| ACER | 286 | 3Com 16 bits | C.I.E. | Italiano |
| ACER | 286 | 3Com 16 bits | C.I.E. | Portugués |
| **Edificio de Gobierno** | | | | |
| ACER | 386 | Cabletron 8 bits | Dirección | C-111 |
| ACER | 386 | HP 16 bits NE2100 | Dirección | C-111 |
| ACER | 286 | 3Com 16 bits | Co. Serv. Acad. | E.G. PB. |
| ACER | 286 | 3Com 16 bits | Srio. Direcc. | C-219 |
| ACER | 286 | Cabletron 8 bits | Srio. Gral. | C-111 |
| ACER | 386 | 3Com 16 bits | Planeación | C-203 |
| ACER | 486 | 3Com 16 bits | Planeación | C-204 |
| **Divisiones** | | | | |
| HYUNDAY | 386 | Cabletron 8 bits | Div. Dis. Edif. | A-3 |
| HP VECTRA | 286 | Cabletron 8 bits | Div. Hum. | A-8 |
| HP VECTRA | 286 | HP 16 bits NE2100 | Div. Mat. Ing. | A-1 |
| HP VECTRA | 286 | Cabletron 8 bits | Div. Soc. | C-602 |
| HP VECTRA | 286 | Cabletron 8 bits | Div. Juridicas | A-12 |
| **Secretaría Administrativa** | | | | |
| Acer | 286 | 3Com 16 bits | Cajas | A-4 P.B. |
| **Centro de Información y Documentación** | | | | |
| Acer | 386 | 3Com 16 bits | Biblioteca | Biblioteca P.A. |

| Centro de Cómputo | | | | |
|---|---|---|---|---|
| GAMMA | 486 | HP 16 bits NE2100 | Talleres | C-201 C. Comp. |
| HP | 486 | HP 16 bits NE2100 | DSI | C-207 |
| ACER | 486DX/33 | Cabletron 8bits E1119 | DSI | C-207 |
| HP | 486 | HP 16 bits NE2100 | DSI | C-209 |
| ACER | 486DX/33 | Cabletron 8bits E1119 | DSI | C-211 |
| ACER | 486 | Cabletron 8bits E1119 | DSI | C-213 |
| ACER | 486DX/33 | Cabletron 8bits E1119 | DSI | C-213 |
| ACER | 486DX/33 | Cabletron 8bits E1119 | DSI | C-215 |
| HP | 486 | HP 16 bits NE2100 | DSI | C-217 |
| HP | 486 | HP 16 bits NE2100 | DSI | C-217 |
| ACER | 486DX/33 | HP 16 bits NE2100 | DSI | C-218 |
| HP | 486 | Cabletron 8bits E1119 | DSI | C-220 |
| ACER | 386 | Cabletron 8bits E1119 | DSI | C-221 |
| ACER | 486DX/33 | HP 16 bits NE2100 | DSI | C-222 |
| HP VECTRA | 286 | Cabletron 8bits E1119 | DSI | Terminales |
| HP VECTRA | 286 | Cabletron 8bits E1119 | DSI | Terminales |
| HP VECTRA | 286 | HP 16 bits NE2100 | DSI | Terminales |

Las computadoras descritas anteriormente pertenecen todas a la red que se forma con el servidor DSI, no quedando descartadas aquellas que sin tener una cuenta asignada puedan en un momento dado acceder a este servidor con la debida notificación al responsable del mismo.

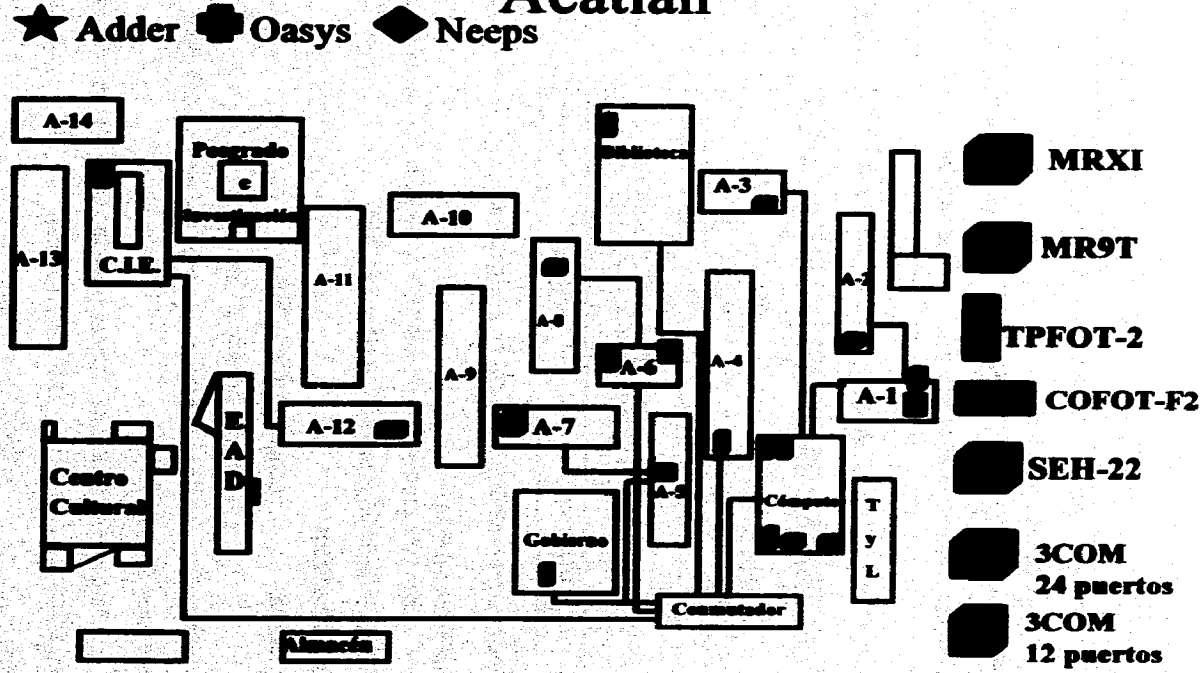
**UBICACIÓN DE LA RED DE LA ENEP ACATLAN.**

La siguiente gráfica muestra un plano conjunto de la ENEP Acatlán en donde se muestra la ubicación de los edificios, los cuales mediante cables de fibra óptica, coaxial y par trenzado están conectados como una red del tipo ethernet. Cada edificio del plantel contiene nodos de red conectados a concentradores de 12 puertos o bien concentradores de 9 puertos según sean las necesidades del edificio al que les dan servicio.

Para el diseño de esta red se contó con el servicio de tres diferentes compañías las cuales se presentan también en la gráfica con diferentes colores para mostrar el trabajo realizado por cada una de ellas. Es importante mencionar

que esta red no estaba segmentada, es decir, que el tráfico que se generaba desde cualquier punto de la red interferia con todos los demás usuarios de la red no importando su ubicación. Por ejemplo si una máquina ubicada en el Centro de Cómputo hacía un requerimiento de información al servidor del DSI (ubicado aprox. a 15m de distancia), este requerimiento viajaba por toda la red del campus y finalmente llegaba al servidor.

# Red de Área Local de la ENEP Acatlán



En materia de cableado se consideró para esta red diversos tipos de cableado tanto para conexiones entre edificios como para las conexiones internas, es decir entre computadoras.

| [illegible] | [illegible] |
|---|---|
| Cable de fibra óptica de 6 hilos de uso rudo, y el algunos casos 8 hilos. | Entre edificios. |
| UTP Unshield Twisted Pair (Cable de par trenzado sin blindaje) Nivel 4 y 5. | Conexiones entre computadoras y concentrador. |

## *Relación de Concentradores de la red en la ENEP Acatlán*

| [illegible] | [illegible] |
|---|---|
| A-1 | HubStack SEH-24<br>TPFOT-2 |
| A-2 C202-3 | MR9T-E 9 |
| A-3 | MR9T-E 9 |
| A-4 | MRXI |
| A-5 | COFOT F2<br>MR-2000C Multiport Repeater |
| A9 C902-1 | HUBSTACK SEHS 22 C.12 puertos TPFOT-2 |
| A-7 | 3com de 24 puertos |
| A9 C906-3 | MR9T-E 8 puertos |
| A-12 | MR9T-E 9 |

## *Descripción de equipos de conectividad*

***HubStack SEH-24:***

Este hub proporciona escalabilidad, pese a ser no inteligente del tipo 10BASE-T tiene 26 puertos (24 RJ45 y 2 EPIMs).

Especificaciones

Distancia: Longitud típica 100m

Longitud máxima 200m

Impedancia: Soporta cable de par trenzado de 75 a 165 ohm.

***HubStack SEH-22:***

Este hub proporciona escalabilidad, pese a ser no inteligente del tipo 10BASE-T tiene 13 puertos (12 RJ45 y 1 EPIM).

Distancia: Longitud típica 100m

Longitud máxima 200m

Impedancia: Soporta cable de par trenzado de 75 a 165 ohm.

***MRXI:***

Este tipo de concentradores vienen con 12 puertos 10BASE-T y dos ranuras, que el usuario puede configurar, para módulos de interfaz de puertos simples opcionales (SPIM). Este tipo de concentradores vienen equipados con diodos emisores de luz que proporcionan un diagnóstico de nivel físico incorporado para la rápida detección de problemas.

| | |
|---|---|
| Tipo de conector: | MRXI:Telco (50 pines) |
| Cables que soporta: | AUI, UTP/STP de fibra óptica. |
| Longitud de cables: | 125m (común) 200m (máximo) |
| Peso: | 3.2Kg |
| Tiempo promedio entre fallas: | 83,133 hr. |

***TPFOT-2:***

Este convertidor permite conectar segmentos de cable de fibra óptica 10BASE-FL/FOIRL, puede soportar distancias de cables hasta de 100 metros.

Especificaciones

| | |
|---|---|
| Tipo de interfaz: | 1 conector RJ45 |
| | 1 conexión 10BASE-FL/FOIRL |
| | (dos conectores físicos ST de fibra) |
| Largo máximo: | fibra 2km |
| | 10BASE-T 100m |

***COFOT F2:***

Este tipo de adaptador permite que los dispositivos en redes de cable coaxial delgado se conecten a redes de fibra óptica, este COFOT tiene capacidad hasta para 100 metros de cable coaxial delgado y hasta un kilómetro de fibra óptica de 50/125 um. El cable coaxial tiene capacidad hasta para 10 nodos.

Especificaciones:

| | |
|---|---|
| Tipo de interfaz: | 10BASE-2 |
| Número de puertos: | 1 |
| Largo máximo de coaxial: | 100m |
| Largo máximo de f.o.: | 1km |
| Tiempo promedio entre fallas: | 539,956 |

***MR9T***

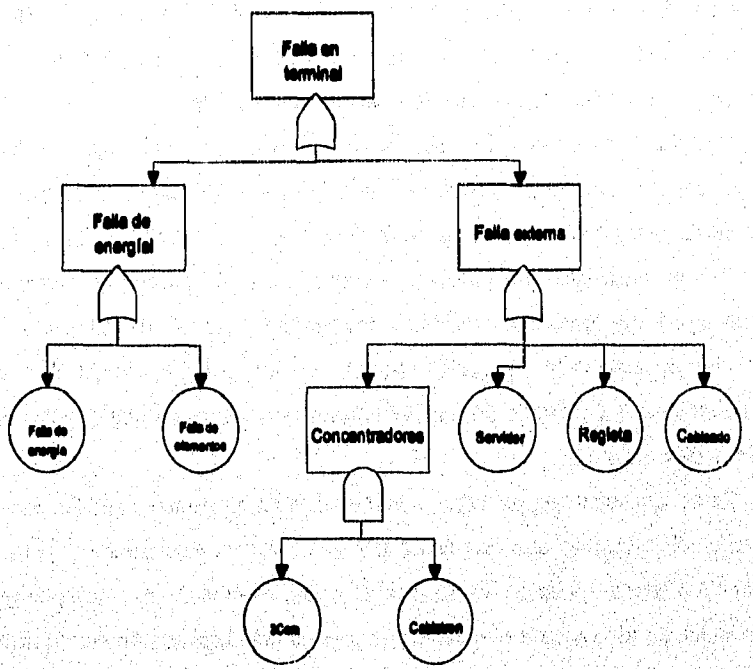
Proporciona 9 puertos RJ45 para conexiones UTP o STP y un módulo de interfaz de puerto Ethernet (EPIM) que el usuario puede configurar.

**Especificaciones.**

| | |
|---|---|
| Tipo de interfaz: | MR9T: 9 RJ45 para conexiones UTP/STP |
| Tiempo promedio entre fallas: | 453,103 hr |

**ARBOL DE FALLA.**

La siguiente gráfica presenta el árbol de falla de un componente de la red tan básico como sería una terminal o estación de trabajo.




***Descripción:***

**Falla en la terminal.**

En el esquema siguiente se advierte la probabilidad de que una máquina falle, lo cual puede ser ocasionado por una *falla de energía* o bien por una *falla externa*. Si se diera la primera falla, es decir, una *falla de energía* la causa más común es un corte en el suministro de energía eléctrica o bien la falla de los elementos que componen el sistema eléctrico que abastece a la computadora como podrían ser en cableado de la electricidad o bien un corto circuito en el mencionado sistema.

Si el problema fuera una falla externa, entonces, la solución del mismo sería, sino más compleja, si menos clara de detectar dados los factores que intervienen en la construcción y operación de la red.

El primer punto a revisar cuando la conexión falle es la verificación de que la tarjeta esté conectada al cable por donde se transmitirán los datos, si este al parecer no presenta problemas, la causa del fallo estaría en la tarjeta y los problemas presentados por éstas se detallan en el capítulo dos.

Otra causa de errores se presenta en los concentradores, cuya principal falla, por absurdo que parezca se debe a que éstos se encuentran sin la debida alimentación de energía eléctrica, es decir, desconectados. Sin embargo es claro que no es la única falla que puede presentar, ya que en base a los estudios realizados con anterioridad se mostró que los tiempos promedio de fallas son de 83,133 horas, que como se puede observar es tan grande que difícilmente sucederían ya que por medio de una sencilla división sabremos que ocurre una falla cada diez años.

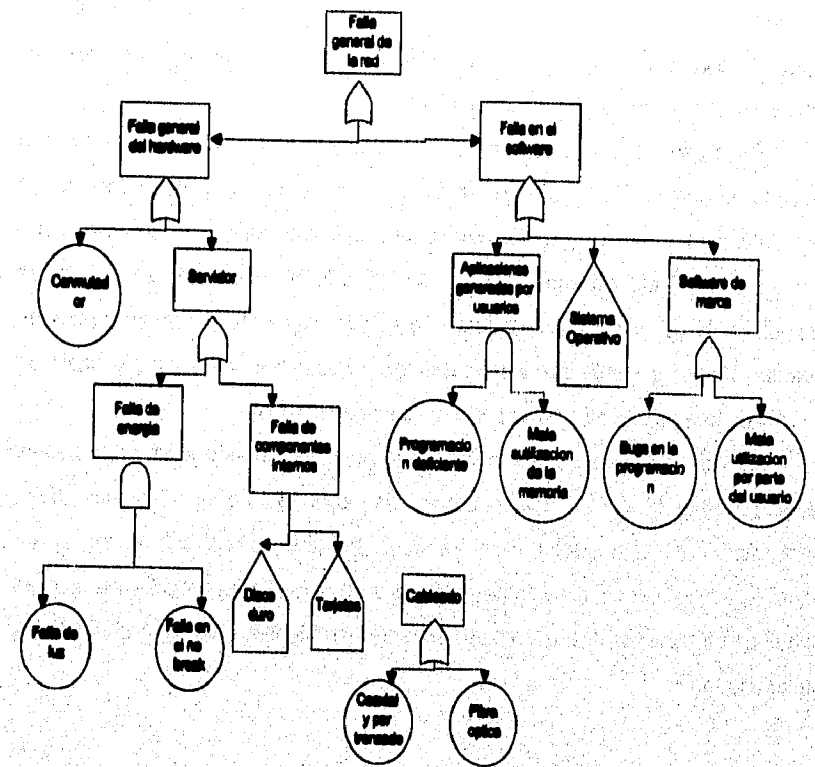
Cabe mencionar que así como ocurren fallas en terminales, también éstas ocurren en el servidor ya que éste no es sino una máquina mas dentro de la red, que puede presentar fallas en su disco duro, vídeo, memoria, etc. y que por ser una máquina donde se realiza un intenso trabajo es más fácil que en ella ocurran en menor tiempo un mayor número de fallas. En la primera parte del capítulo dos se mostraron pruebas con diferentes computadoras corriendo el sistema operativo Netware y cabe hacer mención que existen problemas generados por los controladores de disco que proveen los fabricantes y que no se tienen en Netware. De tal forma que si llegara a fallar el servidor se tendría una falla de manera escalonada ya que al ser este la parte fundamental de la red las estaciones de trabajo quedarían sin conexión alguna y con el severo problema que muchos de los archivos con que se trabajan cotidianamente se encuentran centralizados en el servidor.

Otro punto importante a tratar es la falla en el cableado o bien, en las conexiones del mismo, el cual puede presentar fallas en cuanto a que los

conectores se llenen de polvo y al señal no pueda enviarse de manera confiable, ya que la duración de los cables es de 219,000 horas para los de cobre, variando para cada uno y en relación al recubrimiento.

Poco antes de concluir el presente trabajo el edificio A-5 que cuenta con una red de cable coaxial había presentado una serie de problemas relacionados con colisiones y tráfico que ocacionaba una extrema lentitud al conectarse de otros edificios fuera de ese. Después de un análisis exhaustivo en el cual se verifico cable por cable se descubrio que era un segmento de cable coaxial de aproximadamente 4 mts. que estaba dañado y que al ser sustituido por cable en buen estado reparó al menos en parte la velocidad de la red.

