UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

"REDES LOCALES DE COMPUTADORAS P. C. INSTALACION, MANEJO, APLICACIONES Y MANTENIMIENTO"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

Francisco Héctor Manuel Alvarez López

ASESOR: ING. MARTHA URRUTIA VARGAS

CUAUTITLAN IZCALLI, EDO. DE MEX. 1992

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

REDES LOCALES DE COMPUTADORAS P.C.
INSTALACION, MANEJO, APLICACIONES Y MANTENIMIENTO

PROLOGO

Sabemos que es una necesidad del mundo actual el manejo de grandes cantidades de información y la importancia de poder compartir esa información de manera rápida, ordenada y eficiente.
Las computadoras en primera instancia, solucionaron la necesidad de manejar grandes volúmenes de información. Pero es hasta la creación del concepto actual de red que la problemática de compartir información tiene un enfoque revolucionario.

El propósito de esta tesis es mostrar la factibilidad de instalar una red local (LAN) en la oficina en México de AFS Intercultural Programs, Organización internacional con sede en la ciudad de Nueva York dedicada al intercambio de estudiantes a nivel preparatoria entre más de 50 países.

Para lograr esto, presento un compendio de información de los elementos que forman una red local tanto a nivel hardware como software.

Las redes, presentan una opción para pequeñas y grandes empresas desde unos cuantos usuarios hasta cientos de ellos. Por ejemplo, una empresa podría desear instalar una pequeña red de 5 a 10 usuarios localizados en el mismo piso pero con la necesidad de consultar un mismo archivo de clientes o provedores. Gracias a la red, estos 5 ó 10 usuarios podrían estar consultando el mismo archivo practicamente al mismo tiempo sin necesidad de interrumpir o interferir en el trabajo del otro. Este beneficio se hace más

evidente conforme crece nuestra red, o nuestra aplicación requiere de más información compartida.
La habilidad de poder compartir información no es exclusiva de la redes, lo que las hace diferentes es la forma en que realizan lo anterior. En esta tesis trataremos de establecer las ventajas de un proceso distribuido (en red) sobre un proceso compartido (usando terminales tontas).

A lo largo de esta tesis, iremos presentando los conceptos básicos y la terminología de redes locales para irnos familiarizandonos con ellos. Analizaremos diferentes tipos de topologías, protocolos, cableado y equipo necesario con el que se cuenta para instalar una red y trataremos de establecer los parámetros para tomar un adecuada decisión dependiendo de las condiciones de la empresa.

Los capítulos I al IV los dedico a las bases teóricas y consideraciones necesarias para diseñar e instalar una red local, empezando por un análisis de las necesidades de la empresa que nos interesa pasando por las diferentes opciones que están presentes en el mercado de redes a nivel hardware.
El capítulo V se desarrolla sobre el concepto de "sistemas abiertos" y compatibilidad entre diversos equipos lo que hizo necesario crear o establecer un serie de reglas o protocolos descritos en este capítulo.

Los capítulos VI. y VII versan sobre el software de redes. Ya que todos sabemos que una computadora sin software es como un coche sin llantas. El capítulo VI es una reseña de los sistemas operativos de mayor vigencia en el mercado poniendo un mayor énfasis en LANTASTIC y LAN Manager y comparando todos ellos con Netware de Novell. Las prácticas para la realización de esta tesis fueron realizadas en una red con topología de bus usando un server 386 con 4 Mb de memoria RAM y 126 Mb en disco duro corriendo el sistema operativo Advanced Netware 286. Ya que considero a Netware un sistema operativo muy confiable y de gran difusión anexo el apéndice A como un introducción al manejo de menús y la administración de la red.
Finalmente. el capítulo VII se refiere a las aplicaciones de la red y las consideraciones generales para el uso de software de aplicación en red.

La Conectividad. tratada en el capítulo VIII, podría definirse como la capacidad de la red a crecer y ser compatible con otros sistemas. En este capítulo vemos la integración de UNIX y Macintosh al ambiente de red así como la participación de minis y mainframes y el enfoque más amplio del concepto de red que puede crecer a convertirse en redes de area amplia (WAN's) que puede incluir desde distintos edificios en una misma area hasta la comunicación internacional por medio de un correo electrónico.
Por último. el capítulo X lo dedico a tratar el mantenimiento de redes mostrando los principales equipos de mantenimiento de cableado y demás accesorios de la red.

INTRODUCCION

1.1 ANTECEDENTES

El almacenamiento y el análisis de información ha sido uno de los grandes problemas a que se ha enfrentado el hombre desde que invento la escritura. No es sino hasta la segunda mitad del siglo XX que el hombre ha podido resolver, parcialmente, ese problema gracias a la invención de la computadora.

En la década de los 50's el hombre dio un gran salto al inventar la computadora electrónica. La información ya podía ser enviada en grandes cantidades a un lugar central donde se realizaba su procesamiento. Ahora el problema era que esa información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser acarreada al departamento de proceso de datos.

Con la aparición de las terminales en la década de los 60's se logro la comunicación directa entre los usuarios y la unidad central de proceso, logrando una comunicación más rápida y eficiente, pero se encontró un obstáculo, entre más terminales y otros periféricos se agregaban al computador central, la velocidad de procesamiento decaia.

Hacia la mitad de la década de los 70's la delicada tecnología del silicon (silicio) e integración en miniatura 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 ese

momento cada usuario tenia su propia microcomputadora en su escritorio.

A principios de la década de los 80's las microcomputadoras habian revolucionado por completo el concepto de computación electronica asi como sus aplicaciones y mercado. Los gerentes de los departamentos de informatica fueron perdiendo el control de la información puesto que el proceso de la información no estaba centralizado.

A esta época se le podria denominar la era del floppy disk. Los vendedores de microcomputadoras proclamaban "En estos 30 diskettes puede usted almacenar la información de todo su archivo".

Sin embargo, de alguna manera, se habia retrocedido en la forma de procesar la información. Habia que acarrear la información almacenada en los diskettes de una micro a otra y la relativa poca capacidad de los diskettes hacia dificil el manejo de grandes cantidades de información.

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

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

redes locales.

Las primeras redes locales estaban basadas en "Disk Servers". Estos equipos permiten a cada usuario el mismo acceso a todas las partes del disco. Esto causaba obvios problemas de seguridad y de integridad en los datos.

Actualmente se maneja el concepto de "File Server" en el que todos los usuarios pueden tener acceso a la misma información, compartiendo archivos y contando con niveles de seguridad, lo que permite que la integridad de la información no sea violada.

El primer desarrollo del comcepto de red surgió en los años 70's. En ese entonces, las redes de computación fueron definidas por cada fabricante para poder aprovechar las características propias del mainframe. La arquitectura de sistema de red (SNA) de IBM fue anunciado en 1974, seguido en 1976 por la arquitectura de red digital (DNA) de Digital Equipment Corporation. Pronto les siguieron otros fabricantes como la arquitectura de red Burroughs, La arquitectura de sistemas distribuidos de Honeywell y otras. Cada una de estas redes, sin embargo, tenía un tema principal: una arquitectura propia, diferentes protocolos y una variedad de interfases. Algunas de las especificaciones de estas redes cumplieron con los estandares de la industria como la EIA-232, y algunas otras permanecieron propias.

En esta tesis, trataremos a las redes desde un punto de vista de arquitectura abierta, es decir, con capacidad de compartir recursos desde diferentes plataformas y trabajando con distintos ambientes. Por ejemplo, PC's y machintosh en la misma red o aplicaciones de MS-DOS, OS/2 y Unix también interactuando entre si.

1.2 CONCEPTOS BASICOS

Red Local(LAN): Conjunto de computadoras conectadas en ambiente multiusuario compartiendo recursos. Es un sistema de proceso distribuido muy diferente al proceso compartido. Se trabaja con terminales inteligentes cada una capaz de procesar información.

Red Metropolitana (MAN): Red de comunicación de alta velocidad que abarca 80 kms. aproximadamente.

Red de area amplia (WAN) Redes de comunicación mayores de más de 80 kms. Esto incluye comunicación entre ciudades y aún entre paises.

Red Digital de Servicios Integrados: Conjunto de protocolos y demás elementos propuestos para transmitir señales de voz, datos, fax y video en una red.

Red Heterogenea: Red local o remota con hardware y software de diferentes compañias, usualmente implementando diferentes protocolos, sistemas operativos y aplicaciones.

Ambiente multiusuario: Sistema en el que dos o más personas trabajan con posibilidad de compartir información pero donde el proceso está centralizado y se accesa a la información mediante terminales tontas.

Ambiente multitareas: Sistema en el cual el mismo procesador es capaz de realizar dos o más tareas u operaciones casi a la vez.

Servidor: El servidor es la máquina donde reside el sistema operativo de la red y la cual sirve de administrador de la red.

- -El server pude ser desde una PC AT hasta un mainframe.
- -Puede utilizarse más de un servidor, dependiendo de los recursos.
- -Existen dos tipos de servidores.

Servidor dedicado: Es aquel que funciona única y exclusivamente como servidor, controlando el flujo de información en la red.

Servidor no dedicado: Este tipo de servidor aparte de controlar la red, puede también ser utilizado como una terminal de trabajo pero con la consiguiente pérdida de velocidad y eficiencia.

File Sever: Computadora que actúa como "almacén" de información y aplicaciones para los usuarios de una red.

Terminal de trabajo (workstation): La terminal es la computadora desde la cual un usuario trabaja como parte de la red. Las terminales puden ser desde una PC XT. Este tipo de terminales se les denomina terminales inteligentes ya que comparten el trabajo con el servidor y pueden ser usadas independientemente de la red. Se diferencian de las terminales tontas , ya que estas sólo muestran el trabajo que realiza el procesador central sin contribuir en nada a la realización de éste.

Sistema Operativo de red: Es el software base de operación. Generalmente es un shell de otro sistema operativo.

Shell: Es un programa cuya finalidad es hacer más amigable el manejo del sistema operativo.

Plataforma: Se le llama plataforma al sistema operativo base del servidor, éste pude ser MS DOS, OS/2, Unix, Machintosh, Vax VMS.

Arquitectura abierta: La arquitectura abierta es la tendencia de los nuevos sistemas y consiste en soportar las diferentes plataformas e integrarlas a una misma red.

Correo electrónico (e-mail): Consiste en un sistema de mensajes computarizado para intercambiar "correo" electrónicamente.

EISA (Expanded Industry Standard Architecture): Conjunto de normas para computadoras personales que amplian la capacidad del bus ISA desarrollado por IBM para su PC original.

ISA (Industry Standard Architecture): Arquitectura de bus desarrollada por IBM para sus PC XT, AT.

IEEE (Institute of Electrical and Electronics Engineers) El Instituto de Ingenieros Eléctricos y Electrónicos es una organización profesional que formula las normas de computación y comunicación en los Estados Unidos. El Instituto trabaja con una variedad de otras instituciones normativas como la Organización Internacional de Standards (ISO).

OSI (Open Systems Interconection) Modelo de referencia de la ISO el cual especifica las diferencias entre dispositivos de computación como tarjetas de interfase, puentes y ruteadores.

Puentes: Los puentes son un dispositivo para interconectar dos redes locales y estos operan en la capa de control de acceso al medio.

Ruteadores: Son dispositivos un poco más sofisticados que los puentes ya que éstos direccionan la información por el camino que más le convenga.

Gateways: Dispositivo para conectar dos o más redes diferentes o una red con un mainframe. Los Gateways operan en la capa de sesión, presentación y aplicación.

Hub: Es una caja central de conección de cables o un repetidor que enlaza la conexión de multiples nodos de red.

MAU (Multistation Access Unit): Unidad de acceso múltiple para conectar nodos de red a un medio de transmisión.

TCP/IP (Transmision Control Protocol/Internet Protocol): Uno de los primeros protocolos de comunicación para resolver el problema de interconectar computadoras.

IPX (Internetwork Packet eXchange): Protocolo de Novell para comunicar PC's en red. Es como un interprete entre el sistema operativo base y el de red.

Cableado: medio por el cual se conectan físicamente las estaciones de trabajo y el server.

Tarjetas de Interface: Es también un elemento de hardware que controla la comunicación entre terminales y server.

Mbps: Unidad de velocidad de transmisión de datos (Mega bits por segundo).

Existen otros términos los cuales iremos detallando conforme se presenten y sea necesario profundizar en ellos.

1.3 NECESIDADES DE COMUNICACION EN AFS INTERCULTURAL PROGRAMS.

Cualquier persona familiarizada con las computadoras puede asegurarle que una computadora por si sola es una herramienta muy poco efectiva en cualquier empresa y que para poder sacarle el mayor provecho posible se deben combinar una serie de factores tales como: software adecuado, personal calificado y una correcta administración de los recursos.

Por otro lado, cuando una persona o compañía desea adquirir una computadora se puede ver abrumado con una enorme cantidad de opciones: diferentes fabricantes, diferentes tipos de maquinas, sistemas operativos, software, etc. Para poder tomar una decisión acertada debemos hacernos una serie de preguntas:

¿Para qué queremos una computadora?

¿Que tareas vamos a procesar?

¿Cuál es el software conveniente para realizar eso?

¿Cuáles son los requerimientos de equipo (hardware)?

¿Existe personal capacitado?

¿Es necesario programar cursos de capacitación?

¿La instalación eléctrica es adecuada?

¿Cuál es el presupuesto?

En la actualidad, es muy comun el uso de computadoras en casi todas las actividades y es raro encontrar una empresa que no cuente en su inventario con al menos algunas computadoras. Desafortunadamente, tampoco es extraño encontrar que la adquisión de esos equipos se hizo sin el debido cuidado y planeacion. Así

podemos ver como una maquina 386 es usada para procesar textos - en el otro sentido se puede tener una XT sin suficiente memoria para correr una aplicación.

En el caso que nos interesa en esta tesis, "AFS Intercultural Programs" cuenta en la actualidad con dos computadoras: una XT Printaform con 512 Kb en RAM y disco duro de 20 Mb y una XT ACER con 640 Kb en RAM y 30 MB en disco duro. Ademas se cuenta con dos impresoras de matriz de punto, una de 10 pulgadas y la otra de 15. AFS es una organización no lucrativa cuya oficina central esta ubicada en N.Y. y cuenta con oficinas de representación en mas de 50 paises. Su actividad principal consiste en el intercambio de estudiantes entre 15 y 17 años durante un año escolar durante el cual todos los participantes viven con una familia y asisten regularmente a clases de preparatoria en el extranjero. Lo anterior implica procesar información de más de 2500 estudiantes tal como edad, sexo, escolaridad, religión, intereses, etc. Ya que estos estudiantes son ubicados con familias afines a sus caracteristicas, es necesario localizar y por lo tanto procesar información relativa a por lo menos 3000 familias. Cada familia por su parte representa una escuela que recibirá a los estudiantes. Siendo AFS un organismo no lucrativo, se ha sostenido gracias al apoyo de una gran base de más de 75000 voluntarios en todo el mundo cada uno actuando como una pequeña oficina en su comunidad y consecuentemente es necesario amnetener una base de datos de estas personas.

Al movilizar cada año más de 2500 estudiantes entre 50 paises es obvia la necesidad de tener un método y una infrestuctura de

comunicacion entre las distintas oficinas y voluntarios. Se debe de llevar un control de visas, pasaportes, boletos de avion, etc. En otro orden de cosas, el departamento de contabilidad tambien necesita estar al tanto del pago de cuotas, gastos médicos, etc.

El departamento de sistemas de AFS en Nueva York, viendo la necesidad de comunicación y control y considerando el crecimiento potencial de la organización, inició un proyecto hace algunos años de automatización de oficinasque empezó desde la introducción de computadoras en todas las oficinas hasta la meta final que sería la instalacion de una red en cada unidad nacional. Esta red local, a su vez sería parte de una gran red mundial con la implementación de un correo electrónico para la comunicación y el intercambio de archivos. Como ya he mencionado, el propósito de esta tesis es estudiar y analizar lo concerniente a las redes locales y tomar una decisión respecto al futuro informático de AFS México.

El software de uso general, y que es más o menos un estandard en casi todas las oficinas nacionales es el siguiente: Word Perfect, Dbase III PLus, Lotus y un sotware desarrollado por sistemas en N.Y. llamado "AFS Sending/Hosting System" y "AFS Membership System".

Este sistema fue desarrollado en Fox base y el primero es para el manejo de estudiantes, familias y escuelas durante su año de participación o "activo". Al término de ese año, se hace una transferencia al segundo sistema donde son catalaogados como miembros de AFS.

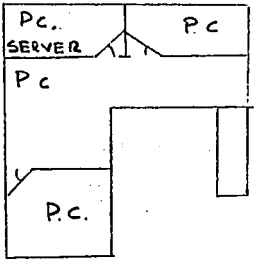
Word Perfect es utilizado para cartas a estudiantes, familias,

escuelas, embajadas, etc.

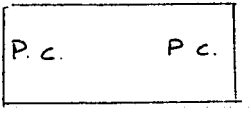
Lotus es utilizado por contabilidad para elaborar presupuestos, reportes mensuales, etc.

Finalmente, Dbase III Plus se usa para mantener una base de datos de voluntarios y demas organizaciones que apoyan a AFS en diversos sentidos. Estas organizaciones pueden ser: embajadas, lineas aereas, gobierno e iniciativa privada en general. AFS México ademas cuenta con Hardvard Graphics y Ventura para desarrollo de material publicitario.

AFS México está ubicado en una casa habitación acondicionada como oficina, por lo que uno de los primeros pasos antes de instalar una red sería la instalacion eléctrica adecuada. Suponiendo que esos detalles ya fueron resueltos, nos concentraremos en la red en si. La distribución de la oficina es la mostrada en la siguiente figura:



PLANTA BAJA



PLANTA ALTA

Los requerimientos mínimos para esta red serían de un servidor que pudiera ser no dedicado y por lo menos 4 estaciones de trabajo. La instalación de cableado y el sistema operativo de red.

Las necesidades específicas de AFS México para el año 92-93 incluyen el envío de más de 80 estudiantes mexicanos al extranjero y la recepción de más de 120 estudiantes extranjeros en México. Sin embargo es importante recordar que la red se planea a mediano y largo plazo y hay que considerar el crecimiento potencial.

AFS México cuenta con la ayuda de voluntarios localizados en más de 15 ciudades de la república de donde provienen y/a donde irán a vivir los estudiantes participantes. Un organigrama general de funciones es el siguiente:

Director Nacional

Coordinación de Envío Coordinación de hospedaje

Contabilidad

La coordinación de envío es responsable de los estudiantes mexicanos y a su vez la coordinación de hospedaje se encarga de los extranjeros. Sin embargo es imprescindible la comunicación entre ambas coordinaciones debido a que muchas familias que envían estudiante también reciben a uno. Por otro lado, hay una infinidad de actividades que se deben coordinar conjuntamente y con apoyo de los voluntarios.

Por su parte, la dirección nacional debe estar al tanto de todos los movimientos en ambas coordinaciones y tener en todo momento la información actualizada y a la mano.

Por último, pero no menos importante, está el departamento de contabilidad, el cual debe saber en todo momento quienes son los

estudiantes participantes, quien se enferma y de que para poder pagar sus gastos médicos, quien o quienes necesitan hacer viajes dentro de la republica o de regreso a su país de origen. Se debe controlar la compra de boletos de avión o autobus, el pago de la cuota de participación de estudiantes mexicanos, extender recibos, etc. Teniendo toda esta información disponible en su propia estación de trabajo y actualizada automáticamente al compartir el mismo archivo de las coordinaciones se incrementa enormemente la productividad y se reduce considerablemente el tiempo de ejecución.