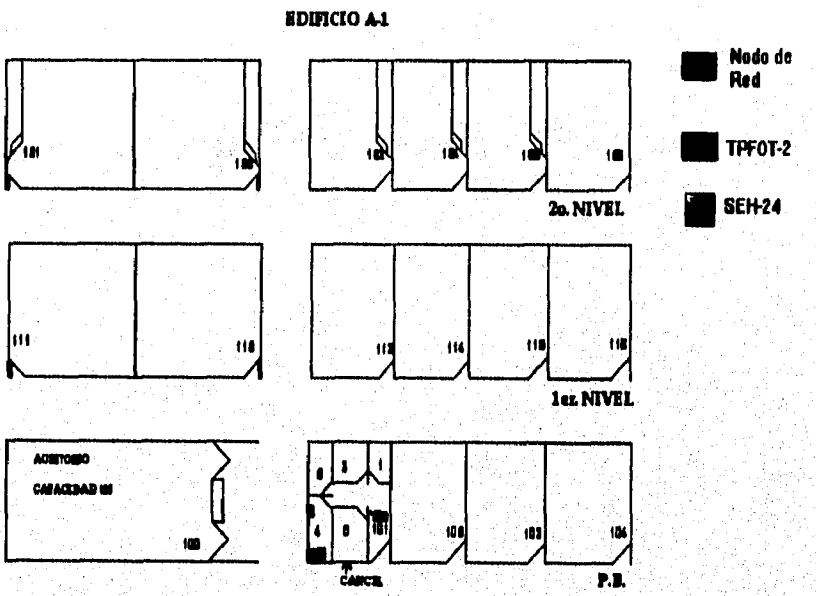
Es claro que después de este pequeño ejemplo cuando existan problemas en las redes se deberá tomar en cuenta todos y cada uno de los elementos que la conforman; pero en especial hacia las redes de cable coaxial que si bien en un principio y aún ahora siguen funcionando bien se deberá tener mucho cuidado en el bus o cable que es el que presenta mayores problemas e incrementa las fallas de toda la red.


Falla general de la red
Falla general del hardware
Falla en el software
Conmutador
Servidor
Aplicaciones generadas por usuarios
Sistema Operativo
Software de marca
Falla de energía
Falla de componentes internos
Programación deficiente
Mala utilización de la memoria
Bugs en la programación
Mala utilización por parte del usuario
Falla de luz
Falla en el no break
Disco duro
Tarjetas
Cableado
Coaxial y par trenzado
Fibra óptica

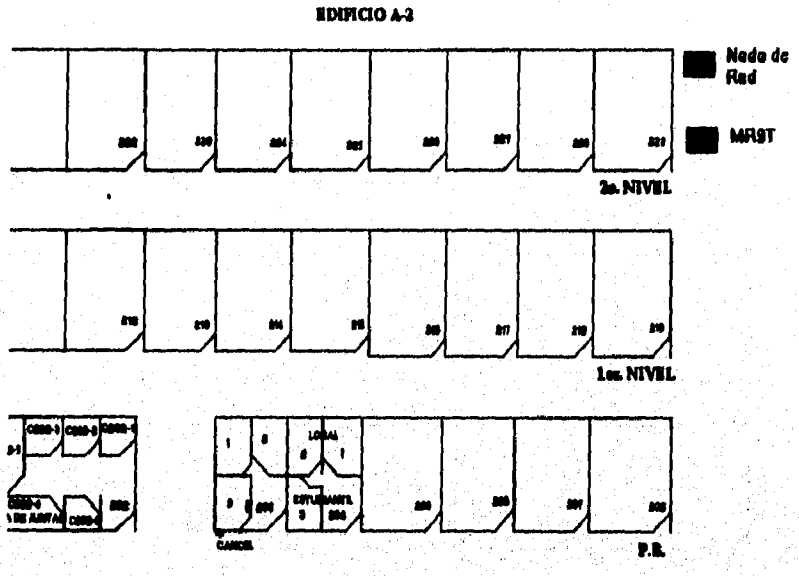
# *DETALLE DE EDIFICIOS.*

A continuación se presenta una descripción gráfica de la red de la escuela, cada edificio tiene diferentes puntos de red en donde se localizan o localizarán computadoras que darán servicio particulares a las divisiones.