En los siguientes puntos habalare ampliamente de las diferentes opciones y de la forma en que funciona una red.

1.4 EJEMPLOS DE REDES LOCALES

En este punto veremos diferentes ejemplos de los beneficios que ofrece una red, sus ventajas y lo que podemos esperar de una red local.

1.4.a. PARQUE DE DIVERSIONES "SIX FLAGS"

Como una corporación, "Six Flags" tiene que controlar las funciones típicas de todo negocio, tales como nómina y contabilidad. Cada uno de los siete parques "Six Flags" es también como una pequeña ciudad, con una fuerza policíaca, departamento de sanidad y tienda de abarrotes. Además, cada parque debe ser capaz de operar independientemente de la cabeza central localizada en Arlington, Texas. Los parques de diversiones por sí mismos son un reto inusual. Por ejemplo, el cablear alrededor de juegos con troncos y agua.

Hasta hace cuatro años, "Six Flags", había estado manejando sus operaciones con un mainframe tradicional en un ambiente de minicomputadora. Sin embargo, el crecimiento acelerado de la compañía rebasó la capacidad de las minis, forzando cambios frecuentes y costosos. Finalmente, a fines de 1987, la compañía puso fin a las minis y decidió reemplazarlas con una red.

La red ha mejorado la eficiencia de los parques enormemente. "Con una mini o un mainframe, cada vez que añades un usuario es una carga más al sistema. Con una red de P.C.'s cada vez que se agrega un nodo se aumenta el poder".

El proceso de cambio fue quizá lo menos difícil de todo. Ya que la compañía ya poseía las minis que estaban controlando sus operaciones, no hubo una urgencia real de implementar las LANs inmediatamente. Lo que es más, entre los siete parques y las

oficinas centrales, había aproximadamente 200 PC's, y en 1986, uno de los parques ya había instalado una pequeña red de Novell.

EL RETO DEL CABLEADO

El gran obstaculo a vencer al instalar la red en cada uno de los parques fue el cableado. Como en una ciudad, donde las compañías no pueden construir sus propios túneles para cableado en terreno público en caso de que interfieran con lineas de agua o lineas eléctricas. No se pudieron construir lineas dentro del parque por la misma razón. Mientras que una red Ethernet era la adecuada para cada edificio principal de cada parque. Está red hacía difícil conectar con otras computadoras dentro del parque. En lugar de tratar de "cablear" alrededor de la Montaña Rusa, el departamento de sistemas decidió usar el cable de par trenzado ya instalado en conjunción con una solución propiedad de Networth.

La solución de Networth, una compañía de Texas, es similar a Ethernet en su protocolo de comunicación: CSMA, sólo que en lugar de utilizar detector de colisiones, esta implementado con un eliminador de colisiones. La distancia típica entre las estaciones y la caja de conexiones o hub es de 30 metros, sin embargo a través de hubs en cascada puede incrementarse a 180 metros. La información tiene una velocidad de transferencia de 800 Kbps. Independientemente de su menor velocidad, la solución de Networth es ideal para la configuración física de los parques. Por ejemplo, el edificio de personal en el parque de Los Angeles es una casa adaptada que se localiza en los límites de un estacionamiento que sólo puede ser conectado prácticamente a través de las líneas telefónicas existentes.

El único problema de utilizar cable de par trenzado es que la red

ocasionalmente recibía interferencia de rayos que eran propagados por todo el sistema telefónico. Al no encontrarse una compañía America de protección de potencia, Six Flags decidió contratar a Citel, una compañía francesa con oficinas en Miami. Six Flags utiliza los dispositivos de aislamiento de Citel, de 50 dólares cada uno para proteger las redes Ethernet en los edificios principales y los nodos de par trenzado en todo el parque.

Cada parque, incluyendo las oficinas centrales, tiene una red Advanced Netware 286 de Novell con un servidor único y hasta 30 nodos. La mayoría de los servidores son 386 con un mínimo de 650 Mb en disco duro, aunque algunos tienen hasta 900 Mb. Las estaciones son AT 286 de 16 Mhz con monitores VGA.

APLICACIONES

Los requerimientos físicos no fueron el único obstáculo. Las aplicaciones que controlan cada aspecto de los parques son igualmente unicas. Cada parque tiene que hacer todo desde ordenar hamburguesas hasta realizar análisis demográficos de sus visitantes durante los meses de verano. El volumen de información de empleados, visitantes e inventario está ahora completamente automatizado.

Por ejemplo, Los parques Six Flags guardan información de los pases de temporada en su red. En el pasado, cada visitante, aún los que habían estado yendo al parque por años, tenían que llenar una nueva forma de pase de temporada al principio de cada verano. Con el nuevo sistema, los visitantes reciben un pase con código de barras que puede ser renovado cada año. El codigo de barras también elimina el problema de varias personas compartiendo el mismo pase, que es solo válido por una entrada al día. Si el pase

a los usados ese día, el sistema lo rechaza.

Los pases también permiten a los parques el recolectar información demográfica referente a las horas de uso en relación con el sexo y la edad. Los parques tienen sistemas de monitoreo de asistencia para evaluar la efectividad de sus programas de mercadotecnia. Cada quinto grupo que entra al parque es encuestado en relación a su edad, sexo, etc. La información es almacenada en el sistema y comparada con una base de datos externa para así evaluar.

Los parques también están usando código de barras en las identificaciones de los empleados para controlar el acceso. Todos los empleados pueden usar las facilidades del parque sin cargo alguno cuando estan fuera de servicio. Sin embargo, en el pasado, cuando algún empleado renunciaba o era despedido, la notificación era enviada a la oficina central donde la procesaban. Podía tardar varias semanas el registrar la renuncia o despido. En algunos casos, el parque contrató a personas a quienes se les dió identificación pero nunca se presentaron a trabajar, pero sí utilizaron el parque libre de cargo. Con el nuevo sistema, cuando un empleado renuncia o es despedido, su pase es invalidado inmediatamente.

El parque también emplea a jóvenes de 15 años, que, de acuerdo a la ley laboral, sólo pueden trabajar un número limitado de horas. Anteriormente, dado el tamaño del parque era muy difícil llevar un control al respecto, y detectar cuando un menor estaba trabajando de más. Con la nueva identificación, el parque puede fácilmente monitorear el tiempo que cada quien trabaja.

La compañía tiene que expedir aproximadamente 20,000 cheques cada verano. Con el cambio de empleados esta cifra llega hasta 35,000.

lo que significa 35,000 formas de papel. Mientras que la nómina es administrada centralmente, la información es también almacenada en cada parque como respaldo y para una rápida actualización a los expedientes de los empleados.

Durante la primavera de 1990, Six Flags empezó a transformar su programa de bancos, el cual llevaba un registro de todos los parques, a un sistema de red. El sistema de bancos registra las ventas diarias de cada parque.

Actualmente, todos los expendios de comida en el parque tienen una caja registradora IBM 4680 la cual usa cable de par trenzado IBM tipo 1. Pero debido a la diferencia entre la terminal el tipo de cable de la LAN, el sistema puede reportar en dólares y centavos cuanto está vendiendo un expendio, pero no es posible el saber qué es lo que está vendiendo. Un sistema de punto de venta conectado a la LAN permitiría al parque auditar su inventario basandose en lo que se está vendiendo y así automáticamente ordenar las provisiones necesarias.

La red no se usa para controlar los juegos, pero sí se usa para su mantenimiento, controlando los servicios, partes y refacciones.

Todavía hay mucho que hacer e implementar en Six Flags, sin embargo esto es un ejemplo claro de las aplicaciones de una red.

1.4.c. FUERZA AEREA DE LOS ESTADOS UNIDOS

La fuerza aerea tiene su base de operaciones en Wright-Patterson cerca de Dayton, OH. Esta base es responsable de servir y dar mantenimiento a todos los aviones de la fuerza. Cada año examina 1,300 aviones, reconstruye 3,400 motores, procesa 4 millones de requisisiones de material y repara dos millones de componentes.

Hay cinco centros logisticos en todo el país que participan en la red de trabajo. Estos centros están localizados en Georgia, Texas, Oklahoma, Utah y California. Una cantidad impresionante de información debe ser almacenada y procesada cuando se ordena materiales o se reciben éstos o cuando llega algún equipo a servicio. De acuerdo al gerente de redes de la Fuerza Aerea, antes de 1987, no existia ninguna red organizada de trabajo. Habia muchas minis y PC's, pero no existia ningún método de recolectar y distribuir información. Todos los datos referentes a servicio y materiales eran alamacenados por paquetes. En ese entonces se decidió por modernizarse.

El proyecto de modernización tiene un costo de $1.5 billones de dólares y está programado a 10 años. El sistema de computo tenia que ser mejorado en dos niveles. Los programas que manejaran toda la información de mantenimiento y existencias y la implementación de una red de comunicaciones. La red tenia que proveer conexiones de comunicación para aproximadamente 35,000 usuarios de PC terminales, y comunicación entre servidores anfitriones.

IDEAL PARA BANDA ANCHA

La Fuerza Aerea eventualmente decidio la banda ancha como su medio de transmisión. La Fuerza Aerea utiliza video de dos vias para entrenamientos y teleconferencias entre locaciones.

Cada centro logistico, al igual que el centro de operaciones, tiene una red de banda ancha de cable dual (Figuras 1 y 2). Existen algunas conexiones de fibra para futuras ampliaciones, pero la mayor parte se utiliza red de banda ancha. Las comunicaciones entre estación y servidor son sobre un canal de 2 Mbps, y las que son entre servidores a 10 Mbps. Las locaciones están enlazadas a la red de información de la Defensa (DDN).

Este proyecto fue iniciado en 1988 y ha progresado en varias etapas. La primera etapa fue la instalación de red a nivel local, en cada edificio de los centros logisticos y de la oficina base, con unidades de interfase de red (NIUs) y conectadas utilizando unidades inteligentes (ICU). El siguiente paso fue conectar dos edificios dentro de la misma localización. En 1987, empezo la construcción mayor, en la cual las bases fueron literalmente desmanteladas para poder colocar el cableado necesario para transmisión de banda ancha. En 1988 y 1989, edificios adicionales fueron cableados, y la fase final, con los edificios restantes conectados, y todos los programas de mantenimiento listos se completó en la primavera de 1990.

ADMINISTRANDO INFORMACION MASIVA

Las redes de la Fuerza Aerea tienen varias aplicaciones que manejan la cantidad enorme de información que es almacenada diariamente. Todos los programas corren bajo diferentes servidores y proporcionan un acceso casi inmediato a la información. Canales especificos en el rango de 40 MHz a 450 MHz están designados a aplicaciones especificas. De este modo, el ancho de banda puede balancearse conforme se necesite de acuerdo a las aplicaciones.

El sistema de modernización logistica consiste en ocho programas

para adquisición y distribución de materiales. El banco de datos de requerimientos, por ejemplo, determina que artículos se necesitan. El programa no solo determina el artículo y la cantidad necesarios, sino también prepara presupuestos y hace simulaciones. Indudablemente el mas interesante e importante sistema a implementar en la Fuerza Aerea es el de Sistema de Información de Sistemas de Armas. (Un sistema de armas es un avión armado como el F16). Este sistema es un programa modelo que estima la habilidad de la Fuerza Aerea para poder ostener un nivel deseable de combate en una guerra y computa los requerimientos en tiempo de guerra. Resume los reportes de apoyo de un sistema de armas, complementandolo con un calendario de reparaciones para cualquier falla.

El sistema de información automatizada de transportes maneja la transportación de materiales realizada por la línea aerea de la Fuerza aerea. Este sistema comunica todos los sistemas de transporte marinos, aereos y terrestres y proporciona un sistema de control para el transito de materiales.

El Sistema de distribución y control de inventarios -el más grande de los programas- controla el inventario, localización y distribución de todas las existencias. La confiabilidad y mantenimiento de sistemas de información controla los intercambios de información de mantenimiento. Es la principal base de datos de la Fuerza Aerea para recolectar y procesar contratos de mantenimiento e información de inspección e incluye un reporte para problemas de análisis.

En adición a las funciones administrativas, información técnica también se comunica a través de la red. El Sistema de información

técnica, maneja las informaciones más recientes respecto a la aviación. El Sistema de Ordenes Técnicas es responsable de una gran cantidad de información ya que actualiza ordenes técnicas o manuales que contienen información específica de las partes.

Todos estos sistemas, de alguna u otra manera necesitan compartir información, y esto se logra de manera eficiente con la red instalada.

MANTENIMIENTO

Las LAN's de la Fuerza Aerea usan un aplicación de mantenimiento de red llamada *sistema de control y monitoreo técnico*, que incluye software comercial y software escrito especificamente para el programa.

En la base de operaciones de la Fuerza Aerea y en los centros logísticos, las redes son administradas usando una red de herramientas de mantenimiento con sus propias estaciones.

Desde un punto central, el gerente de redes puede detectar problemas casi de cualquier tipo. Por ejemplo, cada hora, El número total de peticiones y respuestas es acumulado por cada canal de banda ancha, de tal manera que el gerente puede ver cuantas peticiones no han sido contestadas y decidir si existe o no un problema.

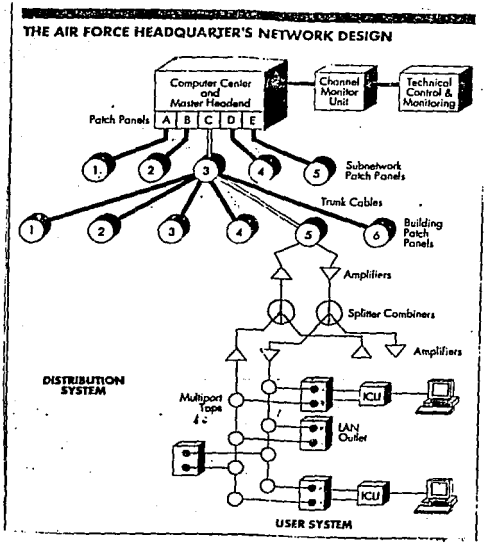


Figura 1.1 El Centro de logistica de la Fuerza Aerea decidio instalar una red de banda ancha ya que solo la banda ancha podria soportar las conexiones estacion-servidor,servidor-servidor y video de dos caminos. Los cinco centros y la base de operaciones tienen su propia red local y estan conectadas entre si por medio de la Red de datos de la Defensa.

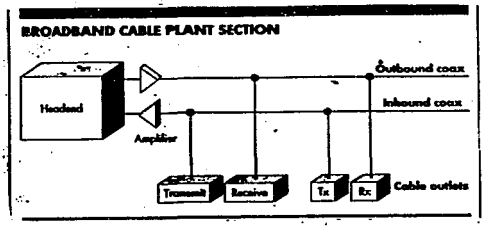


figura 1.2 El centro de logistica de la Fuerza Aerea instalo redes de banda ancha con cable dual. El "cerebro" de la red es la cabeza (headend), el cual cambia la frecuencia de las senales de entrada a la frecuencia del canal de salida. En un sistema de cable dual, un usuario tiene un cable para transmitir y otro para la recepcion.

Estos ejemplos muestran claramente la versatilidad de las redes locales y su aplicacion a tareas muy diferentes entre si pero siempre manejando el concepto de compartir recursos. Los recursos son tanto fisicos (hardware) como, y estos son más importantes, de datos e información (software).

Una vez teniendo más claro el concepto de red y su aplicación práctica en la industria y los negocios, podemos proseguir con nuestro estudio.

CAPITULO II

TOPOLOGIAS DE RED

Una topología se refiere a la manera física en que está conectada una red local.

Existen cuatro topologías básicas para redes locales:

2.1 TOPOLOGIA DE BUS

En esta topología todos los nodos o estaciones de la red están interconectados a un único cable de comunicación llamado BUS o troncal de comunicación, formando una trayectoria abierta y limitada en sus extremos por terminadores.

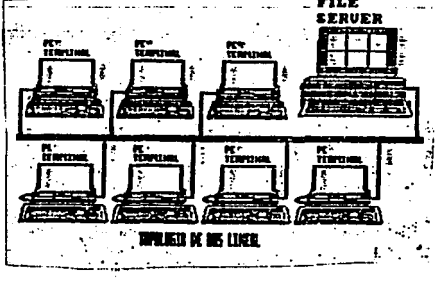


Fig. 2.1 Topología bus lineal

2.2 TOPOLOGIA DE ESTRELLA

La topologia tipo estrella se caracteriza por un file server centralizado con una conexión directa para cada estación de trabajo. Las comunicaciones en esta topologia son bidireccionales y éstas son manejadas a traves del File server. Una falla de alguna estación de trabajo no afecta el funcionamiento de la red. Esta configuración es la más rápida en condiciones de un gran número de entradas y salidas de información.

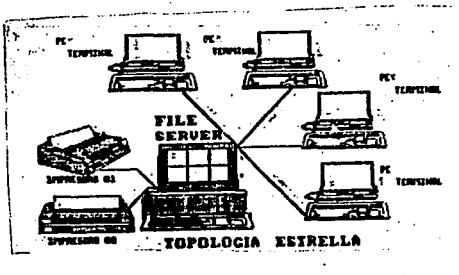


Fig. 2.2 Topologia estrella

2.3 TOPOLOGIA DE ANILLO

La topología de anillo se caracteriza por entablar una comunicación circular, ya que cada estación de trabajo está conectada a otras dos y éstas a su vez con otras dos hasta cerrar un anillo. En la actualidad no existen verdaderas topologías de anillo en el mercado, ya que una desventaja que presenta es el riesgo de que la comunicación de la red se interrumpa a causa de una falla en una de las estaciones de trabajo.

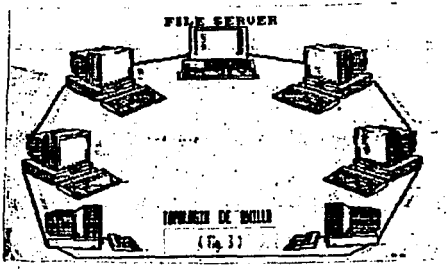


Fig. 2.3 Topología de anillo

2.3.a. TOPOLOGIA DE ANILLO MODIFICADO

La topología de anillo modificado consta de una caja a la que se le conectan las estaciones de trabajo y el server, de forma que a partir de ahí se entabla la comunicación, por lo que si una estación de trabajo se descompone no se pierde la comunicación en el resto de la red.

La caja a la que se conectan las computadoras es un MAU o un HUB.

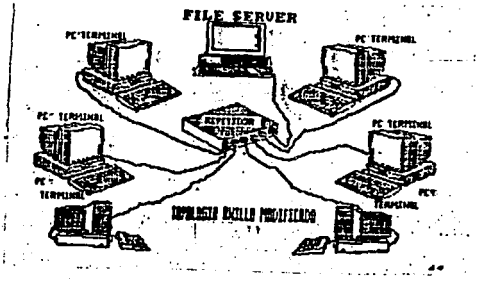


Fig. 2.4 Topología de anillo modificado

Es importante hacer notar que la topología de red se refiere a la forma en que están conectadas las computadoras más que a la ubicación física de éstas. Es decir que podríamos tener una red con las computadoras ubicadas físicamente en forma circular, y estar conectadas en topología de BUS.