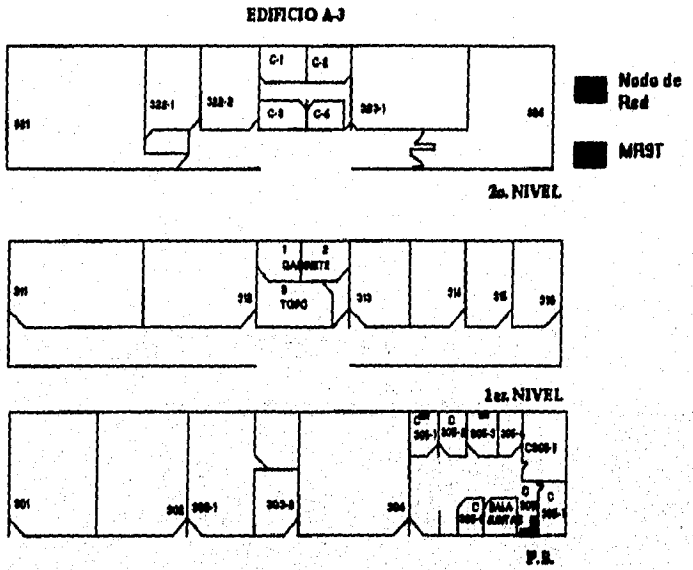
## EDIFICIO A-1



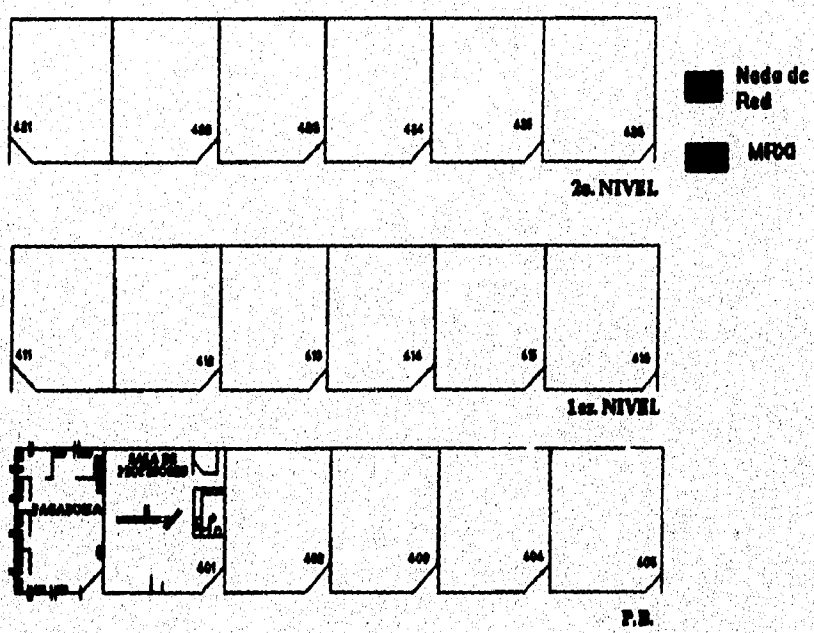
# EDIFICIO A-2



# EDIFICIO A-3

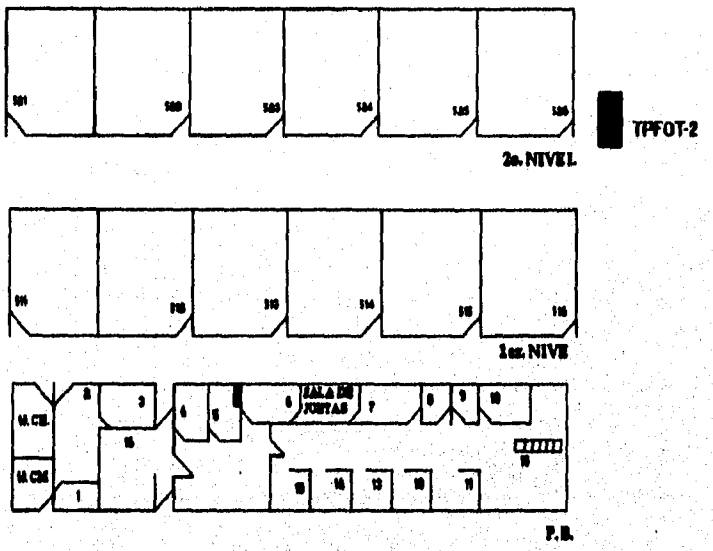



# EDIFICO A-4



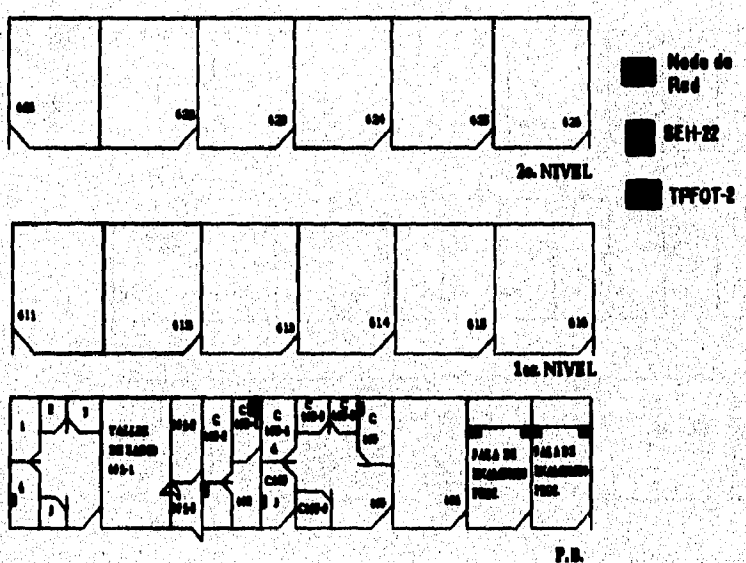
## EDIFICIO A-5

EDIFICIO A-5

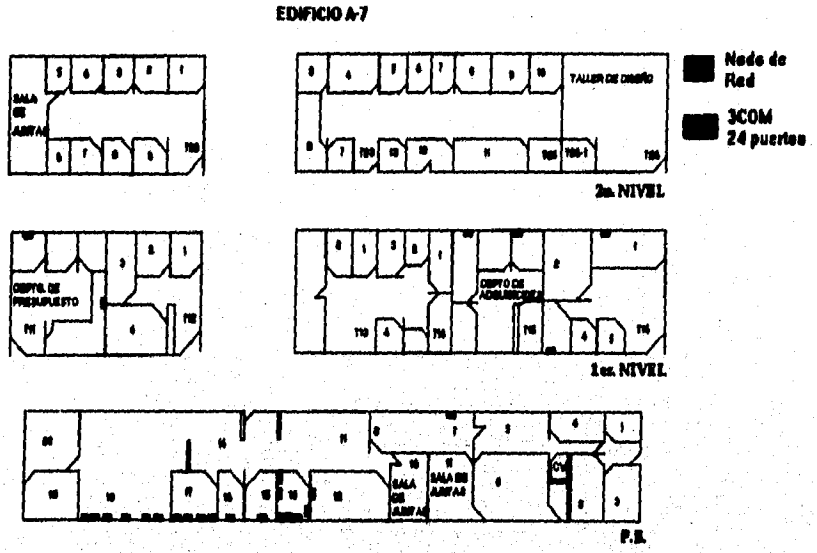



## EDIFICIO A-6

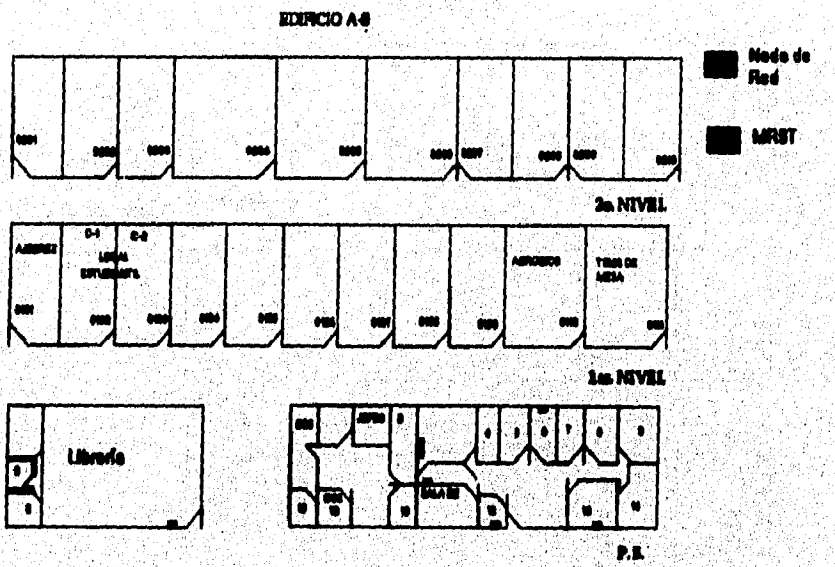
EDIFICIO A-6



# EDIFICIO A-7

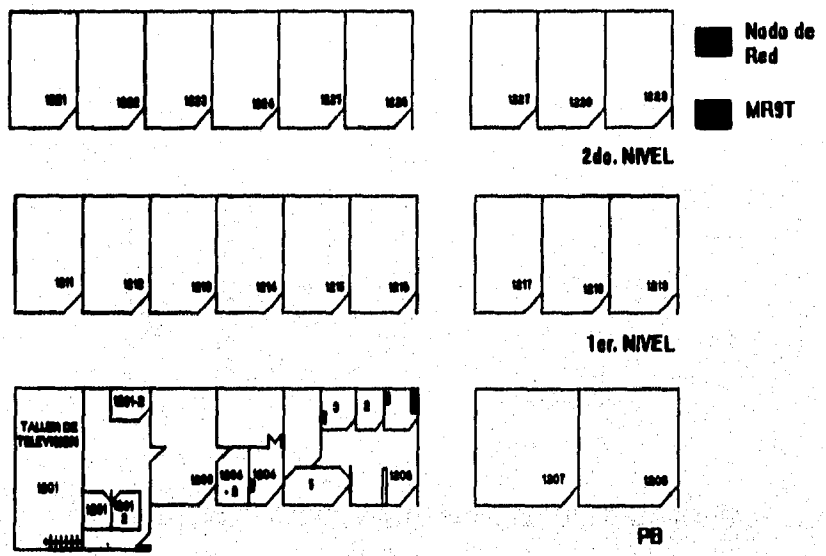



# EDIFICIO A-8

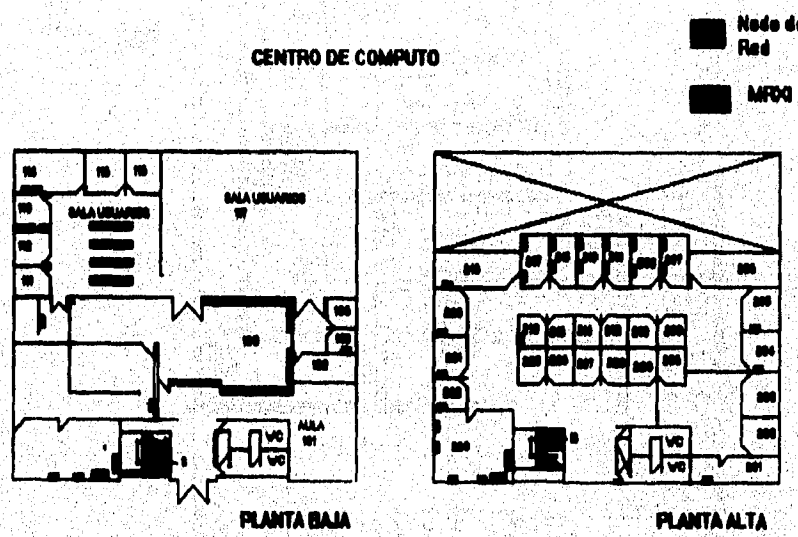


## EDIFICIO A-12

EDIFICIO A-12

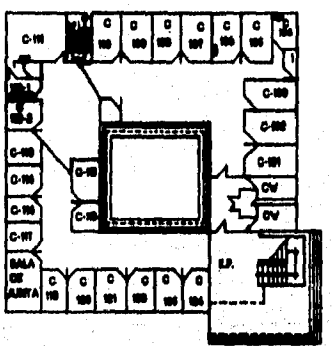



## CENTRO DE COMPUTO

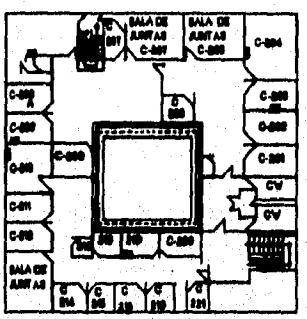


## EDIFICIO DE GOBIERNO

EDIFICIO DE GOBIERNO



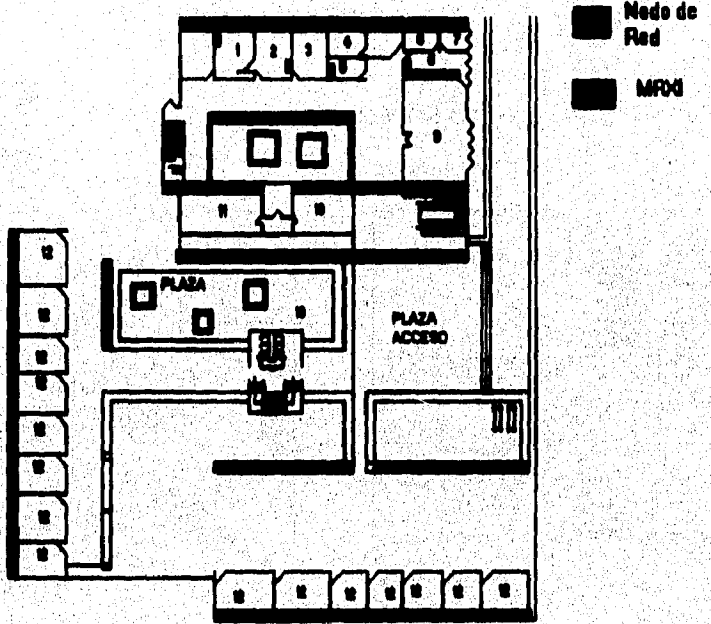
PLANTA BAJA



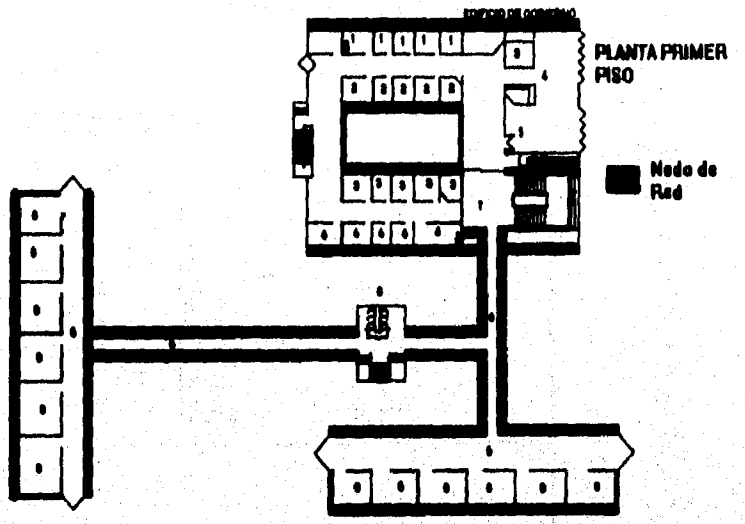

PLANTA ALTA

## CENTRO DE IDIOMAS EXTRANJEROS PLANTA BAJA

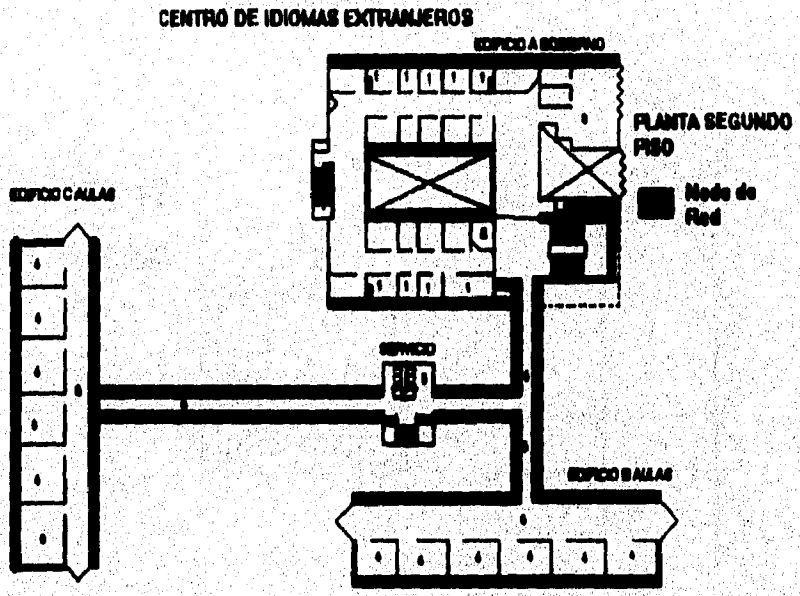
CENTRO DE IDIOMAS EXTRANJEROS



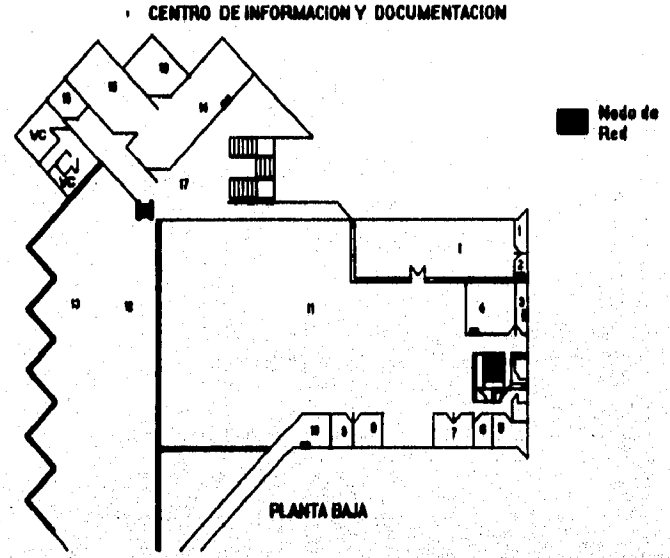
## CENTRO DE IDIOMAS EXTRANJEROS PRIMER PISO



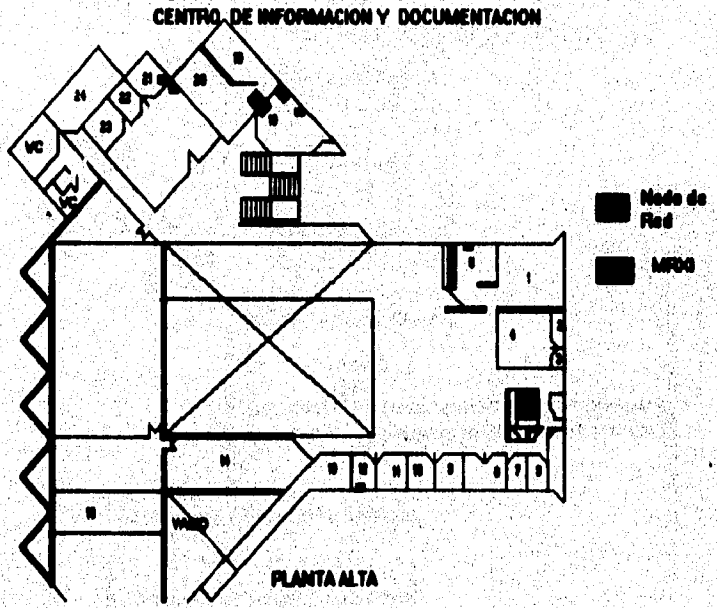

## CENTRO DE IDIOMAS EXTRANJEROS SEGUNDO PISO



## CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN PLANTA BAJA

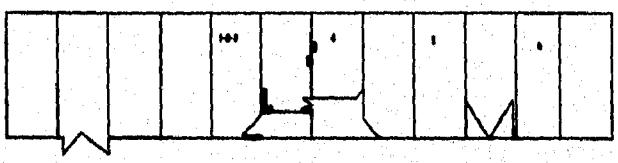



## CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN PLANTA ALTA



## EDIFICIO DE ALMACENES E INVENTARIOS

ALMACENES E INVENTARIOS [redacted] 3COM DE 8 PUERTOS



# PLANES DE EXPANSIÓN.

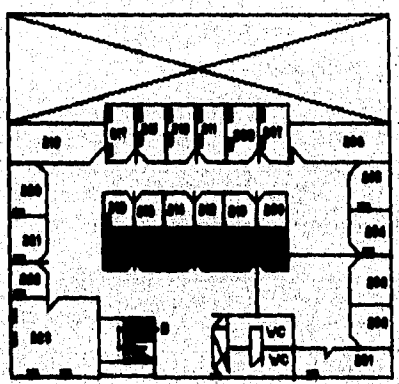
Dentro del plantel se contempla la expansión debido a necesidades de diferentes órganos.y planta acedémica de la escuela.

Se contempla la ampliación de la red en algunos edificios con la utilización de los concentradores ya existentes o en su defecto la adquisición de nuevos materiales de conectividad como podrían ser concentradores, fibra óptica y otros.

En el centro de cómputo se pretende añadir nuevos puntos o nodos de red para la utilización de profesores que tienen asignadas horas de apoyo. A continuación se presentan los cróquis de los edificios a expandir.

Los cubículos marcados en color inverso denotan los lugares donde se proponen nuevos nodos.

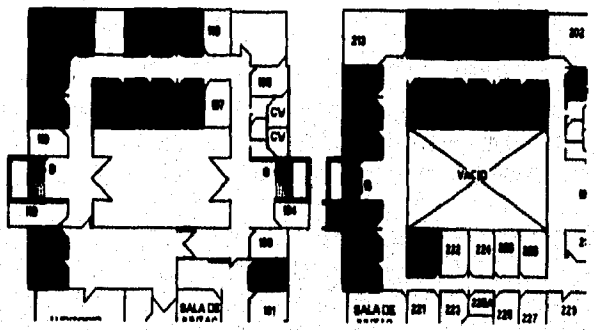
## CENTRO DE CÓMPUTO.



PLANTA ALTA

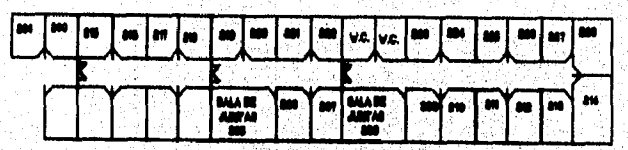
# EDIFICIO DE POSGRADO E INVESTIGACIÓN.

EDIFICIO DE INVESTIGACION

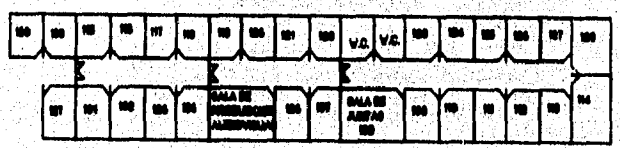


# EDIFICIO A-11.

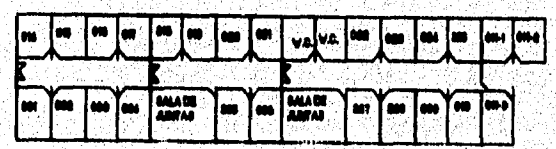
EDIFICIO A-11



2o. NIVEL



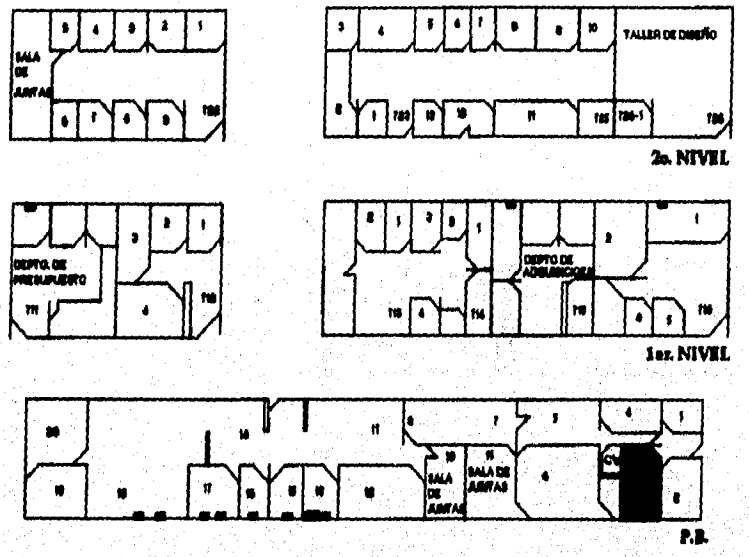
1er. NIVEL



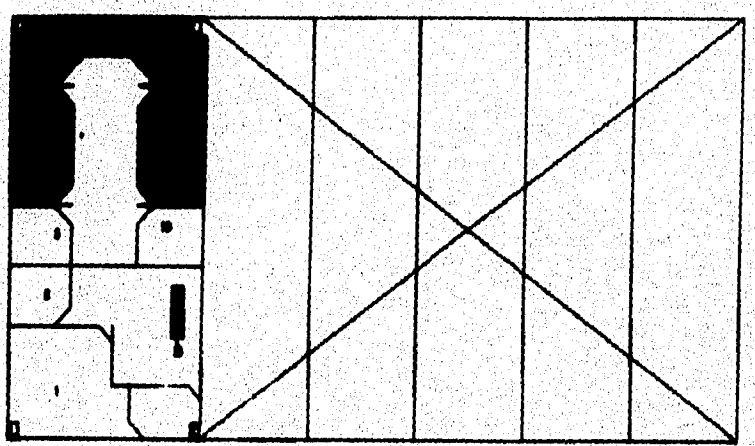
P.B.

## EDIFICIO A-7.

EDIFICIO A-7

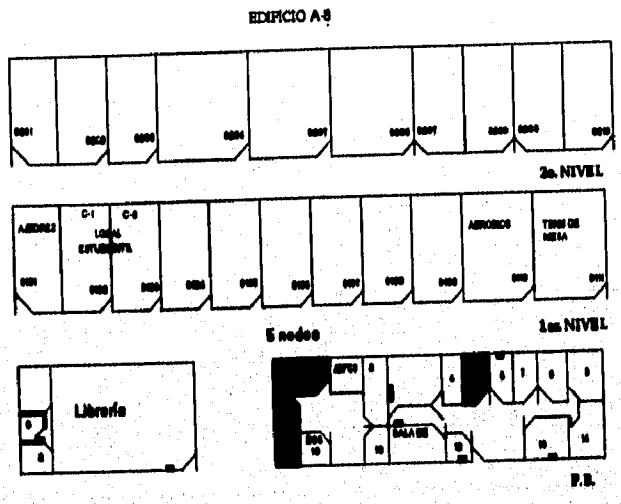



## EDIFICIO DE TALLERES Y LABORATORIOS

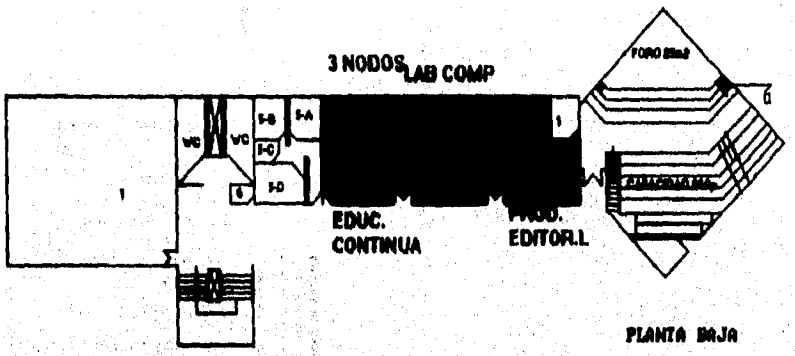


PLANTA ALTA

## EDIFICIO A-8
## 5 NODOS


EDIFICIO A-8
2o. NIVEL
1er NIVEL
5 nodos
Librería
P.B.

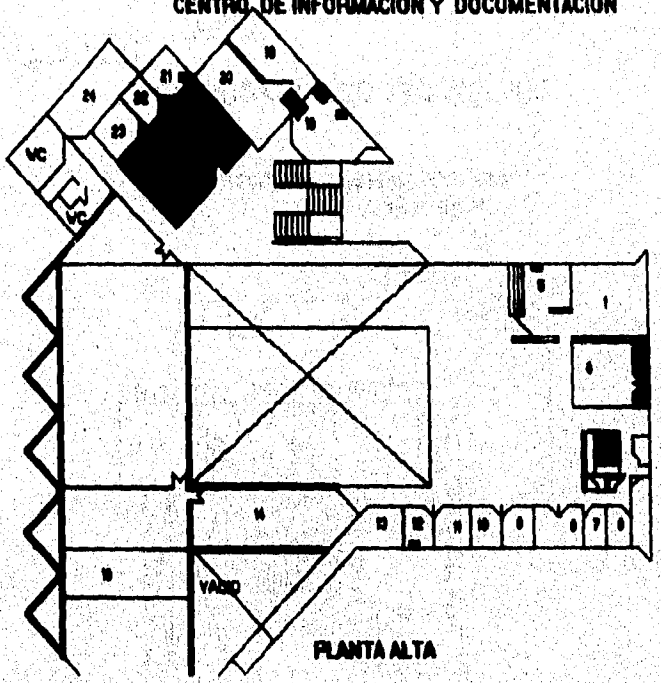
**EDIFICIO DE APOYO A LA DOCENCIA**




PLANTA BAJA

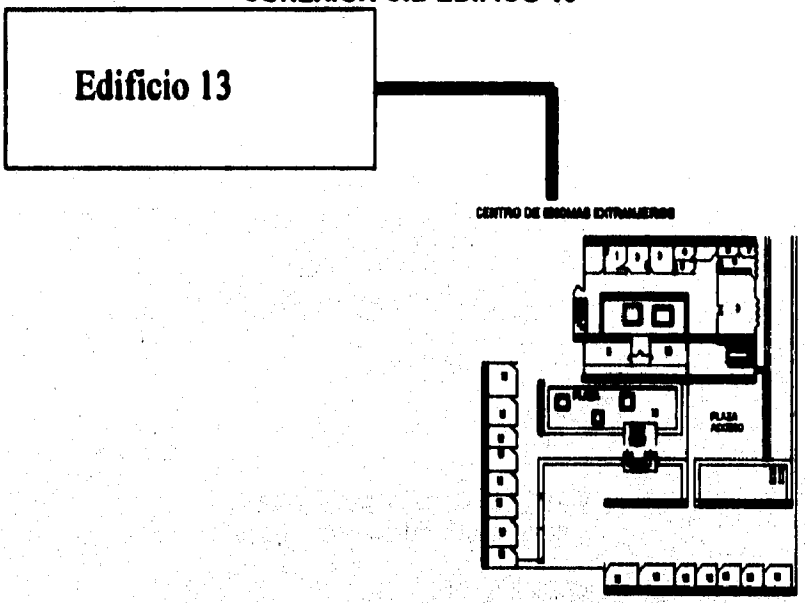
**HEMEROTECA Y MAPOTECA**

**CENTRO DE INFORMACION Y DOCUMENTACION**



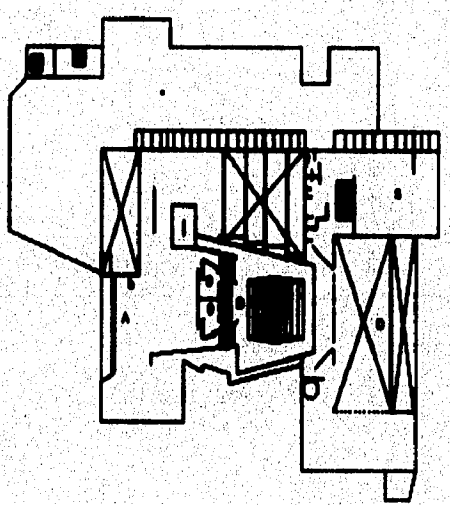

PLANTA ALTA

**CONEXIÓN CIE-EDIFICO 13**



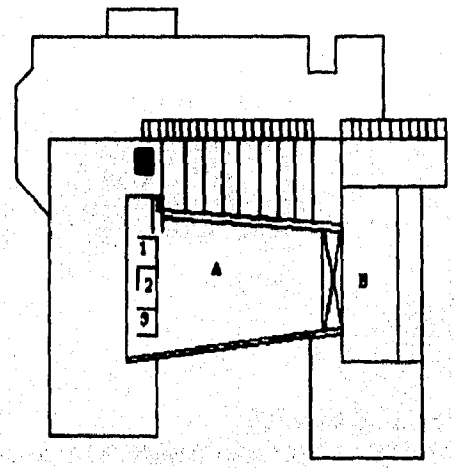

**EDIFICIO DEL CENTRO CULTURAL**

**CENTRO CULTURAL ACATLAN**
**PLANTA BAJA**



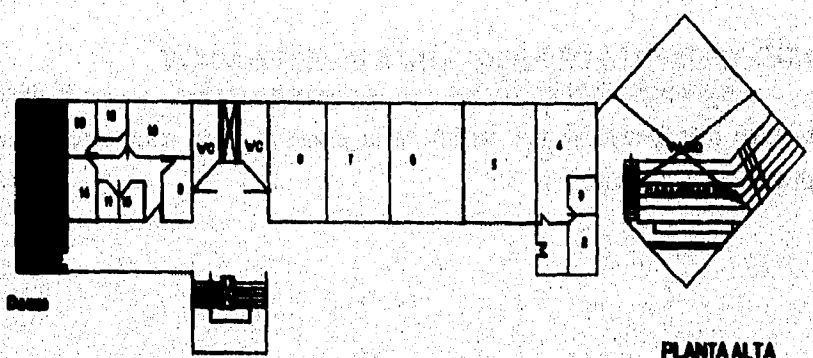
**CENTRO CULTURAL ACATLAN**

**PLANTA ALTA**



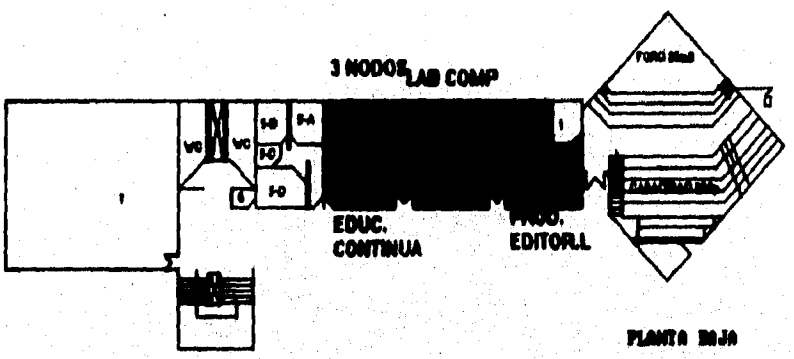

## EDIFICIO DE APOYO A LA DOCENCIA

**EDIFICIO DE APOYO A LA DOCENCIA**



**PLANTA ALTA**

EDIFICIO DE APOYO A LA DOCENCIA




PLANTA BAJA

## NUEVO CENTRO DE CÓMPUTO.

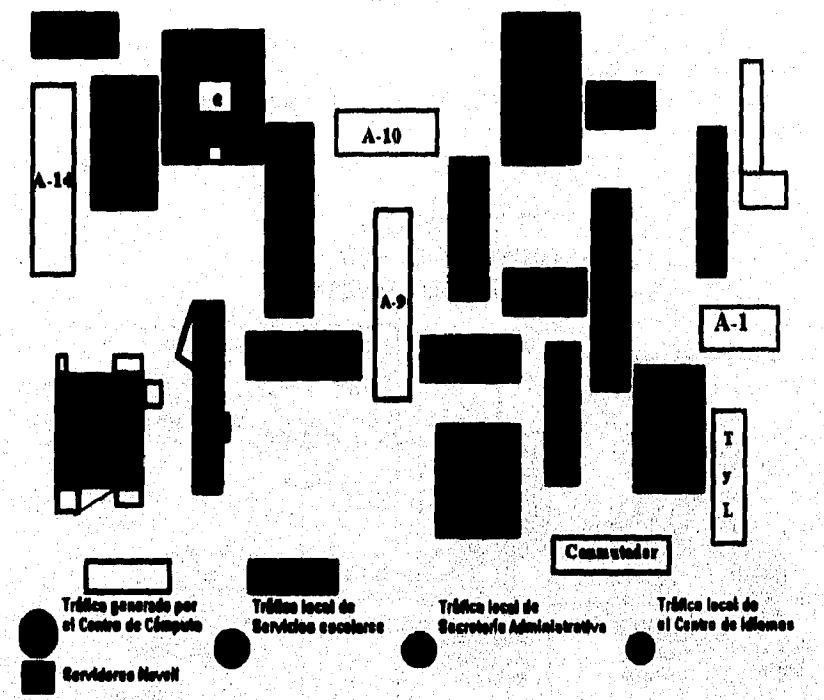
Para el nuevo edificio del Centro de Cómputo se ha propuesto la instalación de cerca de 400 nodos de red que tendrán una interacción de diversos equipos y sistemas operativos que incluyen plataformas como Solaris, Irix, Ultrix, DOS, Windows, Windows NT, etc. y que será objeto de un estudio amplio por parte de los departamentos involucrados en su correcto funcionamiento.

## NUEVO EDIFICIO DE POSGRADO E INVESTIGACIÓN.

Este edificio también contará con opciones de cómputo y vale la pena también mencionarlo ya que tendrá en la planta alta una sala de cómputo dedicada a la investigación.

# FLUJO DE INFORMACIÓN.

Dentro de el plantel se genera un tráfico de red que se describe en la siguiente gráfica los colores muestran el tráfico generado y a que servidor se conectan con regularidad.




En esta gráfica el flujo de información se dirige o está más acentuado en el edificio del Centro de Cómputo ya que este proporciona los servicios de administración de toda la escuela, además de proporcionar servicio a alumnos en redes como Sun, Silicon Graphics y Novell.

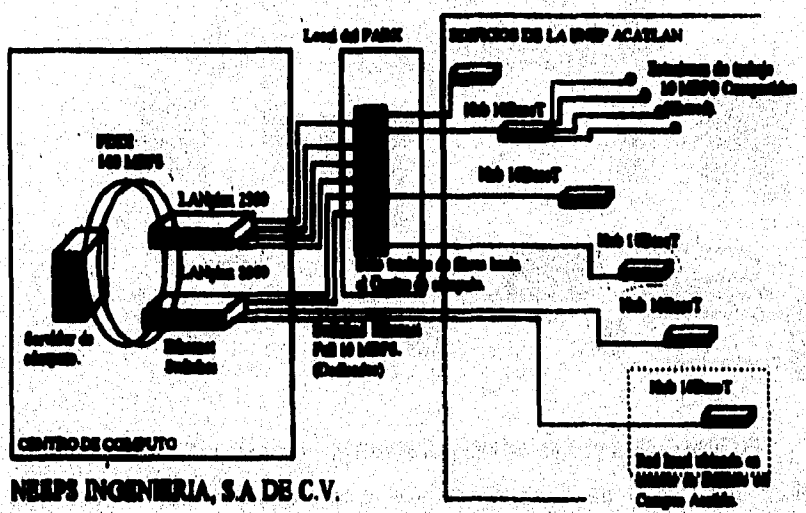
Desde su creación, la red de la escuela ha presentado problemas por el tráfico constante dado el diseño de la red que se explicó con anterioridad. A continuación se presentan los problemas mas frecuentes:

1. Falta de planeación
2. Crecimiento desmedido
3. No existen responsables directos
4. Falta de información
5. Colisiones de datos
6. Caída de conexiones
7. Lentitud excesiva
8. Fallas por falsos contactos o malas conexiones

Siendo estos los problemas, había que buscar una solución para aumentar la confiabilidad de la red.

Lo que se muestra a continuación es la solución que se dará a los problemas:

**ENEP ACATLAN**
**PROYECTO DE RED**
**FDDI / SWITCHED ETHERNET**



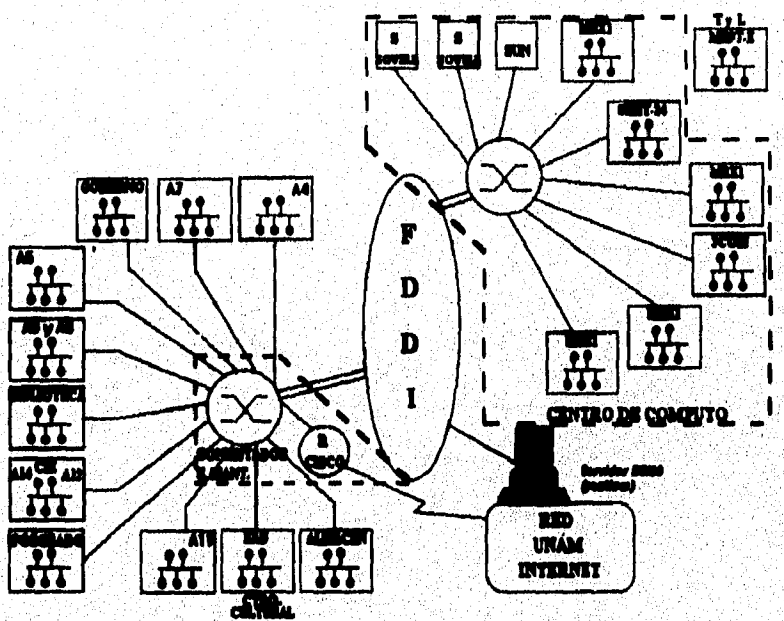

**NEEPS INGENIERIA, S.A DE C.V.**

Este es el proyecto presentado por la compañía Neeps Ingeniería y que utiliza un anillo de fibra óptica de donde se desprenden dos Switches y un servidor, la transmisión se hará en FDDI en el anillo y será la velocidad de 100Mbps y los puertos de los switches serán a 10Mbps dedicados. El servidor que

se utilizará para el DSI es Compaq Proliant, que es Pentium a 100Mhz con un disco duro de 2Gb y una tarjeta FDDI.

Cabe mencionar que en esta solución la propuesta de la compañía Cabletrón es la misma y serán ellos quienes realicen el trabajo, pero también valdría la pena ahondar más en esta solución y considerar tecnologías como ATM y 100 VG; pero eso sería tema para otro estudio.

La siguiente gráfica muestra el trabajo final realizado por Cabletron Systems y que ayudó a que al "switchear" la señal de cada puerto del equipo se consigan 10Mbs dedicados.




En la parte final del trabajo se presentan las conclusiones a las que esta investigación llegó y que representan el fin de un trabajo que seguirá dando muchos más temas de investigación que por supuesto se prevee se realizarán por parte del personal del Centro de Cómputo.

# *CONCLUSIONES*

**Conclusiones:**

La tecnología que se ha venido desarrollando a través de los años permite a la rama computacional el manejo de redes con un alto grado de confiabilidad. Esta confiabilidad se ha comprobando desde el momento en el que se desarrollan todos y cada uno de los componentes que intervienen en la creación tanto de las computadoras como del software que se desarrolle en el entorno de redes.

El firmware permite que el elemento computacional ofrezca al usuario un margen más amplio para el desarrollo de sus aplicaciones sin alterar el desempeño de las terminales.

La introducción de componentes que incluyen la terminología redundante permiten que el usuario se preocupe lo menos posible por la integridad de la información, además de que se realiza una verificación automática de cada uno de los elementos que intervienen en el manejo de la información.

Los elementos que intervendrían en el fallo de una red están considerados en gran medida dentro de las aplicaciones que el usuario desarrolla, como por ejemplo: una mala utilización de las localidades de memoria, un sobreflujo en el manejo de la información, etc.; pero todas estas situaciones se podrían eliminar si se trata de educar computacionalmente a los usuarios.

También podemos observar en la presente investigación que los elementos básicos de una computadora, como lo son el software y el hardware, difícilmente podrán ser un obstáculo para un buen desempeño de las redes.

***TOMAR PRECAUCIONES.***

Aun cuando no hay maneras de garantizar la existencia de un sistema a prueba de errores, al menos uno puede tomar ciertas precauciones. No se debe

trabajar regularmente con versiones de prueba de los programas, y hay que respaldar siempre la información. Una norma más sutil es diseñar el software con la ayuda de gente que comprende la función para lo que será utilizado o bien para lo que podría ser utilizado.

"El misil antimisiles Patriot, elaborado por Raytheon, fue diseñado para actuar en situaciones en las que sería activado no más de 14 horas a la vez. Sin embargo, al calor de la batalla durante la guerra del Golfo Pérsico, el misil fue mantenido en alerta durante cien horas, lo que permitió que un pequeño error en el control de tiempos en el software se incrementara, A resultas de ello, un escud iraquí logró colarse y matar a 28 soldados."[1](sic)

Dentro de INTERNET existe una base de datos que contiene hasta la fecha más de 100,000 casos registrados de errores de software en compañías y que muestran que un programador debe ser humilde y esperar errores, los datos de los de errores de programación mencionado se ubica en el archivo comp.risk. Lo que si es definitivo es que las computadoras hoy en día son cada vez más útiles, pero también la mala utilización de las mismas hace correr más riesgos a las empresas que las ocupan.

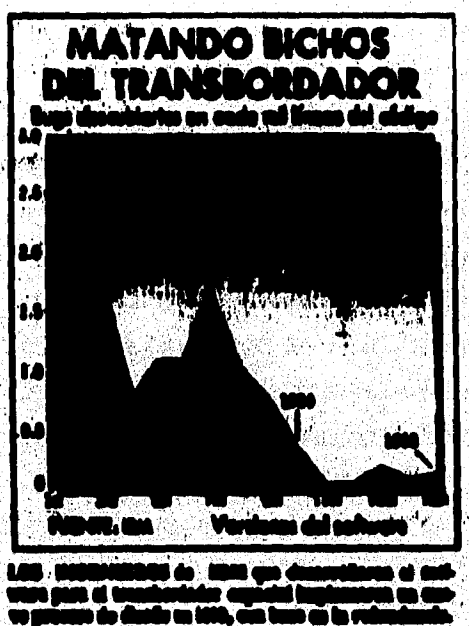
Dado que el software que ocupamos es cada vez más poderoso es también probable que nos confiemos a el, por lo tanto es riesgoso si en el software se logran colar bugs. Es claro que el software domina más la vida cotidiana: en los frenos del automóvil, el tráfico aéreo, etc. de tal manera que la redundancia solo nos libera en forma parcial de ellos.

Dentro de los "errores" que presentan los sistemas computacionales cabe hacer mención que los mas fuertes se presentan en el software y como se mencionó antes, es relativamente fácil reparar una computadora o bien remplazarla, pero cuando el error se encuentra en el software, el trabajo no es tan sencillo.

[1] Tomado de el Excelsior Sección Financiera 25 de abril de 1994 Página 6-F

Mediante pruebas de laboratorio se han desarrollado programas increíblemente confiables. Estas pruebas consisten en probar los sistemas como si se estuvieran trabajando de manera real, además de que, aunque suene redundante se crea software que extrapola lo que sucedería en diez años de trabajo continuo. Es lo más común en estos tiempos que las empresas tengan un departamento dedicado exclusivamente a la confiabilidad del software que manufacturan. Tal es el caso de empresas como SAS Institute, Microsoft, Borland, Lotus, Mcafee, etc..

La siguiente gráfica muestra bugs descubiertos en el software del transbordador espacial:




La gráfica muestra los errores descubiertos en el software del transbordador espacial; en 1990 se trató de generar un nuevo tipo de software basado en la redundancia, éste consiste en generar rutinas del tipo doble que, a pesar de multiplicar los procesos evita que errores ocurran durante su operación, si llegara a fallar el primer proceso, la rutina duplicada llevará a cabo la operación.

El problema en que podría incurrir este tipo de programación es en la generación de miles de líneas de código extra con los conocidos problemas de memoria restringida que tienen las computadoras actualmente, se tendría que evaluar si por hacer el software más rápido tendría que ser menos confiable.

Los análisis llevados a cabo al software de la compañía Borland demostraron que para el caso de la hoja de cálculo Quattro Pro trabajando en un sistema de red de 25 usuarios decremento el rendimiento del producto en un 5% en relación a la hoja de cálculo de la compañía Microsoft llamada Excel que sin embargo mostró alteraciones a la memoria por lo que tuvo que reiniciarse el sistema en más de dos ocasiones.

La comparación anterior trae por consiguiente la comprobación de que el software de Borland para su hoja de cálculo tiene puntos redundantes y por consiguiente más código y en cambio Microsoft mostró un programa mas veloz.

El ejemplo anterior tuvo como finalidad mostrar el ejemplo en una red local, pero, ¿que pasaría si el software del transbordador espacial fallara de la misma manera?, bueno la pregunta quizás saldría sobrando. El transbordador espacial trabaja con un software del que dependen vidas humanas, también los aviones cuentan con software de este tipo, los frenos de los automóviles, los controladores de tráfico aéreo, los conmutadores telefónicos, etc., etc. lo cual nos lleva a pensar que el software redundante ayuda en algo a corregir problemas, pero no siempre. Hay quien atribuye la explosión del transbordador espacial Challenger a una falla en el software, esto no fue debidamente comprobado, pero sin embargo existen casos documentados de que cuando el software ha fallado han ocurrido muertes de seres humanos. Incluso si se elaboran programas perfectamente consistentes, podrían actuar como si las especificaciones básicas no reflejarán a detalle el mundo externo. Uno de los más terribles ejemplos de un error de este tipo es el que registró el Therac-25, una máquina de radioterapia elaborada por Atomic Energy of Canada Ltd.

Para el tratamiento de tumores cancerosos internos, la máquina puede configurarse para emitir rayos X mediante el establecimiento de su rayo de

electrones de alta potencia y la interposición de una tableta de tungsteno entre la fuente de emisión y el paciente. Para tratar lesiones superficiales directamente con electrones, puede remover la tableta y reducir el poder del rayo. Sin embargo, algunas veces cuando los operadores por error seleccionaron el modo de rayos X y corrigieron luego su equivocación mediante instrucciones en un teclado, la máquina fue tomada por sorpresa. Eliminó la tableta intermedia sin reducir la potencia del rayo, sin ofrecer ninguna advertencia de esta posición intermedia.

En consecuencia, el haz de electrones golpeó al paciente con la fuerza de un relámpago. Aunque las funciones de precaución detuvieron el tratamiento después de una fracción de segundo, la medida fue tardía. En 1986, dos pacientes de cáncer en Galveston, Texas, murieron. Otros fueron lastimados en otros centros médicos.

En el caso descrito el error no se debió a un bug en el software, sino a que el modelo contemplado por la computadora no correspondía a la realidad. Nadie había pensado probar la reacción de las máquinas a un cambio súbito de instrucciones. Las funciones de precaución debieron ser accionadas antes que el rayo fuera emitido. Sobre todo, nadie se había preocupado por hacer una máquina fácil de usar, con mensajes de error claros y confiables, y con protocolos de seguridad libres de errores.

Sin embargo, incluso el conocimiento más preciso del uso probable de una máquina no puede evitar una causa más profunda de errores de programación: la sola complejidad de los programas.

Deseamos hacer mención que a lo largo del presente estudio se encontró una fuerte relación entre las dos áreas principales que constituyen la carrera de Matemáticas Aplicadas y Computación demostrando que se puede interactuar y llevar a cabo estudios del estilo presentado aquí, en el que el especialista en sistemas aporta la capacidad del análisis de la parte computacional y el especialista en simulación combina sus conocimientos para lograr los resultados presentados; y gracias a la formación de los primeros semestres para ninguno de

los dos es desconocido el campo ajeno, sin llegar a ser un especialista en los mismos.