Dependiendo de la topología que se utilice, se determina también el protocolo de comunicación. A continuación presentamos un cuadro sinóptico de las diferentes topologías:

TOPOLOGIA	PROTOCOLO	VENTAJAS	DESVENTAJAS
BUS	CSMA/CD	File server XT,AT. 386 Muy sencilla de instalar Utiliza menos metros de cable.	Dificil deteccion de fallas Hay colisiones Debe hacerse una cuidadosa planeacion de la ruta del cable.
ESTRELLA	POLLING	Protocolo rapido No hay colisiones Gran numero de usuarios Cable barato	Red costosa File server especial Mucho cable Dificil reinstalacion
ANILLO MODIFICADO	TOKEN PASSING	File server XT,AT, 386 Permite grandes distancias	Dificil instalacion Cable caro Cuidadosa planeacion de red.

Nota: Esta tabla de ventajas y desventajas de tomarse con la debida precaucion, ya que establece caracteristicas demasiado generales.

CAPITULO III
TARJETAS DE RED

3.1 ETHERNET

Ethernet es sin duda la red mas difundida de todas, rebasando los tres millones de nodos vendidos, además Ethernet cuenta con mayor numero de vendedores y empresas investigadoras. Ethernet fue creada por XEROX en 1974 e inicialmente su velocidad de transmisión fue de 3 Mbps. La primera versión comercial de Ethernet de 10 Mbps fue desarrollada por DEC, Intel y XEROX a finales de los años 80 y publicada en sep. de 1980.

Las Redes Ethernet se caracterizan por contar con un protocolo de comunicación denominado CSMA/CD (Carrier Sense Multiple Access/Colision Detection) el cual se basa en un esquema de detección de colisiones y por una topología de bus lineal en donde todos los nodos de la red, tanto servidores de archivos como estaciones de trabajo, se encuentran unidos entre sí a través de un cable de interfase, al cual se le conoce con el nombre de segmento troncal.

El segmento troncal de cable está formado por un conjunto de segmentos conectados por medio de conectores que lo hacen ver como si fuera un cable continuo.

Este segmento troncal obedece a ciertas reglas y características de funcionamiento, sin embargo, las Redes Locales Ethernet no tienen por que conformarse con las limitaciones de un sólo segmento troncal dado que se puede extender el tamaño de un segmento troncal hasta cinco veces, mediante la implementación de dispositivos como amplificadores, puentes (bridges) o ruteadores

(routers).

Existen dos tipos de cables diferentes para Ethernet. El primero es denominado cable delgado Ethernet (figura 3.1) y es mas barato que el segundo que es llamado cable grueso Ethernet o cable estándar Ethernet.

Ahora bien, revisemos las diferentes alternativas de cableado con que cuentan las Redes Ethernet.

Redes de cable delgado

Hardware necesario para redes Ethernet con cable delgado:

Tarjeta de interfase Ethernet. Esta tarjeta es colocada en un slot de cada una de las estaciones de trabajo de la red. La velocidad de transferencia de información con este tipo de interfase es de 10 Mbps.

Conector BNC tipo plug. Estos conectores son usados para interconectar el hardware de la red.

Cable delgado Ethernet. Conocido como cable coaxial RG-58 A/U de 0.2 pulgadas de diametro y una impedancia de 50 ohms.

Conector BNC tipo "T". Utilizados para unir dos tramos de cable delgado a una trajeta de interfase de la estación de trabajo.

Terminador BNC. Este tipo de dispositivo de 50 ohms, debe ser colocado en cada uno de los extremos del segmento troncal. Existen del tipo aterrizados y sin aterrizar, sin embargo, ambos se pueden instalar de manera adecuada.

Limitaciones de la red Ethernet con cable delgado:

* Máximo número de segmentos troncales: 3
* Máximo largo de cada segmento troncal: 300 mts.
* Máxima distancia de la red de punta a punta: 925 mts.

* Maximo número de estaciones conectadas a un segmento: 30
* Mínima distancia entre dos conectores tipo "T": 0.5 mts.

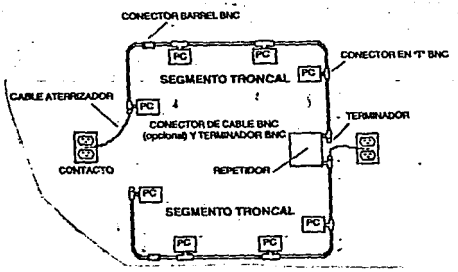


figura 3.1 Red Ethernet con cable delgado.

Redes de cable grueso

Hardware necesario para redes Ethernet con cable grueso:

Tarjeta de interfase Ethernet.

Transceiver. Cada estación de la red Ethernet que está conectada con cable grueso, se comunica a la misma red a través de un transceiver que se encuentra unido al segmento troncal o bus principal.

Cable grueso Ethernet. Tiene 0.4 pulgadas de diámetro y su impedancia es de 50 ohms. Este cable es utilizado para conformar el segmento troncal.

Cable del transceiver. Este cable es utilizado para conectar la estación de trabajo al transceiver.

Conector tipo DIX. Los conectores DIX macho y hembra son utilizados para unir la estación de trabajo al transceiver.

Conectores serie "N". Estos conectores se instalan en los extremos del cable grueso y permiter colocar un terminador serie "N".

Terminadores serie "N". Son utilizados para indicar el final del segmento troncal. Existen aterrizados y sin aterizar.

Limitaciones de la red Ethernet con cable grueso:

* Máximo número de segmentos troncales: 5
* Máximo largo de cada segmento troncal: 500 mts.
* Máxima distancia de la red de punta a punta: 2,500 mts.
* Máximo número de estaciones que pueden ser conectadas a un segmento: 100.
* Mínima distancia entre dos transceivers: 2.5 mts.
* Máximo largo del cable del transceiver: 50 mts.

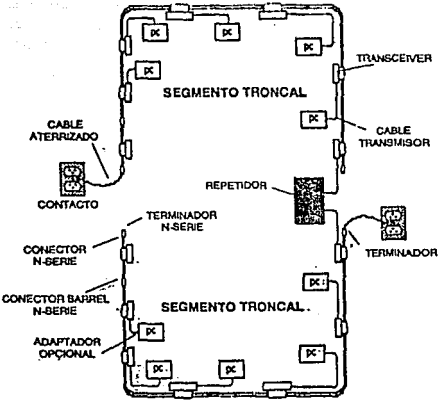


figura 3.2 Red Ethernet con cable grueso.

¿Como funciona Ethernet?

Ethernet es el ambiente de comunicación entre microcomputadoras más utilizado en la actualidad. Este tipo de red cumple con la norma IEEE 802.3, y probablemente es el que más industrias abarca en su instalación como son empresas de iniciativa privada, fábricas, sector educacional, sector gobierno y científico.

Ethernet como se explicó antes, puede usar cable delgado o grueso, cable UTP (Unshield Twisted Pair, Cable de Par Trenzado sin

blindaje) o fibra optica.

En una red Ethernet, cada estación se encuentra monitoreando constantemente la línea de comunicación con el objeto de transmitir o recibir sus mensajes. Si la línea presenta trafico en el momento que una estación quiere transmitir, la estación espera un periodo muy corto (milisegundos) para continuar monitoreando la red. Si la línea está libre, la estación transmisora envia su mensaje en ambas direcciones por toda la red. Cada mensaje incluye una identificación del nodo transmisor hacia el nodo receptor y solamente el nodo receptor puede leer el mensaje completo.

Cuando dos estaciones transmiten sus mensajes simultáneamente ocurre una colisión y es necesaria una retransmisión. Ya que el nodo aún esta monitoreando, sabe que ha ocurrido una colisión, es decir, es capaz de detectar la colisión, e intentará de nuevo la transmisión del mensaje.

El protocolo incluye las reglas que determinan cuánto tiempo tendrán que esperar los nodos o estaciones para realizar sus servicios nuevamente.

La velocidad de transferencia de Ethernet se dijo es de 10 Mbps, por lo contrario de lo que se pudiese pensar conforme al tipo de comunicación y operación, en el que se tienen tiempos de respuesta inconsistentes e impredescibles, su rendimiento es muy superior al de otro tipo de redes locales.

Cuando utilizamos cable UTP o fibra óptica, el concepto varia un poco. El concepto de bus lineal se altera, ya que en este tipo de cableado la topología no es precisamente un bus lineal sino tipo estrella.

Se parecería físicamente a las redes Arcnet o Token Ring, ya que los nodos se conectan a través de un centro de alambrado (wire closets) o concentradores y éstos podrían o no enlazarse a un bus de cable coaxial o de fibra óptica.

Lo que realmente esta sucediendo es que estos concentradores Ethernet de cable UTP internamente con su electronica llevan ese bus lineal para la conexión de los nodos.

Esta forma de conexión con cableado UTP día a día se introduce en el grueso de las instalaciones, ya que presentan una instalación más fácil, un monitoreo y administración de la red, así como el bajo costo del cableado y un crecimiento de la red mucho más sencillo.

Actualmente este tipo de redes bajo el cableado UTP y por la misma evolución de la tecnología está regida bajo el nuevo estandar 10BaseT.

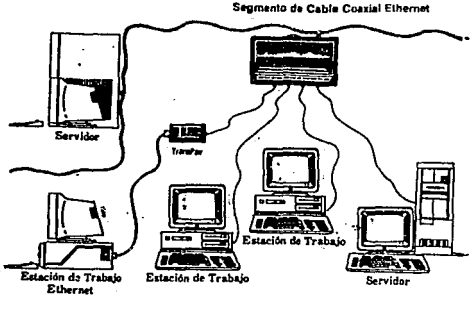


figura 2.8 Ethernet con cable UTP o cable telefonico.

3.2 ARCNET

ARCNET fue desarrollado por Datapoint en 1975 con el principal objetivo de que varios procesadores accedieran a un conjunto de discos, debido a que en aquel entonces los discos eran muy costosos. Aún si se agregaban las tarjetas Arcnet a los procesadores, era más económico que agregar un disco a cada procesador. El resultado fue un éxito, se creó una red muy eficiente y económica. Sus primeras instalaciones como redes verdaderas (compartiendo recursos, intercambiando información, etc.) se dieron hasta 1977 y desde entonces Arcnet es una de las preferidas.