En nosotros descubrimos que gracias a la formación que nos dio nuestra carrera pudimos darnos cuenta que en general el profesional de las Matemáticas Aplicadas y Computación puede interactuar con especialistas de otras ramas tan diversas como la sociología, las leyes, los internacionalistas, etc., llevando a cabo tareas interdisciplinarias para construir proyectos que involucran no solo números y computadoras sino seres humanos y que gracias a este tipo de profesiones se puede modelar mejor la realidad.

Aunado a esto, la experiencia profesional que adquirimos a 3 años de haber terminado la licenciatura nos permitió una solidificación de nuestros conocimientos aplicados a la vida cotidiana de la experiencia profesional.

***Francisco Argüelles Arredondo y Raúl Bañuelos Ponce.***

# APÉNDICES

# GLOSARIO DE TÉRMINOS

# A

**ACF:** Siglas de "Advanced Communications Functions". Facilidades de software que,, cuando se agrega a otro sistema de Software, permite la creación y operación de Sistemas de Arquitectura de red entre computadoras IBM.

**AdvanceNet:** Solución de red local de Hewlett Packard, basada en Ethernet.

**Algoritmo:** Una secuencia finita de pasos, dirigidos a realizar una tarea específica, (método de solución).

**Amplificador:** Dispositivo que eleva la potencia de una señal.
Utilizado para prevenir la atenuación (deterioro) de las señales transmitidas.

**Amplitud Modulada:** Método de añadir información a una señal electrónica, donde el peso (amplitud) de la onda se cambia para lograr la información en cuestión.

**Amplitud:** Distancia entre los puntos alto y bajo de una forma de onda o un señal.

**Ancho de banda:** La diferencia entre la frecuencia más alta y la más baja de un canal de transmisión, expresada en Hertz (Hertz=ciclos por segundo). Una medida de la capacidad de información de un canal de transmisión. El ancho de banda varía de acuerdo al tipo y método de transmisión.

**ANSI:** Abreviación de "American National Standard Institute". Una institución voluntaria que ayuda a definir estándares, y que también representa a los E.U. en la Organización Internacional de Estándares (ISO).

**APIs:** Siglas de "Aplication Program Interface". En general, todo el grupo de funciones o procedimientos, que se invocan desde un programa de aplicación para utilizar un software de base. Por ejemplo: APIs para OS/2, APIs para un cierto gateway, etc.

**APPC:** Siglas de "Advaced Program to Program Comunication". APPC es un protocolo "Puerto-a-Puerto", definido por IBM (y ahora también por SAA). No está restringido a micros, ni a equipo IBM. Define un conjunto de verbos (mapeados y básicos para que dos dispositivos puedan lograr una "conversación" en la cual no exista una jerarquía maestro-esclavo. Existen ya diversas implementaciones de APPC para micros. Bajo el léxico IBM, para que un dispositivo sea capaz de "hablar" APPC, debe tener una categoría de unidad lógica 6.2 (LU6.2) por lo que frecuentemente ambos términos son usados como sinónimos.

**Archive Server:** Un servidor (server) enfocado a realizar respaldos. Nombre de un producto de Novell que nunca se liberó, que integra en un equipo dedicado, el software necesario para realizar en forma automática respaldos de uno o más servidores.

**ARCnet Plus:** Propuesta de un nuevo tipo de ARCnet para trabajar a 20 Mbps. Espera ser avalado por IEEE y/o ANSI. Es interoperable con ARCnet de 2.5 Mbps.

**ARCnet:** Abreviación de "Attached Resource Computer NETwork". RED creada por Datapoint. Transmite a 2.5 Mbps. Muy utilizada en el mundo debido a su bajo costo, gran confiabilidad y versatilidad del cableado con topología de estrella.

**ARP:** Siglas de "Address Resolution Protocol". Proceso TCP/IP que mapea el protocolo de Internet direccionado a la dirección física de Ethernet.

**ARPA:** Siglas de "Advanced Research Projects Agency". Agencia dentro del Departamento de Defensa de E.U. que da soporte a la red ARPANET.

**ARPANET:** Una red de área amplia que utiliza protocolos de paquetes diferidos (tipo X.25). La red fue creada por ARPA junto con el Departamento de Defensa de E.U. para dar soporte a las comunidades militares. ARPANET se divide en dos partes interconectadas: Milnet, para uso militar e Internet, para uso comercial y académico.

**ASCII:** Siglas de "American Standard Code for Information Interchange". Forma estándar de codificar los caracteres en un patrón de 7 bits. El ASCII extendido utiliza 8 bits y logra codificar 256 patrones (2^8), en lugar de 128 ( 2^7).

**Asíncrona:** Forma de transmisión que no requiere que el receptor y el transmisor mantengan en "sincronía" sus relojes. Pero en cambio necesita que el receptor lo reconozca. Es más barata que la transmisión síncrona, pero menos eficiente.

**Atenuación:** Reducción de la potencia de una señal eléctrica durante la transmisión. Medida en decibeles. Opuesto a Ganancia. Los decibeles son medidos logaritmicamente.

**AUDIOTEX:** Proceso por medio del cual una base de datos libera información a un sistema de correspondencia, el cual la traduce en un mensaje hablado.

# B

**Back-End:** En general, software o hardware que actúa sin ser visto. En un manejador de Bases de Datos (DBMS) se denomina así a la parte del software,

generalmente ubicada en el Servidor, que se encarga de seleccionar, controlar, ordenar, indexar y administrar la información. Ver Front-End.

**BackBone:** Generalmente se denomina de esta manera a la conexión entre varias redes locales.

**Backup Server:** Un producto, generalmente software, que asegura que al menos las dos últimas versiones de un archivo son almacenados continuamente.

**Balun:** Del inglés "balanced-unbalanced". Dispositivo de tamaño reducido utilizado para poder conectar un medio balanceado (par trenzado) con un medio no balanceado (cable coaxial). Esto no quiere decir que convierta de cable coaxial a UTP, ya que este último posee características adicionales que el Balun no puede proveer.

**Bandwidth:** Ancho de Banda. Segmento de un espectro de frecuencias que pueden utilizarse de manera efectiva para transmitir información. Algunas veces se utiliza para catalogar la cantidad máxima de transferencias de bits por segundo a través de un medio determinado.

**Baseband:** Las redes locales, de acuerdo a su utilización del canal, pueden ser de tipo Baseband o Broadband. En el primer caso, todo el ancho de banda del canal, se utiliza para enviar datos.

**BASIC:** Siglas de "Beginners All-purpose Symbolic Instruction Code". Un lenguaje muy popular para usuario final, utilizado ampliamente en computadoras personales (PCs). Dicho lenguaje fue desarrollado en Dartmounth College en la década de los 60s.

**Batch:** Un método de procesamiento de datos en donde todos los trabajos se agrupan primero para después enviarse, en forma secuencial, a la computadora para su proceso.

**Baudio (baud):** Medida de velocidad de transmisión de datos. La velocidad en baudios es igual al número de veces que cambia la condición de línea por segundo. A velocidades bajas, los baudios y los bits-por-segundo, son lo mismo. Sin embargo, cuando la velocidad aumenta, por cada baudio son codificados varios bits, por lo que dejan de ser sinónimos.

**BIOS:** Siglas de "Basic Input/Output System". Servicios de software y/o firmware que definen la forma en que interactúan las aplicaciones y todos los puertos seriales y paralelos de entrada / salida.

**Bit de paridad:** Método sencillo para detectar errores en la transmisión. Se agrega un bit en 0 ó 1 dependiendo del número de unos que tenga el patrón a enviar. (v.g. si trabajamos paridad par, y en el patrón original existen 3 unos, el bit de paridad irá en 1 para completar un número par).

**Blindaje:** El proceso de proteger un cable con un metal aterrizado, de tal forma que las señales eléctricas no pueden interferir con la transmisión dentro del cable.

**BNC:** Conector utilizado para los cable coaxiales.

**Boot Remoto:** En una red; proceso de encender una estación de trabajo, haciendo el "boot" desde el servidor de la red.

**Boot:** Proceso de carga de los programas básicos para encender la computadora. Bajo el léxico IBM, IPL (Initial Program Load).

**Bootp:** Protocolo que se utiliza para transferencia de información de inicialización (booting), entre un Boot-Server y el dispositivo.

**Bps:** Abreviación de bits por segundo. La medida de velocidad de transmisión más utilizada. En redes locales lo más frecuente es hablar de Mbps (Megabits por segundo). Es importante hacer notar que la abreviación de bit es una b minúscula, mientras que la de Byte es una B mayúscula.

**Bridge:** Dispositivo que permite enviar datos de una red a otra (En español sería "Puente").

**Broadband:** En este tipo de Red Local el ancho de banda se divide en canales de voz, datos y video. Esto se logra a través del manejo de varias frecuencias en un mismo canal.

**Brouter:** Un bridge que puede llevar a cabo funciones de ruteador (yuxtaposición de bridge y router).

**BSC:** Abreviación de Binary Synchronous. Un método arcaico de transmitir datos creado por IBM en 1964.

**Buffer:** Es un espacio en donde se almacenan datos temporalmente mientras se les puede enviar a su destino final.

**Bus:** Es un circuito de transmisión eléctrica que sirve para transportar información entre varios dispositivos de una computadora.

**By Pass:** Significa que rodea al nodo donde se produce una interrupción.

# C

**Cable Coaxial:** Un tipo de cable eléctrico en el cual un alambre sólido de metal es cubierto por un aislante, todo lo cual es protegido por una malla de metal cuyo eje de curvatura coincide con el del alambre, de ahí el nombre de coaxial (eje común).

**Cable Null Modem:** Un cable RS-232C en el cual las señales 2 y 3 están invertidas, haciendo ver a las dos computadoras a las cuales conecta, como si transmitieran a través de modems.

**Cache, Caching:** En computadoras muy rápidas, la memoria cache tiene como objetivo suministrarle los datos al procesador a la velocidad que los solicita (sin retrasos). Para tal efecto, dado que la memoria cache es de menor tamaño que el RAM ordinario, trata de "saber" qué datos son los más usados y tenerlos disponibles para el procesador. (El porcentaje de aciertos se le llama Hit-Ratio). Por similitud, hacer "caching" de disco, es la tarea de tener en RAM los sectores más utilizados de disco, agilizando de esta manera su acceso.

**Canal:** Un camino físico o lógico que permite la transmisión de información. En algunos casos puede ser sinónimo de Bus.

**Carrier:** (Portadora) Una forma de onda continua (normalmente eléctrica) cuyas propiedades le permiten ser modulada o alterada por una segunda señal que "porta" información. La portadora en sí misma no lleva información hasta que es alterada de alguna forma. Estos cambios son los que traen la información.

**CASE:** Siglas de " Computer Aided Software Engineering". La utilización de software para ayudar en la definición, elaboración, designación, documentación y algunas otras áreas del desarrollo de programas.

**CCITT:** Siglas de " Comité Consultivo Internacional de Telegrafía y Telefonía". Fija estándares internacionales en comunicaciones. Se encuentra ubicado en Ginebra, Suiza.

**CMIP:** Siglas de "Common Management Internet Protocol". El protocolo propuesto por OSI, para realizar la administración de redes.

**CMOT:** Siglas de "CMip On Tcp/ip". El camino de compatibilidad entre CMIP (mundo OSI) y la familia de protocolos de TCP/IP.

**Colisión:** El resultado de que dos o más estaciones traten de usar simultáneamente un medio de transmisión (cable) común. Después de una colisión la transmisión se corrompe y hay que reintentarla.

**Compatibilidad:** Estado que permite la transmisión precisa de información desde el origen hasta el destino. (Esto no implica que el destino entenderá la información).

**CompSurf:** Software propietario de Acer que permite hacer particiones en discos duros.

**Compuserve:** Es un servicio público de consulta a bases de datos, que opera con una red de conmutación de paquetes propia.

**Concentrador:** Para fines generales; caja que concentra (de ahí su nombre) segmentos de cable de una red local para su mejor distribución y administración.

**Conectividad:** Estado que permite la transferencia de señales eléctricas desde un origen hasta un destino.

**Conector:** Es un accesorio al final de un alambre o conjunto de alambres que facilitan su conexión a un recurso.

**Correo Electrónico:** Sistema de correo basado en computadoras y enlaces de comunicación. Software para transferencia de mensajes en el cual la información se transfiere desde el origen hasta el destino de una manera eléctrica. Generalmente proveen servicios de soporte que comprenden almacenamiento/control de mensajes y edición de texto.

**COS:** Siglas de "Comission for Open Systems". Comisión de diversos fabricantes de computadoras, cuyo objetivo es agilizar las implementaciones del modelo OSI.

**CPU:** Siglas de "Central Processing Unit". Generalmente se utiliza este término para definir el Procesador Central de una computadora. Es la base de una computadora digital.

**CRC:** Siglas de " Cyclic Redundancy Check". Código de detección de errores. Se basa en realizar una división del patrón a enviar entre un número binario de X bits (polinomio). El residuo de la división lo pega al número. Del lado del receptor se realiza la operación contraria y se verifica si los bits han llegado correctamente.

**CSMA/CD:** Siglas de "Carrier Sense Multiple Access/Collision Detection". Técnica utilizada para enviar señales dentro de una red local. El cable se utiliza por "competencia", y cuando una tarjeta detecta sólo la portadora, empieza a transmitir, pero debe seguir escuchando por si ocurre alguna colisión. De ser así, requiere hacer una retransmisión.

# D

**DACS:** Siglas de "Direct Access and Cross Conect System". Equipo manufacturado por AT & T que permite la interconexión de líneas T1 de transmisión o cualquiera de los canales de 64-kbps por medio de las facilidades T1.

**DAS:** Siglas de "Dual-Attachment Station". Dispositivo utilizado en las redes Token-Ring que permite el acceso a dos sistemas de cableado al mismo tiempo, ofreciendo protección a los cables dañados.

**Data link, Nivel de:** Nivel 2 del modelo OSI. En este nivel se arman los "frames" y se verifican errores de transmisión (usualmente a través de código CRC).

**Datagrama:** Un método de transmisión en el cual las secciones de un mensaje son transmitidas en cualquier orden, y el orden correcto se restablece en la estación que recibe. Paquetes de datos que viajan individualmente, es decir, sin que exista una conexión.

**DB2:** Manejador de bases de datos de IBM para ambientes MVS (mainframes). Utiliza SQL, y define en sí mismo un dialecto estándar.

**DBase:** Informalmente ha sido reconocido como el lenguaje que surge de los productos dBase-III y III-Plus, así como los principales clones: Clipper, QuickSilver, FoxBase y dB-XL. Este lenguaje no es propiedad exclusiva del extinto Ashton-Tate, puede ser utilizado por cualquier fabricante que lo desee.

**DCE:** Siglas de "Data Comunications Equipment". En la terminología común es sinónimo de modem. Más formalmente DCE es el equipo que se coloca entre los dispositivos terminales (DTE) y la red.

**DIA:** Siglas de "Document Interchange Architecture". Es un conjunto de reglas definidas por IBM que regulan el intercambio de documentos en sistemas de automatización de oficinas.
**DIP Switch:** Siglas de "Dual-In Package". Grupo de pequeños switches que normalmente vienen en dispositivos o tarjetas que ayudan a su configuración.

**Dirección:** Un conjunto de números que identifican de manera única "algo". Puede ser una estación de trabajo en una red, una localidad de memoria, un paquete de datos viajando en una red, una tarjeta de red, etc.

**DLM:**
**DMA:** Siglas de "Direct Memory Access". Método por el cual el procesador se "libera" de atender a cada byte que se transmite entre un dispositivo o programa y la memoria, por lo cual la transmisión se hace sin su atención. El procesador solamente interviene para iniciarla o terminarla.

**DNA:** Siglas de "Digital Network Architecture". Arquitectura de comunicaciones de Digital Equipment Corporation (DEC).

**DRDA:** Siglas de "Distributed Relational Database Architecture". Adición a la especificación SAA que permite que los datos sean distribuidos entre bases de datos DB2 y SQL/DS.

**Driver:** Manejador. Es un conjunto de rutinas de software que se utilizan para controlar el intercambio de información entre un dispositivo y el CPU.

**DTE:** Siglas de "Data Terminal Equipment". Las PCs y las estaciones de trabajo son ejemplos de DTEs. Normalmente utilizadas junto con DCEs y líneas de transmisión.

# E

**EBCDIC:** Siglas de "Extended Binary Coded Decimal Interchange Code". Método de IBM para codificar caracteres en una forma binaria.

**ECMA:** Siglas de "European Computer Manufacturers Association". Asociación que se encarga de especificar estándares para la fabricación de equipo de cómputo. Se encuentra ubicada en Ginebra, Suiza.

**E1:** Estándar europeo de transmisión de datos a través de líneas digitales a una velocidad de 2.048 Mbps.

**EIA:** Siglas de "Electronics Industries Association". Institución que elaboró el estándar de comunicaciones RS 232C. Se encuentra ubicada en Washington, USA.

**EMA:** Siglas de "Enterprise Management Architecture". Una arquitectura de manejo de redes propuesta por Digital Equipment basada en el modelo ISO/OSI. EMA permite la interconexión de todos los productos DEC.

**Emulación:** La imitación que hace un dispositivo de otro. Típicamente una PC actuando como terminal de un equipo mayor.

**Encripción:** Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados.

**Enrutamiento Dinámico:** Si una ruta no está disponible o está saturada, se escoge automáticamente otra ruta. Normalmente una red de comunicación de paquetes tiene enrutamiento dinámico.

**Estación de trabajo:** Cualquier equipo conectado a una red, con capacidad propia de proceso.

**Estación remota:** En general, nombre que se les da a las PCs que se conectan a una red local a través de modem.

**Estación sin discos:** Estación de trabajo que no posee disquetes ni discos duros, y por lo tanto, hace un "boot remoto" (Diskless Workstation).

**Ethernet:** El estándar de tarjetas de red más conocido y sólido. Define una velocidad de transmisión de 10 Mbits/seg, utilizando protocolo CSMA/CD.

# F

**FAT:** Siglas de " File Allocation Table". Tabla del sistema operativo, que se encuentra en las primeras pistas de los disquetes y discos duros, cuyo objetivo es llevar la relación de los sectores usados por cada archivo (a través de listas encadenadas).