La velocidad de transmisión de Arcnet es de 2.5 Mbps, ARCnet de alto rendimiento es de 2.5 Mbps, transmitiendo el doble de información por paquete, simulando así un trabajo a 5 Mbps, y ARCNET plus de 20 Mbps. Todas podrán convivir en la misma red trabajando a sus velocidades naturales.

La base instalada de ARCNET es de más de dos millones de nodos. ARCNET plus saldrá al mercado con sus primeras versiones comerciales a principios de 1992, esperando consolidarse como una de las redes más rápidas que existen.

A diferencia de Ethernet, las Redes Locales Arcnet operan bajo un protocolo de comunicación llamado Token Passing, el cual está basado en un esquema libre de colisiones y en una topología original en forma de anillo pero con una pequeña variante que hace ver a la red con una forma de tipo estrella o conjuntos de estrellas. (Figura 3.4)

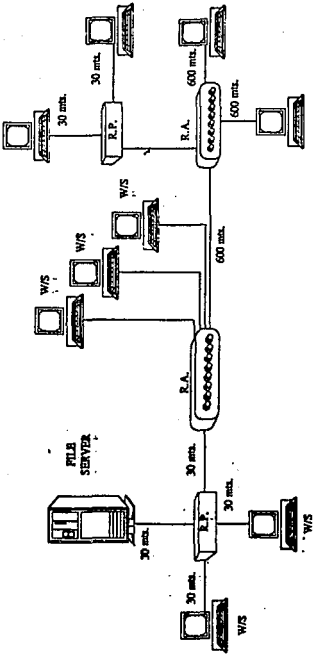


Figura 3.4. Red Arcnet

Hardware para redes Arcnet:

Tarjeta de interfase Arcnet. Esta tarjeta es colocada en [illegible] de cada una de las estaciones de trabajo que conforman la

Repetidor activo. (R.A.) Este tipo de dispositivos cuenta [illegible]ocho puertos de salida para interconectarse con otros repetidor[illegible]con estaciones de trabajo. Los repetidores activos tienen la [illegible] de amplificar y rutear la señal.

Repetidor pasivo. (R.P.) Este repetidor cuenta con cuatro [illegible]rtos de salida usados para conectarse a otros repetidores [illegible]tipo activo o a estaciones de trabajo. No permite este [illegible] de dispositivos conectarse a otros repetidores de tipo pasiv[illegible]

Cable Arcnet. Es un cable coaxial conocido como RG-62/U, [illegible]ual tiene 0.2 pulgadas de diámetro y una impedancia de 93 ohms

Conector BNC tipo plug. Este tipo de conectores son ut[illegible]zados para interconectar el cable Arcnet con las estaciones de t[illegible]jo y con los repetidores.

Limitaciones de la Red Arcnet.

* Un puerto activo de un repetidor puede conectarse a un puerto activo de otro repetidor o bien, a una estación de trabaj[illegible]que se encuantre a una distancia máxima de 600 mts.
* Un puerto activo de un repetidor puede conectarse a un puerto pasivo de otro repetidor hasta una distancia máxima de 30 [illegible].
* Es posible conectar un puerto de tipo pasivo a una est[illegible]ón de trabajo que se encuentre a una distancia máxima de 30 mts.
* Es posible conectar hasta un máximo de 10 repetidores en[illegible]rie a lo largo de la red, lo que permite tener una distancia m[illegible]ma de 6.000 mts. entre estaciones de trabajo en los extremos de [illegible]red.

* No pueden conectarse puertos pasivos de un repetidor con puertos pasivos de otro repetidor.

* Dos puertos del repetidor nunca pueden conectarse entre ellos.

* Algunos repetidores cuentan con una salida adicional llamada *daisychain*. esta salida permite conectar en cascada a varios repetidores activos sin tener que desperdiciar ningun puerto activo.

¿Como funciona Arcnet?

La Red Arcnet utiliza el protocolo de acceso Token Passing y la topologia de anillo, con cableado en forma de estrella.

El paquete de información viaja a través de la Red de un nodo a otro, en forma ascendente. Es decir, el paquete de informacion *TOKEN*, por ejemplo, en una red de cuatro nodos primero parte del primer nodo pasando por cada uno de los demás (2,3,4) y regresa nuevamente al número uno atendiendo a cada nodo según lo solicite.

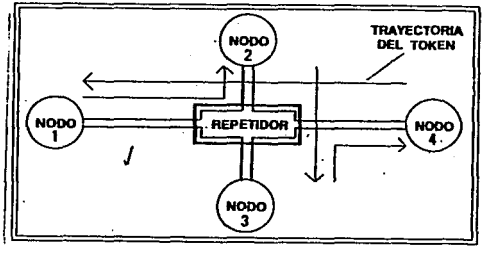


Figura 3.5 Trayectoria que sigue el Token en una Red Arcnet

Para explicar esto imaginese un tren que tiene que llegar a diferentes destinos. En cada uno, entregará o recogerá algun paquete el cual ostenta una etiqueta de quién la envia y para quién es.

El tren (token) viajará a través de esa via (cableado) primero hacia el destino (nodo) marcado como primer número (nodo uno); a continuación se dirigirá al siguiente destino que tendrá un número superior ascendente al cual ya visitó. Después de haber recorrido todos los destinos (nodos), regresará al primero para reanudar con ese mismo viaje. Si se le agrega un nuevo destino (nodo) el operador del tren (sistema operativo) revisará en qué número de importancia está ese destino adicional para atenderlo conforme a su nueva ruta. En ARCNET todo esto se realiza a una velocidad de 2.5 Mbps dentro del cableado.

La Red Arcnet funciona en realidad como un anillo modificado, ya que recorrerá los nodos en forma de anillo por ser un ciclo de atención a cada uno de ellos. Pero esto lo hará no en la posición física en que se encuentran,sino en el orden lógico que se le dé a cada uno. Por tal razón, cada tarjeta lleva un numero asignado de nodo, el cual tiene que ser distinto a cualquier otro en la red. Este número de nodo (node adress) se direcciona físicamente a cada tarjeta. Si existiesen dos nodos con números iguales en la red, como consecuencia, habría fuertes conflictos en la comunicación de ésta, inclusive no podría existir respuesta en nodo alguno.

Cada mensaje incluye una identificación del nodo fuente y del nodo destino y sólo el destino puede leer el mensaje completo. En este tipo de red no es necesario que cada estación regenere el mensaje

antes de transmitirlo al siguiente. Todas las estaciones tienen la capacidad de indicar inmediatamente si pueden o no aceptar el mensaje y, además, reconocen cuando ya se recibió.

Este tipo de red ARCNET existe tanto en cableado coaxial como en cableado telefónico, siendo el primero el mas utilizado.

Físicamente sería conflictivo tender una red de este tipo ya que se tendría que cerrar ese anillo y agregar o eliminar un nodo sería muy complicado. En la actualidad, este tipo de red se maneja por centros de alambrado o repetidores (HUBs, los que se encargan de hacer ese anillo.

Este tipo de red se recomienda ampliamente cuando el trabajo o el procesamiento en la misma no es muy fuerte. El tráfico de la red no es tan importante cuando se utilizan procesadores de palabra y/u hojas de cálculo. Por el contrario es muy importante cuando se realizan procesos de compilación y/o manejo de base de datos.

3.3 TOKEN RING

La Red Token Ring, estandarizada por el IEEE 802.5, es una implementacion comercial del "Anillo de Zurich" desarrollado por el centro de investigaciones de IBM en Zurich, a finales de los años 70. Token Ring es un anillo lógico cableado como estrella física y opera con banda base a velocidades de transmisión de 4 Mbps o 16 Mbps. Token Ring de 16 Mbps puede convivir con 4 Mbps, pero opera a 4 Mbps debido a que Token Ring es inherentemente una red sincrona.

La base instalada de Token Ring es de casi dos millones de nodos y está creciendo rápidamente debido al fuerte impulso que le ha dado IBM y por la serie de fabricantes que se han apegado a producir Token Ring y software para él.

De manera similar a las redes Arcnet, las redes Token Ring están constituidas por un protocolo de comunicaciones Token Passing y topologia de tipo anillo. (figura 3.6)

Hardware necesario para Redes Token Ring:

Tarjetas de interfase Token Ring.

Centros de alambrado. Conocidos como unidades MAU (Multi-station Access Unit). Este tipo de dispositivos cuentan con ocho puertos de salida del tipo RJ-45 o UTP (Unshield Twisted Pair)Par torcido desprotegido para los conectores RJ-45, o bien, ocho puertos del tipo 802.5 o STP (Shield Twisted Pair)Par torcido protegido para conectores 802.5, para hacer la conexión entre estaciones de trabajo.

Las unidades MAU cuentan adicionalmente con una salida Ring-in y una salida Ring-out, utilizadas para conectarse con otras unidades

similares en cascada.

Existen unidades MAU inteligentes y no inteligentes. las primeras son las mas utilizadas por su gran capacidad de deteccion y correccion de errores en el anillo por medio de un software analizador de red.

Centros de alambrado para grupos de trabajo. También conocidos como Centros de Alambrado Satelitales. Este tipo de dispositivos tiene cuatro puertos de salida para interconectar estaciones de trabajo y un puerto de entrada Ring-in para recibir un cable proveniente de una unidad MAU principal.

Los Centros de Alambrado Satelitales son comunmente utilizados para unir en red a diferentes grupos de trabajo con un menor costo en la implementación.

Cable para Token Ring. Escencialmente existen dos tipos de cable: UTP y STP.

UTP. (Unshield Twisted Pair) Par torcido no protegido para usarse con conectores RJ-45. Un ejemplo de este tipo de cable es el conocido como Belden AWG-24.

STP. (Shield Twisted Pair) Par torcido protegido para usarse con conectores 802.5. El cable IBM tipo 1 es un ejemplo de este cable.

Conectores 802.5. Estos conectores son usados para interconectar el cable STP con las estaciones de trabajo y las unidades MAU.