**FAT Indexing:** Característica del Sistema Operativo Netware V2.1 y mayores, bajo la cual cada vez que se abre cualquiera de los archivos especificados por el supervisor, Netware "carga" a memoria toda la tabla de sectores que le corresponde, agilizando con esto, las búsquedas a los bytes más alejados del inicio del archivo.

**FAX:** Texto o gráficas transmitidas vía líneas de comunicación a un punto remoto donde un original es reproducido. La transmisión puede ser análoga o digital. Existen tarjetas para integrar este servicio a una red local.

**FDDI:** Siglas de "Fiber Distribuided Data Interface". El estándar para transmisión de datos en redes locales utilizando fibra óptica, a una velocidad de 100 mbps. Utiliza un doble anillo en una topología similar a Token-Ring, incluso en la definición del frame. Igualmente utiliza un protocolo de Token-Passing para control de la RED.

**FDM:** Siglas de "Frecuency Division Multiplexing". Bajo esta técnica, el ancho de banda total de un canal, se divide en varias bandas, cada una de ellas capaz de manejar una señal de información. Esto permite que diversos mensajes se envíen simultáneamente sobre el mismo medio de transmisión.

**Fibra Óptica:** Un medio de transmisión de datos que consiste en una fibra de vidrio (o de plástico). Una fuente luminosa (LEDs o Lasers) emite un haz de luz que se va reflejando dentro del cable gracias a los diferentes grados de refracción entre el material de la fibra y una cubierta de un material similar. Aunque el costo de la fibra ha bajado, todavía resulta costoso y complejo el instalar fibra óptica en redes locales. Generalmente se utiliza para construir Back-Bones (conexión entre redes).

**File Server:** Servidor de Archivos. Computadora dedicada a compartir los archivos que tiene almacenados en su(s) disco(s) entre los usuarios de una red local. El File Server puede ser un equipo especial (servers 3Com), una micro (AT386, etc) o incluso en algunos casos una mini (con Lan Manager/X, por ejemplo).

**Firmware:** Conjunto de programas requeridos para implementar una función específica. Estos programas se encuentran almacenados en ROM. (Memoria que sólo permite leer).

**Físico, nivel:** Primer nivel del modelo OSI. Define las características del medio de transmisión (cable en la mayoría de los casos), velocidad, forma de codificar los bits, etc.

**Frame:** Unidad de información del nivel 2 del modelo OSI. Usualmente un frame consta de tres partes: un Header (o encabezado) que trae información de control, direcciones fuente y destino, etc. Un campo de información y un campo de CRC (verificación de errores).

**Frecuencia Modulada:** Proceso en donde se varía la frecuencia de una señal analógica para poder transportar información digital. FM es el método de modulación que más se utiliza en modems diseñados para utilizar líneas telefónicas analógicas.

**Frecuencia:** Número de ciclos por unidad de tiempo. Normalmente medida en Hertz (Hz), que son ciclos por segundo.

**Front-End Processor:** Dispositivo encargado de "lidiar" con todas las comunicaciones, descargando así del trabajo al procesador central (CPU). En IBM se denomina Communication Controller.

**Front-End:** En ambientes de bases de datos, el software que le presenta la información al usuario (reside en la estación de trabajo).

**FTP:** Siglas de "File Transfer Protocol". Un servicio de alto nivel bajo ambiente TCP (Ver TCP/IP) que permite y controla el proceso de transferencia de archivos a través de una red.

**Full Duplex:** Forma de transmisión donde la transferencia de datos puede llevarse a cabo simultáneamente y en ambos sentidos del sistema de comunicación.

# G

**GAN:** Siglas de "Global Area Network". Red que involucra comunicación remota y sin embargo posee una administración centralizada.

**Ganancia:** Incremento en la potencia de una señal, normalmente como resultado de una amplificación.

**Gateway:** Dispositivo que permite conectar dos redes (locales o geográficas) con diferentes protocolos. Un gateway cambia al menos, los protocolos de los primeros 4 niveles del modelo ISO/OSI.

**Gigabyte:** Equivale a 1000 Megabytes. Medida que cada vez es más frecuente encontrar al referirnos a capacidades de almacenamiento secundario.

**GOSIP:** Siglas de "Government OSI Profile". Reglamentación gubernamental americana que promueve la utilización del Modelo OSI, adquiriendo a partir de 1991, sólo equipo y software que se apegue a estos nuevos protocolos.

**Groupware:** Término genérico con el cual se define el software cuyo principal objetivo es automatizar la interacción entre un grupo de personas.

**GUI:** Siglas de "Graphical User Interface". Enlace de comunicación o interfaz entre un usuario y el sistema operativo de una computadora. Generalmente utiliza

pantallas diseñadas con base en iconos (figuras) que representan las funciones disponibles para el usuario. Windows de Microsoft es un ejemplo de un GUI.

# H

**HalfDuplex:** Forma de transmisión en la que ambos extremos del sistema de comunicación pueden transmitir pero no simultáneamente.
**Hamming Código:** Código que utiliza bits redundantes para detectar y evitar los errores de transmisión.

**Handshake:** Procedimiento preliminar, normalmente parte de un protocolo, para establecer una conexión entre dos dispositivos.

**HLDLC:** Siglas de "High Level Data Link Control". Protocolo estándar internacional (Nivel 2 del modelo OSI) para redes X.25.

**Header:** Encabezado. La parte de un mensaje, al inicio, que contiene dirección fuente y destino, número de mensaje y posiblemente otra información.

**Hertz (Hz):** Unidad de frecuencia, equivalente a un ciclo por segundo.

**Hexadecimal:** Sistema numérico en base 16, cuyo conjunto de dígitos, el cual incluye letras, es el siguiente: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Se utiliza para representar combinaciones de 4 bits simplificando de esta manera la representación general de instrucciones máquina o datos.

**HLLAPI:** Siglas de "High Level Link APIs" APIs definidos y estandarizados por IBM para escribir aplicaciones que manejan formato de datos 3270, accesando a un mainframe.

**Hollerit Código:** Método arcaico para codificar información de tal forma que pueda representarse por medio de perforaciones en una tarjeta de 80 columnas. Este código toma su nombre de Herman Hollerit (1860-1929).

**Hub:** Utilizado como sinónimo de repetidor o concentrador (Ver concentrador).

**HUI:** Siglas de "Human Interface". Es cualquier dispositivo que permite al ser humano la interacción con cualquier servicio de red. De acuerdo a la NTT de Japón, HUI se refiere a cualquier conjunto de servicios estandarizados que permite al ser humano interactuar con un sistema integrado complejo.

## I

**ICMP:** Siglas de "Internet Control Message Protocol". El proceso de TCP/IP que provee las funciones necesarias para la administración y control del nivel de red del Modelo OSI.

**IEEE:** Siglas de "Institute of Electrical and Electronic Engineers". Instituto de profesionistas que se encarga de crear, promover y soportar especificaciones y estándares de comunicaciones. El comité 802 del IEEE ha definido diversos estándares para redes locales.

**IEEE-802.1:** Define, entre otras cosas, un algoritmo de enrutamiento de frames denominado Spanning-tree (802.1D)

**IEEE-802.2:** Define dentro del nivel 2 del modelo OSI, las tareas de interacción con el nivel 3 (Llamado Logical Link Control).

**IEEE-802.3:** Basado en Ethernet, define una forma de protocolo basada en CSMA/CD. El estándar 802.3 tiene diversas variantes (cable grueso, delgado, par trenzado y broadband).

**IEEE-802.4:** Define un tipo de red Token-Bus. Similar a ARCnet.

**IEEE-802.5:** Define un tipo de hardware "Token-Ring". Aunque IBM patrocinó gran parte de este comité, en última instancia, el Token-Ring que IBM lanza al mercado es un superconjunto del 802.5.

**IEEE-802.6:** Especificaciones propuestas por el comité IEEE 802 para una red metropolitana (MAN - Metropolitan Area Network).

**IEEE-802.8:** Especificación de FDDI. Interfaz para utilizarse en la conexión de dispositivos a un sistema de transmisión basado en Fibra Óptica utilizando Token-Passing como protocolo de acceso.

**IEEE-802.11:** Estándar propuesto por el comité IEEE 802 para redes locales inalámbricas con línea de vista.

**IMP:** Siglas de "Interface Message Processor". Dispositivo que se utiliza para conectar varias computadoras a la red ARPANET. El IMP provee el control "punto-a-punto" necesario para asegurar la integridad de los datos transferidos en un ambiente heterogéneo.

**Infrarrojo:** Porción del espectro electromagnético más allá del rojo visible. El infrarrojo es utilizado para la transmisión con fibra óptica y algunas comunicaciones al aire libre como en el caso de redes inalámbricas.

**Integridad de Entidad:** Regla por la que cada entidad en un archivo, debe ser reconocida de manera única. Un buen manejador de base de datos (DBMS) debe observar esta regla.

**Integridad Referencial:** Regla por la cual se garantiza que; en el caso de que cualquier dato dentro de una identidad, haga referencia a (sea llave de ) otra entidad en otra tabla, esta última entidad siempre existirá. En resumen, no se permite hacer referencia a un registro que no existe en el otro archivo.

**Integridad:** Característica de la información de reflejar datos congruentes con la realidad.

**Inteleat:** Siglas de "International Telecommunications Satellite Consortium". Organización fundada en 1964 cuyos miembros son naciones interesadas en mantener una red satelital que una a todo el mundo.

**Internet:** Enlace entre redes (internet). También una de las redes más grandes del mundo que concentra actualmente los trabajos de estandarización de la familia de protocolos TCP/IP (IETF).

**Interoperabilidad:** Proceso donde las computadoras pueden operar interactuando con otras a través de una red sin conversión de datos o intervención humana.

**Interrupción:** Acto de detener la ejecución de un programa que estaba corriendo, para que el procesador "atienda" alguna otra tarea. Una interrupción puede tener su origen en el propio hardware (trap) o en software.

**IP:** Siglas de "Internet Protocol". En la familia de TCP/IP, IP es el encargado de definir la mejor ruta y enviar por ella los paquetes, en una comunicación sin

conexión (connectionless). Es decir, IP en sí mismo, no garantiza la recepción correcta de paquetes, ni su ordenamiento correcto.

**IPC:** Siglas de "InterProcess Communication". Un buen sistema operativo de red, multiusuario o multitasking, debe proveer mecanismos para que dos procesos puedan enviarse datos y comandos o simplemente señales de sincronización, a esto se denomina "Comunicación entre Procesos". Ejemplo de formas de IPCs son: semáforos, queues, pipes, memoria compartida, mailslots, etc.

**IPX:** Protocolo "puerto-a-puerto", propio de Novell, que actúa en el nivel 3 del Modelo OSI (Nivel de Red). Entre sus ventajas está el tener direcciones de tres campos: nodo, red y socket, que le permiten tener enlaces entre redes y varios procesos corriendo en diferentes servidores. Está basado en el protocolo de nivel 3 de XNS.

**ISDN:** Siglas de "Integrated Services Digital Network". Red digital de servicios integrados. Estándar que define una línea digital telefónica, con canales para voz y datos.

**ISO:** Siglas de "International Standard Organization". Institución internacional que se encarga de especificar estándares en diversas áreas.

**IVDT:** Siglas de "Integrated Voice and Data Terminal". Es una terminal con bocina integrada y una interfaz de voz. Dicha terminal, generalmente, se encuentra unida a algún canal de comunicaciones.

# J

**J-Bit:** Un bit de transmisión codificada, que no representa datos y se utiliza solamente para el control de la transmisión.

**J-Carrier:** Sistema de transmisión que maneja 12 canales telefónicos que utilizan frecuencias hasta de 140 Kilohertz.

**Jam:** En una red IEEE 802.3 la señal "jam", que generalmente se define basándose en el número mínimo de bytes que deben transmitirse, se utiliza para asegurar que, si se produce una colisión, todos los dispositivos en la red la detectarán.

**JPEG:** Siglas de "Joint Photographic Expert Group". Cuando el acrónimo JPEG se utiliza en relación con video, se refiere a una técnica de comprensión de datos que puede utilizarse, independientemente de si los datos son transmitidos o no.

**Jumper:** Pieza pequeña que permite unir dos patas (pins) de algún conector de hardware. En general, conector que une dos extremos.

# K

**K-Bit:** Un bit de transmisión codificada que representa datos y se utiliza solamente para el control de la transmisión.

**Kermit:** Conjunto de protocolos que fue desarrollado para facilitar la transmisión de archivos. Es popular debido a que lo desarrolló la Universidad de Columbia y se encuentra disponible gratuitamente.

**Kerberos:** Sistema de seguridad desarrollado en MIT el cual otorga autenticidad a los usuarios. No da acceso a servicios o base de datos sino que establece identidad al logon, el cual es utilizado durante una determinada sesión.

**Kernel:** Parte del Sistema Operativo que interactúa directamente con el hardware.

**Kilobit:** Medida que significa mil bits, se representa por la abreviación Kb.

**Kilohertz:** Medida que significa mil hertz, se representa por la abreviación Khz.

# L

**LAN-MAnager/UNIX:** Versión de LAN-Manager desarrollada inicialmente por Hewlett-Packard y SCO para UNIX. En la actualidad existen versiones para diferentes UNIX. La responsabilidad del código original recae ahora de AT & T.

**LAN-Manager:** El sistema operativo para redes locales creado por Microsoft, basado en OS/2. También se denomina LAN-Manager a cierto software de IBM, utilizado para monitorear el estado de una red.

**LAN-Server:** La versión de Microsoft LAN-Manager, muy particular de IBM. Soportará entre otros protocolos, APPC de manera nativa.

**LAN:** Siglas de "Local Area Network". La abreviación más común al hablar de Redes de Area Local.

**LANalyzer:** Analizador de protocolos para Ethernet, fabricado por Excelan (División de Novell).

**Laser:** Siglas de "Ligth Amplification by Stimulated Emission". Entre otras cosas, tecnología utilizada para impresoras de alta calidad.

**Layer:** Palabra inglesa (capa o nivel) con la que se designa cada uno de los estratos del modelo OSI.

**LEN:** Siglas de "Low-Entry Networking". Forma de SNA (Systems Network Architecture) implementada por IBM para integrar computadoras del sistema/3x a redes.

**LLC:** Siglas de "Logical Link Control". Definido por el documento IEEE 802.2. Establece las reglas de comunicación entre el software de nivel 3 del Modelo OSI (Nivel de Red) y la tarjeta de red.

**Locking:** Tarea de controlar la concurrencia mediante el bloqueo de ciertos bytes de información, usualmente de un archivo o registro (file locking o record locking).

**Login:** Acción de entrar a utilizar un host o un servidor de red, establecer una sesión de trabajo y ser reconocido como usuario por el Sistema Operativo.

**LPT:** Lan Performance Test. Herramienta de software, desarrollado por Smart Soft. Inc. para medir en forma relativa, la eficiencia de una red.

**LU 6.2:** Siglas de "Logical Unit 6.2". Ver APPC.

**LU:** Siglas de "logical Unit" (Unidad Lógica) en léxico IBM. En forma sencilla una LU es un "puerto" de software que se establece para llevar a cabo una "sesión"

# M

**MAC:** Siglas de "Medium Access Control". Mecanismo a través del cual los dispositivos conectados a una red local, pueden accesar el medio de transmisión. El MAC combina algunas funciones de los niveles Físico y de Datos del Modelo OSI.

**Mainframe:** Computadora Mayor.

**MAP:** Siglas de "Manufacturing Automation Protocol". Una red local de bus, con protocolo de acceso token-passing, diseñada para ambientes de fábricas, patrocinada por General Motors.

**MASER:** Siglas de "Microwavw Amplification by Stimulated Emission of Radiation". Técnica especial de amplificación de microondas utilizada extensamente en las estaciones satelitales terrestres para amplificar la señal recibida desde el espacio.

**MAU o MSAU:** Siglas de "MultiStation Access Unit". Dispositivo fundamental para el cableado de Token-Ring. Su función es cerrar el anillo entre todos los dispositivos que se le conectan.

**MEN:** Siglas de "Management Event Notofication Protocol". Protocolo de nivel de aplicación del modelo OSI propuesto por DEC para utilizarse en DNA.

**Método de Acceso:** Forma en que la tarjeta de red "accesa" el cable o canal de comunicación. Existen dos variantes importantes: CSMA/CD (Ethernet) y Token-Passing (Token-Ring).

**MHS:** Siglas de "Message Handling System". Un protocolo de nivel de aplicación del Modelo ISO/OSI que especifica la infraestructura para la distribución de datos entre redes. MHS transfiere mensajes en modo store-and-forward. MHS es el equivalente de ISO al X.400 de CCITT.

**MIB:** Siglas de "Management Information Base". Manejador de datos estándar que divide el manejo de información en ocho categorías. La elección de cada una de las categorías es importante ya que los identificadores utilizados para especificar artículos incluyen un código.

**MICE:** Siglas de "Management Information Control and Exchange". Protocolo de nivel de aplicación del Modelo OSI, que utiliza DEC en la fase V de su DNA para implementar funciones de administración de redes.

**Microondas:** Transmisión de ondas de radio en el rango de los Gigahertz. Las microondas se utilizan en gran medida para la transmisión de datos en distancias cortas, desde 35 hasta 65 Km. Este tipo de enlace requiere de línea de vista para su funcionamiento.

**Microsegundo:** Una millonésima de segundo.

**Microsoft:** La empresa más importante de software para microcomputadoras. Creadora entre otros productos de: MS-DOS, Windows, MS-OS/2, Lan Manager, Excel, SQL-Server y Word for Windows.

**MIF:** Siglas de "Minimum Internetworking Funcionality". Definición elaborada por OSI sobre las funciones básicas que un nodo de red local, capaz de conectarse a una red de área ancha, debe proveer.

**Milisegundo:** Una milésima parte de segundo. Se representa por la abreviación ms.

**MNP:** Siglas de "Microcom Networking Protocol". Protocolo, definido por Microcom Inc., para proveer transmisión asíncrona sin errores. MNP tiene una utilización difundida ampliamente entre los modems de las computadoras personales.

**Modem Eliminator:** Pequeño dispositivo que puede reemplazar a un modem si la distancia a cubrir por el enlace es corta. No requiere fuente de poder, toma energía de la propia línea.

**Modem:** Yuxtaposición de Modulador/Demodulador. Dispositivo que convierte señales digitales desde una terminal (o PC) a una señal adecuada para transmitirse en un canal telefónico (analógico). En el otro extremo, otro modem reconvierte la señal analógica en digital, y la transmite a la computadora de ese extremo.

**Modulación:** Proceso por medio del cual la señal de transmisión se modifica para llevar algún tipo de información.

**Monitor:** Hardware o software que recibe información sobre el rendimiento y operación de una red, para su almacenamiento o para toma de decisiones.

**Motherboard:** La tarjeta de circuitos principal en una computadora personal. Regularmente posee diversas ranuras (slots) para agregar tarjetas de memoria, monitor, disco duro, red, modems, mouse, etc.

**MOTIF:** Interfaz gráfica para ambiente Unix, estandarizada por la OSF. Se basa en X/Windows y NewWave.

**MSNF:** Siglas de "Multisystem Networking Facility". Software de comunicación implementado por IBM que permite más de un "host" basado en la arquitectura IBM 5370 controle la configuración y el rendimiento de una red.

**MTBF:** Siglas de "Mean Time Between Failure". (Tiempo Promedio entre Fallas). Medida utilizada por los proveedores, para expresar la confiabilidad de un equipo. Normalmente medido en horas.

**Multiplexar:** Enviar varias señales por un mismo medio, variando en cada una de estas señales, algún parámetro para diferenciarlas de las restantes (por ejemplo la frecuencia). Es posible también, separarlas en el tiempo, lo cual se denomina Multiplexaje por división del tiempo.
**Multitasking:** La capacidad de un sistema operativo, de realizar más de una tarea en forma simultánea. OS/2. por ejemplo, es un sistema que brinda capacidades de multitasking.

**MVS:** Siglas de "Multiple Virtual Storage". Sistema operativo de IBM, el cual optimiza operaciones en línea, tiempo real, multiusuario y multitarea.

**MAC:** Siglas de " Medium Access Control ". Mecanismo a través del cual los dispositivos conectados a una red local, pueden acceder el medio de transmisión. El MAC combina algunos funciones de los niveles Físico y de Datos del Modelo OSI.

**MAINFRAME:** Computadora mayor.

**MAP:** Siglas de " Manufacturing Automation Protocol ", una red local de bus, con protocolo de acceso token-passing, diseñada para ambientes de fabrica, patrocinada por General Motors.

**MASER:** Siglas de " Microwave Amplification by Stimulated Emission of Radiation ". Técnica especial de amplificación de microondas utilizada extensamente en las estaciones satelitales terrestres para amplificar la señal recibida desde el espacio.

**MAU o MSAU:** Siglas de " MultiStation Access Unit ". Dispositivo fundamental para el cableado de Token-Ring. Su función es cerrar el anillo entre todos los dispositivos que se conectan.

**MEN:** Siglas " Management Event Notification Protocol ". Protocolo del nivel de aplicación del modelo OSI propuesto por DEC para utilizarse en DNA.

**METODO DE ACCESO:** Forma en que la tarjeta de red " accesa " al cable o canal de comunicación. Existen dos variantes importantes : CSMA / CD ( Ethernet ) y Token-Passing ( Token-Ring).

**MHS:** Siglas de " Message Handling System " . Protocolo del nivel de aplicación del Modelo ISO /OSI que especifica la infraestructura para la distribución de los datos entre redes. MHS transfiere mensajes en modo store-and-forward. MHS es el equivalente de ISO al X.400 de CCITT.

**MIB:** Siglas " Management Information Base ". Manejador de datos estándar que divide el manejo de información en ocho categorías. La elección de cada una de las categorías es importante ya que los identificadores utilizados para especificar artículos incluyen un código.

**MICE:** Siglas " Management Information Control and Exchange ". Protocolo del nivel de aplicación del modelo OSI, que utiliza DEC en la fase V de su DNA para implementar funciones de administración de redes.

**MICROONDAS:** Transmisión de ondas de radio en el rango de los Gigahertz. Las microondas se utilizan en gran medida para la transmisión de datos en distancias cortas, desde 35 hasta 65 km. Este tipo de enlace requiere de línea de vista para su funcionamiento.

**MICROSEGUNDO:** Una millonésima de segundo.

**MICROSOFT:** La empresa más importante de software para microcomputadoras. Creadora entre otra da otros productos: MS-DOS, WINDOWS, MS-OS/2, LAN Manager, EXCEL, SQL-Server, y WORD for WINDOWS.

**MIF:** Siglas de " Minimum Internetworking Funcionality " Definición elaborada por OSI sobre las funciones básicas que un nodo de red local, capaz de conectarse a una red de área ancha , debe proveer.

**MILISEGUNDO:** Una milésima parte de un segundo. Se presenta por la abreviación ms.

**MNP:** Siglas de " Microcom Networking Protocol ". Protocolo, definido por Microcom Inc., para proveer transmisión asincrona sin errores. MNP tiene la utilización difundida ampliamente entre los modems de las computadoras personales.

**MODEM ELIMINATOR:** Pequeño dispositivo que puede reemplazar a un modem si la distancia a cubrir por el enlace es corta. No requiere fuente de poder toma energía de la propia línea.

**MODEM:** Yuxtaposición de Modulador/ Demodulador. Dispositivo que convierte señales digitales desde una terminal ( o PC ) a una señal adecuada para transmitirse en un canal telefónico (analógico). En el otro extremo, otro modem

reconvierte la señal analógica en digital, y la transmite a la computadora en ese extremo.

**MODULACIÓN:** Proceso por medio del cual l señal de transmisión se modifica para llevar algún tipo de información.

**MONITOR:** Hardware o Software que recibe información sobre el rendimiento y operación de una red. para su almacenamiento o toma de decisiones.

**MOTHERBOARD:** La tarjeta de circuitos principal en una computadora personal. Regularmente posee diversas ranuras ( slots ) para agregar tarjetas de memoria, monitor, disco duro, red, modems, mouse, etc.

**MOTIF:** Interfase gráfica para ambiente UNIX estandarizada por la OSF. Se basa en X / WINDOWS y NewWave.

**MSNF:** Siglas de " Multisystem Networking Facility " . Software de comunicación implementado por IBM que permite que más de un "host" basado en la arquitectura IBM 5370 controle la configuración y rendimiento de una red.

**MTBF:** Siglas de " Mean Time Between Failure ". ( Tiempo promedio entre fallas). Medida utilizada por los proveedores para expresar la confiabilidad de un equipo. Normalmente medido en horas.

**MULTIPLEXAR:** Enviar varias señales por un mismo medio variando en cada una de estas señales, algún parámetro para diferenciarlas de las restantes ( por ejemplo la frecuencia). Es posible también, separarlas en el tiempo, lo cual se denomina multiplexaje por división de tiempo.

**MULTITASKING:** La capacidad de un sistema operativo, de realizar más de una tarea en forma simultánea. OS/2, por ejemplo, es un sistema operativo que brinda capacidades de multitasking.

**MVS:** Siglas de " Multiple Virtual Storage ". Sistema operativo de IBM, el cual optimiza operaciones en linea, tiempo real, multiusuario y multitarea.

# N

**NAMED PIPES:** Mecanismo nativo de LAN Manager, para brindar comunicación entre procesos ( IPC ) entre diversos nodos, facilitando el procesamiento distribuido.

**NANOSEGUNDO:** Milmillonésima de segundo. Para su representación se utiliza la nomenclatura ns.

**NAS:** Siglas de " Netware Aplication Support ". Ambiente definido por DEC para proveer integración de servicios en el nivel de aplicación utilizando servicios e interfaces estándares en la industria.

**NCP:** Siglas de " Netware Control Program ". Termino de SNA programa que conmuta las conexiones de circuitos virtuales y opera SDLC. Normalmente es residente en los controladores de comunicaciones o procesadores.

**NET/ONE:** Grupo de productos de red de Ungermann - Bass .

**NETBIOS:** Interfaz estándar (hasta hoy ) Para comunicar dos estaciones de trabajo en una red local Definido por IBM y Sytek en 1984 - 1985 . Dentro del

contesto MS-DOS son los servicio de software y firmware que implementan la interfaz entre las aplicaciones y la tarjeta de red.

**NETVIEW:** Producto de software desarrollado por IBM que permite controlar redes complejas como aquellas que se forman utilizando SNA y redes locales. NetView solamente puede operar con productos de red definidos por IBM.

**NETWARE:** Sistema operativo de red, desarrollado por Novell Inc. Tiene diversas versiones ( Netware - Lite, V2.2, V3.11)

**NETWORTH:** El equivalente canadiense a la red mundial BITNET. NETWORTH conecta universidades y otras universidades de enseñanza superior.

**NeXT:** Computadora de alta tecnología diseñada por la compañía del mismo nombre. Esta compañía se encuentra bajo la dirección de Steve Jobs quien fuera el principal arquitecto de Apple.

**NEWWAVE:** Producto desarrollado por HP que corre entre DOS y WINDOWS. Integra datos y activa tareas dentro del sistema.

**NFS:** Siglas de " Network File System " Sistemas distribuidos de archivos, para poder accesar desde un equipo X, los archivos de otro equipo Y. Creado por Sun Microsystems.

**NIST:** Siglas de " National Institute of Standard and Technology " Agencia del gobierno U.S.A. que controla la operación del U.S.A. Nacional Bureau of Standard.

**NODO:** Este termino se utiliza generalmente para referirse a una estación de trabajo dentro de una red. Punto computacional dentro de una red de comunicaciones.

**NOVELL:** Uno de los principales fabricantes de productos para redes locales. Desde 1988 se ha enfocado preponderantemente al mercado de sistemas operativos, desligándose casi totalmente del hardware para redes de área local. ( estaciones de trabajo, servers, etc.)

**NSFNET:** Siglas de " National Science Fundation Network ". La NSFNET conecta en la actualidad varias universidades y opera a velocidad de T1 ( 1.544 Mbps)

# O

**OCR:** Siglas de " Optical Character Recognition ". Proceso a través del cuál los caracteres de texto pueden ser reconocidos y traducidos a caracteres computacionales tales como el código ASCIII.

**OFFLINE:** Estado de un recurso en el cual no se encuentra disponible para la computadora. Las funciones de un recurso offline no pueden estar bajo el control de la unidad central de procesos.

**OPENVIEW:** Arquitectura para administración de red desarrollada y utilizada por HP.

**OS/2:** Sistema operativo desarrollado por IBM - Microsoft para la línea de computadoras personales PS/2 (Personal System /2 )

**OSF:** Siglas de " Open Software Fundation ". Organización de proveedores de soluciones para UNIX, encargadas de estandarizar este mercado.

**OSI/NM:** Siglas de " OSI Network Managment ". La propuesta de ISO para servicios de administración de redes. El software de administración de redes normalmente permite el control monitoreo y la modificación de todas las funciones de red.

**OSI:** Siglas de "Open System Interconnect ". Estructura lógica y estándar de siete niveles de protocolos definida por ISO para facilitar la comunicación en ambientes heterogéneos.

**OTF:** Siglas de " Open Token Fundation ". Grupo de fabricantes de Token - Ring, enfocado a estandarizar Token-Ring, tratando de presionar a IBM a seguir sus propios estándares ( aún a pesar de la competencia)

# P

**PACKET SWITCHING:** Método de transmisión de datos bajo el cual, un canal solo es ocupado durante el momento de transmisión del paquete. La conmutación de paquetes (así se llama en español envía los diferentes paquetes provenientes de diversas conversaciones, a través de la mejor ruta.

**PAD:** Siglas de " Packet Assembler Disassemble ". Dispositivo utilizado para conectar objetos no-X.25 a dispositivos X.25 (usualmente terminales o computadoras asíncronas hacia X.25) Su función es tomar la información de un extremo, armar paquetes y "meterlos" a la red X.25 y "desarmarlos" para pasarlos al otro extremo.

**PAQUETE:** Unidad de información de los protocolos de nivel tres del modelo OSI. Tiene una estructura similar a la del "frame ", excepto en que un paquete, la dirección destino es la red del puente más cercano.

**PARALELA INTERFAZ:** La interfase entre un recurso, como una computadora o terminal y los canales de transmisión multiple necesarios para soportar transmisiones paralelas.

**PDN:** Siglas de " Public Data Network ". Termino Internacional con el que se define a las redes publicas que operan utilizando conmutación de paquetes.

**PDU:** Siglas de " Protocol Data Unit". Forma en la que deben aparecer los datos definidos por un protocolo.

**PEER- TO - PEER:** Una comunicación Peer- to - Peer ( puerto a puerto ) se establece cuando las dos computadoras pueden iniciar una conversación y no requiere de " permiso" de la otra.

**PERFORMANCE:** Entiendase por performance al rendimiento o desempeño que tiene un equipo, es decir a la capacidad de procesar información ó bien a realizar las tareas asignadas con mayor eficiencia.

**PIGGYBACKING:** Técnica que se utiliza en los niveles de transporte y datos, que permiten insertar información de verificación en frames recibidos del destino y para que sean transmitidos simultáneamente.

**PIPELINING:** Técnica que se utiliza en los niveles de transporte y datos del modelo OSI , para permitir la transmisión de frames múltiples sin tener que esperar para verificar si son recibidos individualmente. Estos frames serán verificados en orden posteriormente.

**POLLING:** Literalmente encuestamiento. Bajo esta técnica, un dispositivo atiende a varios a través de ir " revisando" cada uno de ellos, y verificar si tiene algo que recibir o transmitir.

**POSIX:** Siglas de " Portable Operating System Interface, UNIX ". Propuesta de una interfaz universal para UNIX , de tal manera que los programas de aplicación puedan correr en cualquier equipo, mejorando así la interoperabilidad de sistemas.

**PRESENTACIÓN, NIVEL DE:** El nivel 6 dentro del modelo OSI. Sus funciones principales son realizar labores de "transformación" de la información: Conversión de formatos ( v.g. de ASCIII a EBCDIC), encripción y/o compresión.

**PRESENTATION MANAGER:** Migración al ambiente Windows que se tiene en MS-DOS, pero ahora bajo OS/2. Al igual que en Windows, su objetivo es lograr una interfaz gráfica muy amigable y poderosa.

**PRINT SERVER:** Equipo (puede ser una PC ) enfocado a atender las colas de espera para las impresoras conectadas a él. Un print server es útil cuando deseamos compartir impresoras diferentes de aquellas que están conectadas al servidor de la red.

**PROM:** Siglas de " Programable Read - Only Memory " . Tipo de memoria en la cual se puede escribir y leer, pero no pueden hacerse modificaciones subsecuentes.

**PROPIETARIO:** En el ambiente de redes y comunicaciones, lo contrario a estándar. Un protocolo propietario -por ejemplo- es aquél definido por una empresa y usado solo por esa empresa.

**PROTOCOLO:** Conjunto de reglas convencionales, utilizado para comunicar dos dispositivos de la misma naturaleza.

**PSDN:** Siglas de "Packet- Switched Data Network". Red en la que los datos son transmitidos y ruteados en agrupamientos específicos llamados paquetes. Las especificaciones X.25 del CCITT definen el formato y los procedimientos para las Redes Públicas de Paquetes Conmutados mas importantes en operación.

**PU:** En léxico IBM, unidad física (siglas de "Physical Unit"). Se denota con este término a los dispositivos físicos de una red SNA.

**PULSO:** Un cambio de energía de un estado a otro de corta duración.

# Q

**Q-bit:** Bit calificador en un paquete X.25 que el DTE utiliza para indicar que quiere transmitir datos a más de un nivel.

**Q-bus:** Estructura de interconexión interna de la familia de computadoras VAX de Digital Equipment Corporation (DEC).

**QLLC:** Siglas de "Qualified Logical Link Control". Protocolo de control para el nivel de datos del modelo OSI que permite que los sistemas SNA operar sobre redes de paquetes conmutados CCITT X.25.

**Queue:** Literalmente, cola de espera. Normalmente referida a las colas de espera de la impresora.

# R

**Radio Frecuencia:** Cualquier radiación electromagnética coherente. La mínima frecuencia de dicha radiación es aproximadamente 15 Kilohertz.

**RAM:** Siglas de "Random Access Memory". Memoria que puede ser escrita y leída de manera dinámica. Puede ser accesada por el usuario en cualquier punto con facilidad y sin tener que leer grabaciones anteriores.

**RARP:** Siglas de "Reverse Address Resolution Protocol". Protocolo que descubre una dirección desconocida y otorga una dirección conocida y un servidor RARP para proveer una respuesta.

**Red, Nivel de:** El tercer nivel del modelo OSI. Su función es cambiar las referencias de nombres de nodos, a direcciones de los mismos, y definir la ruta a tomar.

**Red Local:** Conjunto de computadoras, enlazadas por algún medio de comunicación, y en distancias relativamente cercanas (dentro de un mismo edificio o campus). También conocida como LAN (Local Area Network).

**Redirector:** Conjunto de servicios de software de alto nivel, que rutea peticiones de programas de usuario hacia recursos tales como: archivos, impresoras y programas a través de una red.

**Reflectómetro:** Herramienta utilizada para verificar problemas en el cableado. Un deflectómetro envía un pulso eléctrico al cable y espera por su reflexión. En un buen cable no hay reflexiones, que significa que no hay cortes o cortos.

**Relay:** Dispositivo que posee un magneto controlado eléctricamente, cuyo campo magnético permite que se abran o cierren interruptores eléctricos.

**Repetidor:** Dispositivo que retransmite y amplifica la señal recibida. Actúa solo en el nivel I del modelo OSI.

**RFC:** Siglas de "Request for Comment". Procedimiento usado por la comunidad Internet para intercambiar ideas y establecer estándares y especificaciones.

**RIP:** Siglas de "Routing Information Protocolo". Protocolo de TCP/IP utilizado para controlar el intercambio de información entre hosts y gateways..

**RIT:** Siglas de "Rate of Information Transfer". Cantidad de información transferida por unidad de tiempo desde una parte de un sistema hacia otra parte del mismo.
**RJE:** Siglas de "Remote Job Entry". Operación computacional que permite a un trabajo ser ejecutado desde un punto remoto y enviar los resultados a ese mismo punto.

**ROM:** Siglas de "Read Only Memory". Memoria no volátil que puede ser leída pero no modificada.

**RPC:** Siglas de "Remote Procedure Call" El proceso utilizado en ambientes UNIX con TCP/IP para implementar un proceso específico en un nodo local o remoto.

**RS-232C:** Interfaz para conectar un DTE a un DCE. La especificación técnica ha sido publicada por la EIA. Tradicionalmente usa 25 pines (o patas).

**RTAM:** Siglas de "Remote Telecomunications Access Method". Método de acceso utilizado por dispositivos periféricos para accesar recursos de programas en un sistema que no es IBM/SNA.