Conector RJ-45. Estos conectores son usados para interconectar el cable UTP con las estaciones de trabajo y las unidades MAU.

Limitaciones de la Red Token Ring:

A medida que se incrementa el número de dispositivos MAU de tipo principal o satelital, se ve decrementada la longitud maxima de

cable utilizable entre la estacion de trabajo y el MAU al que se encuentra instalada dicha estacion.

Asi por ejemplo, el cable UTP permite distancias del MAU a la estación de trabajo del orden de 77 a 259 metros dependiendo del numero de unidades que se utilicen y el cable STP permite distancias que oscilan entre los 187 y 365 metros.

Los puertos Ring-in solo pueden conectarse a puertos Ring-out y viceversa.

Los puertos 802.5 de los dispositivos MAU solo pueden conectarse a Servidores de Archivos o a estaciones de trabajo. Los puertos RJ-45 de un MAU pueden, adicionalmnte, conectarse a MAU Satelitales.

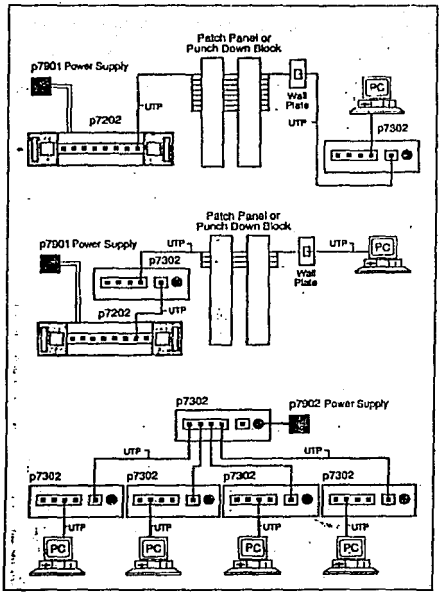


Figura 3.d Red Token Ring con un backbone de 4/16 Mbps.

ESPACIFICACIONES TECNICAS

ETHERNET

NAE1000 Tarjeta Ethernet para Macintosh SE

NAE2000 Tarjeta Ethernet para MAcintosh II

Se recomiendan como estaciones de trabajo, equipo del tipo PC, PC-XT,AT, 386 y PS/2 de IBM en todos sus modelos, así como las estaciones de trabajo Acer.

ETHERNET (NE-1000)

* Protocolo de Red CSMA/CD
* Velocidad de transmisión 10 Megaa-Bits
* Distancia Máxima total 300 mts. sin amplificar
* Capacidad de memoria (Buffer) 8 KB
* Bus IBM PC, XT, AT compatible
* Tipo de cable RG-58 Coaxial
* Tipo de conector BNC 8 Tierra aislada
* Condiciones ambientales 0 - 50 grados centigrados
* Humedad 10 a 90 % no condonsada
* Requerimientos de potencia + 5 VAC +/-5% AT 1.0 Amp
* Interruptores 2,3,4 ó 5 seleccionable

ETHERNET + (NE-2000)

Todo es igual excepto:

* Capacidad de memoria 128 KB estándar
* Condiciones ambientales 0 - 55 grados centigrados
* Requerimientos de potencia + 5 VAC +/-5% AT 2.0 Amp.

Esta red se recomienda para trabajos pesados con mucho tráfico en el canal de comunicaciones y con acceso a disco duro constantes. Existen 3 tipos de tarjetas que apoyan esta configuración: NE-1000 para estaciones de trabajo del tipo PC/XT,AT y 386, NE-2000 para servidores del tipo AT y 386 y NE/2 para la arquitectura microcanal IBM PS/2

ARCNET

* Protocolo de Red Token Passing
* Velocidad de transmisión 2.5 Mbps
* Distancia maxima total 6 Km.
* Capacidad opcional hasta 8 KB de memoria PROM
* Tipo de cable RG-62U 93 ohms (Coaxial)
* Tipo de conector BNC 8 Tierra aislada
* Direccionamiento por switch tipo DIP (0-255)
* Condiciones ambientales 0 - 70 grados centigrados
* Requerimientos de potencia + 5 VAC +/-5% AT 1.0 Amp.
* Incluye:
  Slot corto
  Led indicador de actividad
  Selector de número de nodo externo

Esta red es de fácil instalación y se encuentra ya muy probada en México. Se recomienda para instalaciones que requieran velocidades medias de transmisión, utilizando servidores del tipo PC-AT, 386 o PS/2.

Como estaciones de trabajo se pueden conectar XT,AT,386 ó PS/2.

TOKEN RING

* Protocolo de red Token passing
* Velocidad de transmisión 4 Mbps
* Distancia máxima total 6 kms.
* Método de comunicación tarjeta-CPU DMA (Direct Memory Access)
* Direccionamientos 10 bytes de espacio en registros I/O
* Memoria EPROM con jumpers seleccionables
* Tipo de conector RJ-45 para cable UTP
* Interruptores 3,4,5,6,7,9,10,11 ó 12
* Condiciones ambientales 5-50 grados centigrados
* Requerimientos de potencia +5 VAC a 1.5 Amp.

Esta topología ofrece la mejor opción precio/rendimiento en la industria. Opera con el estandar IEEE 802.5 y las redes IBM Token Ring Recomendable para instalaciones con cable UTP.

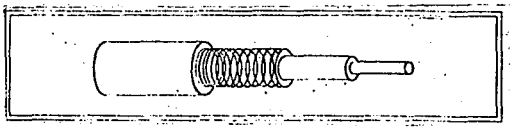
CAPITULO IV
CABLEADO

Las redes locales utilizan tres tipos de cable. Cada cable tiene sus ventajas. Los tipos de cables utilizados comunmente son:

- Coaxial
- Cable telefónico UTP/STP
- Fibra Optica

4.1 CABLE COAXIAL

El cable coaxial está compuesto de un alambre (un conductor) cubierto de otro conductor tubular que actúa como tierra. El conductor y la tierra están separados por un aislante, con todo el cable protegido por un jacket aislante en la parte exterior.



El cable coaxial puede ser de varios tipos y anchos. El cable coaxial más grueso transporta una señal a distancias más largas que el cable delgado. El cable grueso es más caro y menos flexible. En las instalaciones en que el cable tiene que ser colocado en lugares en donde ya existen canales para cableado,

conductos con espacios limitados o por esquinas, el cable delgado puede ser utilizado.

El cable coaxial es el medio físico más comunmente utilizado en redes. ofrece excelentes caracteristicas de aislamiento que minimizan las interferencias que pueden provocar los campos electromagnéticos.

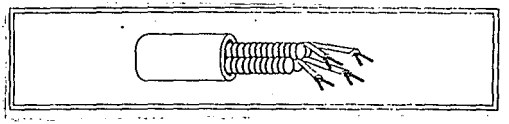
El cable coaxial permite distancias de transmision entre los 185 y 880 mts.

Ventajas:

- Transmite voz, videos y datos
- Se instala facilmente
- Compatible con ETHERNET y ARCNET
- Ancho de banda de 10 Mbps
- Distancia hasta de 800 metros sin necesidad de repetidores.
- Buena tolerancia de interferencias debidas a factores ambientales.

4.2 CABLE TELEFONICO

El cable telefónico está formado por dos alambres que se encuentran aislados y torcidos. El par torcido esta protegido por una capa exterior aislada llamda "jacket".



Este tipo de cable se divide en dos:

PAR TRENZADO BLINDADO. Ofrece excelentes caracteristicas de aislamiento permitiendo distancias de transmisión hasta de 300 mts. Una de las redes con mayor utilización de este cable es Token Ring y es quien más ha sabido aprovecharlo. pues en un sólo cable con dos pares permite la transmisión en ambos sentidos.

PAR TRENZADO SIN BLINDAJE. Es desde luego el cable más económico. pero el que se contamina con más facilidad pues no cuenta con blindaje. Generalmente se utiliza para redes donde los nodos se encuentran muy cercanos. no más de 100 mts. En Estados Unidos se

está volviendo cada vez mas popular, debido a su bajo costo, la facilidad de instalación y a que es el mismo cable utilizado para la red telefonica. Sin embargo no garantiza seguridad para transmision a grandes distancias.

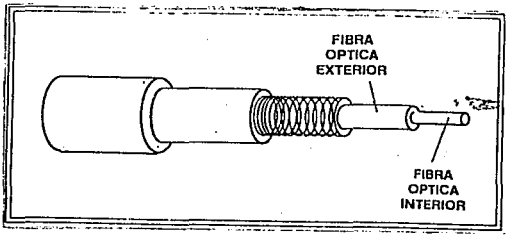
Ventajas:

- Tecnologia conocida
- Fácil y rápido de instalar
- Compatible con ETHERNET, TRN (4 Mbps)
- Ancho de banda de 10 Mbps
- Distancias hasta de 110 mts.
- Muy económico
- Buena relación precio/rendimiento
- Regular tolerancia a interferencias debidas a factores ambientales.

4.3 FIBRA OPTICA

La fibra otica es utilizada para grandes distancias y alta capacidad de aplicaciones de comunicacion y especialmente cuando el ruido y la interferencia eléctrica son importantes.

Un cable de fibra óptica consiste en una fibra muy delgada hecha de dos tipos de vidrio. una para la parte interior y otra para la exterior. Los dos vidrios tienen diferentes indices de refracción. Esta combinación previene que la luz penetre en una parte de la fibra hasta la parte exterior. La fibra está protegida por una cubierta para darle mayor integridad estructural.



Es el cable más costoso de todos los anteriores, pero también el más seguro. Ofrece una inmunidad completa a campos electromagnéticos e interferencias y es posible transmitir datos a casi 3 Km. de distancia. Una red con fibra óptica es muy costosa debido a los altos costos de las tarjetas controladoras y a la propia instalacion de la fibra.