**Ruido:** Señales eléctricas que distorsionan una transmisión, introduciendo errores. El ruido puede provenir de cables de corriente, motores eléctricos, etc.

**Ruteador:** Dispositivo que toma un paquete (Nivel 3 del modelo OSI) y lo envía del punto A al punto B, después de analizar cual es el camino óptimo para llegar a su destino. Esto se logra gracias a la información que cada ruteador almacena sobre todos los nodos de la red.

**RVI:** Siglas de "Reverse Interrupt Character". Señal de control que un receptor envía a un transmisor mientras recibe datos, solicitando que la transmisión se detenga para que el receptor pueda transmitir un mensaje de mayor prioridad.

# S

**S/F:** Store and Forward. Servicio de transmisión donde los mensajes son recibidos en un punto intermedio en la red y después retransmitidos a otro punto en la red.

**SAA:** Siglas de "Systems Application Architecture". Grupo de estándares definido por IBM, enfocado a lograr que las aplicaciones que se desarrollen en un cierto tipo de equipo (micro, mini o mainframe) puedan ser transportadas a otros ambientes sin ningún cambio importante a nivel programación.

**SAG:** Siglas de "SQL Access Group". Grupo de fabricantes de DBMS's que tiene por objetivo crear un estándar de SQL que permita tener datos distribuidos de distintas plataformas.

**SASE:** Siglas de "Special Application Service Element". SASE se refiere a un conjunto de servicios especiales establecidos por los estratos de aplicación de

OSI. Dichos servicios son definidos por los usuarios e incluyen formatos convencionales y diálogos de operación.

**Satélite:** Dispositivo de recepción y transmisión que se encuentra orbitando la Tierra (en órbita geoestacionaria) utilizado para enviar señales sobre grandes distancias.

**SDH:** Siglas de "Synchronous Digital Hierarchy". El equivalente de CCITT del servicio de transmisión de SONET (Synchronous Optical Network).

**SDLC:** Siglas de "Synchronous Data Link Control" Protocolo de nivel 2 del modelo OSI, estándar en la arquitectura SNA de IBM. Se utiliza principalmente para transmisiones punto a punto.

**SDU:** Siglas de "Service Data Unit". Conjunto de datos definido (mensajes) que va del cliente de un servicio a otro cliente.

**Secuenciamiento:** Proceso de dividir un mensaje de datos, en piezas más pequeñas, para su transmisión.

**Serial Interfaz:** Interfaz electrónica ente un dispositivo receptor o transmisor y un canal de transmisión simple.

**Servidor:** Dispositivo de hardware o rutina de software que provee uno o mas servicios predefinidos a una población de entidades usuarias, tales como nodos en una red.

**Sesión nivel de:** Nivel 5 del modelo OSI. Su función es establecer la conexión entre los dos extremos de la conversación.

**Sesión:** En terminología IBM, la plática entre dos Logical Units (Lus), se denomina sesión.

**Síncrona Transmisión:** Forma de transmisión en la que ambos extremos deben tener un mismo pulso de reloj, y con base en éste, ambos extremos conocen en que momento se puede transmitir. Aunque en la transmisión síncrona no se necesitan bits de inicio y final para cada caracter, el hardware requerido para sincronizar los pulsos de reloj, la hace más cara que la asíncrona.

**SLIP:** Siglas de "Serial Line Protocol". Protocolo que controla el proceso de transferir paquetes de TCP/IP a través de una línea serial.

**SMI:** Siglas de "Structure of Management Information". Conjunto de reglas o formatos para definir, accesar y agregar objetos al MIB Internet.

**SMTP:** Siglas de "Simple Mail Transfer Protocol". Protocolo que se utiliza en ambientes UNIX para transferencias de correo electrónico a través de una red.

**SNA:** Siglas de "System Network Architecture". La arquitectura de protocolos para redes creada por IBM.

**SNADS:** SNA Distribution Services. Conjunto de servicios de SNA que permite el envío diferido de información a su destino final. Es la base de diversos productos de automatización de oficinas.

**SNIFFER:** El analizador de redes locales mas versátil del mercado, creado por Network General. Existe también una versión que integra servicios de inteligencia artificial para detección de problemas, conocido como Expert Sniffer.

**SNMP:** Siglas de "Simple Network Management Protocol". Protocolo estándar de la familia TCP/IP, enfocado al manejo, administración y control de redes que utilicen TCP/IP.

**SPOOL:** Siglas de "Simultaneous Peripheral Operations On Line". Comúnmente, el software encargado de controlar las colas de espera en una impresora. Utilería del sistema operativo.

**SPX:** Siglas de "Sequenced Packet Exchange". Protocolo propio de Netware para el nivel 4 del modelo OSI. Apoya a IPX brindándole servicios de secuenciamiento de paquetes y garantía de llegada.

**SQL-Base:** Servidor de bases de datos creado por Gupta Technologies. El primero que surgió en el mercado (1986).

**SQL-Server:** Servidor de bases de datos desarrollado por Microsoft y Sybase (hasta 1989 fue comercializado por Ashton-Tate). Se liberó al mercado apenas en mayo de 1989. Posee características sumamente poderosas en manejo de transacciones, integridad de la información y control de concurrencia.

**SQL-Windows:** Front-End muy poderoso desarrollado por GUPTA Technologies es una herramienta tipo 4GL, para generar programas bajo Windows, que accesan algún motor SQL.

**SQL:** Siglas de "Structured Query Language". El lenguaje de consulta y acceso a bases de datos más común en la actualidad. Definido como estándar por IBM, ANSI e ISO.

**Starlan:** Red local creada por AT&T. Transmite a 1 Mbps, aunque tiene una variante de 10 Mbps. Utiliza cable telefónico. Sus frames son muy similares a Ethernet.

**STP:** Siglas de "Shielded Twisted Pair", Cable de par trenzado de alambre con protección eléctrica adicional, enrollado alrededor del conductor, normalmente en hoja de aluminio. Corresponde al tipo 2 de IBM.

# T

**T-1, Línea:** Sistema de transmisión digital desarrollado por AT&T, capaz de transmitir información a 1.544 Mbps. Existen otras definiciones como T-2, T-3 y T-4 en donde varían los anchos de banda.

**T-conector:** Conector de cable coaxial, que permite se le conecten dos segmentos diferentes de cable coaxial. Tiene forma de T, de ahí su nombre.

**TAP:** Conexión eléctrica que permite que las señales sean transmitidas desde y hacia un bus. La liga entre el bus y el cable AUI (drop cable) que conecta a una estación de trabajo con el bus. Utilizados en Ethernet, también llamados "vampiros" o MAUa (no confundir con MAU de Token Ring).

**TCP/IP:** Juego de protocolos creados en los 70's por Vince Cerf, profesor de Stanford, por encargo del Pentágono. El objetivo era lograr protocolos independientes del hardware. Hoy en día, son los protocolos que permiten la mayor conectividad entre los más diversos equipos (desde una MAC hasta una Cray)

**TCP:** Transmission Control Protocol, nivel 4 de la familia TCP/IP, TCP es un protocolo orientado a conexiones, que garantiza la llegada de paquetes y su ordenamiento.

**TDR:** Siglas de "Time Domain Reflectometer". Véase Reflectómetro.

**TELENET.** Red privada, disponible comercialmente, que provee servicios de paquetes conmutados y circuitos conmutados a sus abonados en Norte América, Europa y Asia.

**Teleproceso:** Sistemas que convinan comunicaciones y proceso de datos de tal forma que permiten ejecutar los procesos computacionales en una localidad distinta del punto de entrada o del punto de salida de información.

**TELNET:** Servicio de terminal virtual especificado por el Depto. de Defensa de E.U. e implementado en la mayoría de versiones UNIX.

**Terminador:** Componente que se coloca al extremo de un cable coaxial, y que consiste en una resistencia de la misma cantidad de ohms que la impedancia característica del cable.

**TFTP:** Siglas de "Trivial File Trandfer Protocol". Protocolo de transferencia de archivos basados en UNIX. TFTP en una simplificación de SFTP.

**Token-Passing:** Una de las dos técnicas básicas de acceso de una red local. Bajo Token-Passing, para que una tarjeta de red empiece a transmitir, debe recibir primero el token. Dicho token es un patrón específico de bits.

**Token-Ring:** Red Local diseñada por IBM. Está creada para conectar diferentes tamaños de equipos. Se basa en que el token pueda circular de nodo en nodo, a través de un anillo. Para enlazar los equipos e ir cerrando el anillo.

**TOP:** Siglas de "Technical Office Protocol". Arquitectura de siete niveles, que utiliza especificaciones de ISO y CCITT en cada uno de los niveles, diseñada para automatización de oficinas. Se encuentra bajo control del grupo de usuarios de MAP/TOP.

**Topología:** Descripción de las conexiones físicas de una red. Generalmente se conoce con este nombre la forma en que se dispone el cable de una red local.

**TOPS:** Sistema operativo utilizado por los sistemas DECSYSTEM-10 y DECSYSTEM-20 de Digital Equipment Corporation. Estas computadoras ya se encuentran descontinuadas pero existen varias todavía en uso.

**Transceiver:** En redes IEEE 802.3 es un dispositivo a través del cual podemos conectar la tarjeta de red al cable de transmisión. Se usa también para designar cualquier dispositivo que transmite y recibe.

**Transductor:** Dispositivo que convierte las propiedades físicas de una señal de un tipo de energía a otro. Un ejemplo es la interfaz entre una computadora (señales basadas en electrones) y un medio de transmisión de fibra óptica (señales basadas en fotones).

**Transporte, Nivel de:** El cuarto nivel del modelo OSI. Sus principales funciones son secuenciar paquetes, y verificar que han llegado todos.

**Twisted-Pair:** Cable que se forma de dos alambres aislados, que se tuercen entre sí. Existen dos variantes básicas: blindado y sin blindar. El blindado permite mayores distancias y es mucho mas inmune al ruido. El no blindado (o UTP) es más económico, pero tiene limitantes de distancia y ruido. En los E.U. ha tenido mucha difusión en los últimos meses, debido en primera instancia a que el costo

de mano de obra para instalar cable es sumamente elevado, y se trata de aprovechar el cableado telefónico que ya existe.

**TYMNET:** Red de paquetes conmutados instalada en E.U. Europa, y otras partes del mundo. British Telecom se encarga de la administración de esta red.

# U

**UDP:** Siglas de "User Datagram Protocol". Formato de paquete que se encuentra definido dentro de TCP/IP, cuya función es la transmisión de mensajes cortos, ya sea de un usuario o de control. La transmisión de UDP no genera mensajes de confirmación de recepción por parte del receptor.

**UHF:** Siglas de "Ultra High Frecuency". Frecuencias de transmisión en el rango de 300 a 3000 Mhz.

**ULTRIX:** Versión del sistema operativo UNIX desarrollada por DEC. ULTRIX se apega a los estándares actuales y funciona sobre plataformas VAX.

**UNIBUS:** La estructura interna de comunicación entre dispositivos de las computadoras DEC de la familia PDP-11.

**UNIX:** Sistema Operativo multiusuario, desarrollado por AT&T. Es considerado muy flexible, poderoso y altamente portable. Corre en muchas plataformas de minis y en algunas micros y mainframes.

**UPS:** Siglas de "Uninterruptable Power Supply". Fuente de poder alterna que nos sirve de respaldo para que cuando se presente una falla de energía, no se suspenda el suministro en los dispositivos que se encuentran conectados a este.

**UTP:** Siglas de "Unshielded Twisted Pair". Cable de par trenzado sin blindar.

# V

**VACC:** Siglas de "Value Added Common Carrier". Una portadora común que ofrece algunos servicios de red, además de la simple transmisión punto a punto. Estos servicios incluyen: ruteo de bajo costo, control de recursos y aclaración de envíos.

**VAN:** Siglas de "Value Added Network". Una red que provee algunos servicios adicionales a los básicos. Ejemplos de estos tipos de RED son: TELNET y Tymnet.

**VHF:** Siglas de "Very High Frecuency". Porción del espectro electromagnético con frecuencias que van desde 30 a 300 Mhz.

**Video Conferencing:** La utilización de infraestructura (salas especiales) de conferencias remotas que incluyen señales de video.

**Video Signal:** Una señal que tenga el rango de frecuencias normalmente requerido para transportar información visual. Esto generalmente de 1 a 6 Mhz.

**VINES:** Siglas de "Virtual Networking System". Sistema Operativo de Red desarrollado por la compañía Banyan Systems. Vines está basado en el sistema operativo UNIX.

**Virtual Circuit:** Circuito virtual. Una conexión que se comporta como si existiera una conexión física entre la fuente y el destino.

**VLF:** Siglas de "Very Low Frecuency". Porción del espectro electromagnético con frecuencias que van de 3 a 30 Khz.

**VMS:** Siglas de "Virtual Memory System". Sistema operativo desarrollado por DEC para su familia de computadoras VAX.

**VSAT:** Siglas de "Very Small Aperture Terminal" Un servicio de transmisión/recepción vía satélite que requiere antenas pequeñas y de bajo de costo.

**VTAM:** Siglas de "Virtual Telecommunications Access Method". El método de acceso a disco utilizado por los sistemas IBM basados en SNA.

# W

**WACK:** Siglas de "Wait while ACKnowledge". Una señal de control de transmisión generada por el receptor para indicar que ha recibido el conjunto de información transmitido pero no ha tenido tiempo de determinar su confiabilidad.

**WAN:** Siglas de Wide Area Network". Se llama así a la red que se extiende sobre distancias muy grandes y que generalmente depende de líneas de comunicación para su funcionamiento correcto.

**Windows NT:** Windows New Technology. Nuevo sistema operativo de Microsoft. Ya no es un ambiente sobre DOS, sino un sistema operativo completo de 32 bits, incluirá varios servicios básicos de red y una arquitectura totalmente diferente.

**Windows:** Ambiente operativo (complemento de MS-DOS) desarrollado por Microsoft, para tener una interfaz sencilla al usuario, pero poderosa. La versión

3.1 se ve prácticamente igual que la interfaz gráfica de OS/2: Presentation Manager.

# X

**X.3:** Estándar de comunicaciones ANSI. No debe confundirse con las especificaciones CCITT X.3 para montar y desmontar dispositivos.

**X.25:** Estándar del CCITT que define el protocolo de comunicaciones por el que una computadora puede accesar una red de conmutación en paquetes (packet switching). En general cuando se habla de X.25 se habla de la familia de protocolos que son: X.3, X.28, etc.

**X.28:** Estándar del CCITT que define la forma que las terminales asíncronas accesan los paquetes de la red y el tipo de comandos y respuestas que utilizan.

**X.29:** Estándar del CCITT que define el protocolo de comunicación entre un DTE del esquema X.25 y un PAD.

**X.400:** Estándar da CCITT que define el intercambio de mensajes entre sistemas de correo electrónico.

**X.500:** Estándar de CCITT para el manejo de directorios en una red de área distribuida.

**XENIX:** Versión de UNIX desarrollada para computadoras de Zenith Data Systems que pertenece a Groupe Bull Company.

**Xmodem:** Un protocolo asíncrono de control del nivel de data-link del modelo OSI. Este protocolo es del dominio público.

**XNS:** Siglas de "Xerox Network Services". Especificaciones de los servicios de alto nivel de una red desarrollada por Xerox Corporation para soportar su línea de productos de automatización de oficinas.

**X/Open:** Organización dedicada a estandarizar los niveles más altos de UNIX para poder crear un medio ambiente común para las aplicaciones y mejorar la interoperabilidad de los sistemas.

**XTEN:** Siglas de "Xerox Telecomunications Network" Servicio de mensajes electrónicos digitales desarrollado por Xerox.

**X/Windows:** Protocolo Cliente/Servidor orientado al desarrollo de interfaces gráficas. Desarrollado originalmente en MIT en el proyecto ATHENA.

# Y

**YP: Siglas de "Yellow Pages". Nombre original de un servicio dentro de la familia de protocolos ONC.**

# BIBLIOGRAFIA.

REDES DE TELECOMUNICACIONES
Protocolos, modelados y análisis
Mischa Schwartz
Addison-Wesley Iberoamericana
Wilmington, Delawere, E.U.A.
217p.

DISEÑO DE REDES LOCALES
Hooper/Temple/Williamson
Addison-Wesley Iberoamericana
Wilmington, Delawere, E.U.A.
772p.

COMUNICACIONES
Lathi, B.P.
Julio 1991.
SISTEMAS DE COMUNICACIÓN
Naucalpan de Juárez, Edo. Méx.
McGraw Hill
703p.

REDES DE AREA LOCAL
Black, Uyless
1990
Redes de Computadoras, Protocolos Normas e Interfaces
México, D.F.
Macrobit

PERIFERICOS E INTERFACES
Varios autores coordinados porMompin Poblet, Jose
1984
Interconexión de periféricos a microprocesadores
Barcelona, España
Marcombo
226p

COMUNICACIONES
Ale, Rafael y Cuellar, Fernando
1991

TELEINFORMATICA
Naucalpan de Juárez, Edo. Méx.
McGraw Hill
261p

COMUNICACIONES
Varios autores coordinados por A. Alabau Muñoz
1991
Teleinformática y Redes de Computadoras
Barcelona, España
Marcombo
347p.

COMUNICACIONES
Stremler, Ferrel G.
1989
Sistemas de comunicación
México, D.F.
Alfa Omega
685p.

HP Ethertwist Product Catalog
May 1992

Technical Reference Guide
(Workgroup LANs HP Ethertwist Family Products)

Technical Reference Guide
(Site LANs and Multisite LANs HP Ethertwist Family of Products)

LAN Topologies for HP Ethertwist Family of Products

Gerez, Victor Ozitron, Veronica
Investigación de Operaciones
1976

Bazovsky, Y.
Reliability Theory and Practice
Prentice Hall Inc.
Unglewood Cliffs, N.J.
1961

Breipohl, A.M.
A. Statical Approach to Tolerances
Scandi Corporation Technical Memorandum
Albuquerque, Nuevo México
1960

Calabro, S.P.
Reliability Principles and Practices
McGraw Hill Book Company, Inc.
New York
1962

Lloyd, D.K. Lipow, M.
Reliability Management, Methods, and Mathematics
Prentice Hall, Inc.
Englewood Cliffs, N.J.
1962

Dummer, G.W. Giffin N.
Electronic Equipment Reliability
Jonh Wiley and Sons, Inc.
New York
1960

Ostle, Bernard
Estadistica Aplicada
Limusa
México
1977