Ventajas:

- Aplicaciones de alta velocidad
- No genera señales eléctricas o magnéticas
- Inmune a interferencia y relámpagos
- Puede propagar una señal, sin necesidad de un amplificador, a distancias muy largas
- Ancho de banda de 200 Mbps
- Compatibilidad con ETHERNET, TRN (16 Mbps)
- Excelente tolerancia a factores ambientales
- Ofrece la mayor capacidad de adaptación a nuevas formas de rendimiento.

Consideraciones que deben tomarse en cuenta al cablear.

Cuando debemos tomar la decision de qué tipo de cable debemos utilizar, surgen invariablemente las siguientes preguntas: Escoger el mas barato o el más caro?, ¿el que me proporciona mas velocidad o el mas seguro?, ¿debo sacrificar velocidad y ahorrar dinero?.
Estas y otras cuestiones hacen que el cableado pase de ser algo relativamente simple a ser una decisión compleja y fuente de muchos problemas en las redes locales. El cable hace difícil el aislar un circuito, no todos soportan las velocidades de transmisión de las computadoras. Añadir cable puede ser muy enredoso y llevar días el hacerlo, cambiar los nodos de ubicación implica mayor costo en cable y una cuidadosa planeación.
La mayoría de los analistas preven una tendencia a utilizar cable de par trenzado básicamente por su facilidad de instalación y bajo costo.
Sin embargo, no todos están utilizando par trenzado y sería más lógico pensar que la fibra óptica es el cable del futuro. Los avances tecnológicos mas recientes hacen de la fibra un medio ideal de transmisión pero sólo puede y debe ser usada por grandes compañías que necesitan el ancho de banda y la calidad de la fibra óptica. Para el resto de los usuarios "comunes" el cable coaxial y el par trenzado son la solución más viable.
Existen seis factores que hacen superior al par trenzado sobre el coaxial:
Tamaño El más pesado de los cables de par trenzado blindado es mas delgado que el mas delgado del tipo coaxial.

Peso. El cable de par trenzado blindado pesa aproximadamente 3 kilos por 30 metros de cable. Un cable coaxial comun como el RG-62 pesa 20 kilos por 30 metros de cable. Uno de los pocos cables de par trenzado que son pesados es el IBM tipo 1 que pesa 30 kilos por 30 metros de cable.

Flexibilidad. Se puede doblar el cable de par trenzado más fácilmente que el coaxial lo que facilita la instalación.

Instalacion. El cable de par trenzado tiene varias ventajas sobre el cable coaxial en lo que se refiere a la instalación. Una ya mencionada es la flexibilidad. La otra es el peso. Una de las más grandes ventajas del par trenzado es que es más simple y sencillo de conectar a cajas de distribución. Esto debido a que es utilizado por la industria telefónica, la cual ha desarrollado herramientas especiales para ahorrar tiempo de instalación. Cuando se utilizan "jacks" modulares la instalación se simplifica aún más.

Una ventaja obvia, se ve cuando no se necesita instalación alguna. Muchos edificios tienen cable de par trenzado ya instalado y sin ser usado, ya que las compañías de teléfono así lo planean.

Precio. El par trenzado sin blindaje cuesta aproximadamente la mitad que el coaxial. Sin embargo no hay mucha diferencia de precio entre el par trenzado blindado y el coaxial.

En cuanto a las ventajas que presenta el cable coaxial podemos mencionar las siguientes:

Capacidad. El cable coaxial tiene un mayor ancho de banda, y por lo tanto pueden transmitir mayor información a velocidades mas altas. El cable coaxial es capaz en funcionar en banda ancha mientras que con el par trenzado no es posible. Si se necesitan varios canales de información en un solo cable, el par trenzado no es una solución factible.

Distancia. La impedancia del cable coaxial le permite transmitir señales a mayores distancias.

Tecnologia probada. El cable coaxial se ha utilizado desde el inicio de las LAN's y la mayoria de los técnicos están mucho más familiarizados con este cable.

Al decidir que tipo de cable vamos a utilizar, un factor que parece ser muy importante es la velocidad de transmisión. Sin embargo, hay que tener en cuenta que la velocidad también depende del procesador y de la aplicación que estemos corriendo.

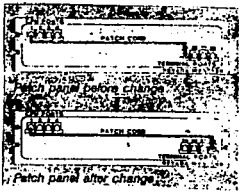
ESQUEMAS MODULARES DE CABLEADO

Al planear la instalación de la Red. debemos tener mucho cuidado de la instalacion fisica del cable. Si vamos a utilizar cable de par trenzado previamente instalado en el edifico. nuestro problema será mínimo. Pero si no existe una instalación previa podemos vernos literalmente "enredados" en una maraña tipo espagueti. Si existe una falla y el cable no tiene un orden. nos puede llevar mucho tiempo localizar quien conecta con quien y en donde. Lo mismo sucede cuando se desea cambiar de ubicación alguna maquina.

Para solucionar este problema se creo el concepto de cableado modular. Definido de una manera simple. se trata de un sistema tipo central telefónica, donde se conectan y desconectan una serie de cables según la necesidad. Sin embargo, no es sólo eso. Se trata de un sistema que utiliza paneles de conexión y gabinetes de alambres para facilitar cambios en los nodos sin necesidad de volver a cablear. En seguida se presenta un ejemplo desarrollado por Nevada Western cabling company. el cual ofgrece un sistema de cableado modular. La compañía introdujo este sistema en respuesta a un estudio realizado en donde se descubrió que el 50 % de las computadoras eran reubicadas dentro del primer año.

Como funciona el sistema.

En el diagrama se muestra el puerto # 1 del CPU conectado a la terminal # 25. Si la persona usando la terminal # 28 necesita conectarse al puerto I/O del CPU



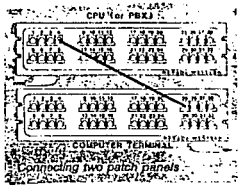
simplemente se mueve el enchufe modular al puerto deseado.

En la mayoria de los sistemas, se utiliza mas de un panel de conexión a menudo solo dedicados a CPUs y otros dedicados a conectar terminales.

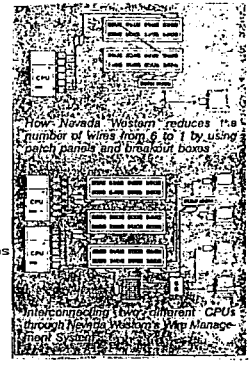
El "parchado" o conexión de cables se logra con un cordón modular con conectores en ambos extremos. Salir del panel a la terminal es tan fácil como entrar al CPU.

La conversión de un sistema de conectores en lugar de un sistema de cable de par trenzado reduce el número de cables a utilizar de 6 a 1.

Si añadimos más paneles de conexión, podemos preveer futuras ampliaciones o cambios al sistema y así evitar el problema de costos y pérdida de tiempo al cambiar nodos o agregar nuevos.



Connecting two patch panels


How Navada Western reduces the number of wires from 6 to 1 by using patch panels and breakout boxes

Interconnecting two different CPUs through Nevada Western's Key Management System

GUIA DE CONSEJOS PARA EL CABLEADO

1.- Evite interferencia eléctrica. Evite colocar sus cabl
de conductores de electricidad, equipo o motores elé
Tambien evite las fuentes de calor como pueden ser tu
agua caliente. Las condiciones del cable varian con el
se aplica, evite colocarlos cerca de equipos de radar.

2.- Coloque el cable lejos de luz fluorescente. La luz
fluorescente puede causar un zumbido de 60 ciclos el cu
causar interferencia en la señal, especialmente en
algunos cables coaxiales o par trenzado sin blindaje.

3.- No pise el cable. No instale su cable bajo alfombra
algún lugar donde las personas caminen constantemente. Es
provocar un cambio en el ancho del cable y un consiguient
en su impedancia lo que a la larga causa problemas.

4.- El cable no es infinito. Adhierase a las especificaci
su equipo y no trate de aumentar la distancia entre term
Hacer lo contrario sólo provoca una reducción en la velo
tiempo de respuesta.

5.- Los diagramas son importantes. Asegurese de que la pers
hace la instalacion dibuje un digrama que muestre claramen
está colocado el cable y cualquier otra información rel
Mantenga siempre una copia en un lugar donde puede consult

caso necesario.

6.- Etiquete todo. No es suficiente tener un buen plan y un buen diagrama si al momento de hacer alguna modificación nos encontramos con una "bola" de alambres y no sabemos cual es cual. Cada cable debe tener una identificación en ambos extremos. De igual manera deben etiquetarse los paneles y cajas de conexión en caso de que existan.

7.- Tenga personal capacitado. Si el cableado lo realiza una compañía externa, alguien de su oficina debe trabajar junto con ellos para que posteriormente esa persona explique el funcionamiento del sistema.

8.- Trate el cable con cuidado. No juegue a Tarzan con los cables, nunca los jale ni trate de doblarlos más allá de su flexibilidad propia. En algunos edificios débiles puede inclusive dañar la pared si jala el cable más de lo debido.

9.- Mire hacia adelante. Anticipe los cambios de nodos o el crecimiento de los mismos aún a áreas que no son usadas. Es mejor hacer un gasto extra al momento de cablear y no toparse con limitantes en el sistema.

CAPITULO V

PROTOCOLOS DE COMUNICACION

5.1 MODELO JERARQUICO DE PROTOCOLOS

Las redes de computadoras surgieron para hacer posible compartir de forma eficiente los recursos y en general esos recursos son heterogéneos: los equipos de fabricantes tienen características diferentes, utilizan y ejecutan software con características específicas y distintas para las aplicaciones deseadas por los usuarios, y manipulan y producen datos con formatos incompatibles. Asimismo, equipos idénticos de un único fabricante, que se integran en aplicaciones distintas, pueden presentar características heterogéneas.

Esa heterogeneidad de los sistemas beneficia al usuario, que no está así limitado a un único tipo de sistemas para sus distintas aplicaciones. Así, se puede seleccionar el sistema que mejor se adapte a las condiciones de aplicación que interesen y al presupuesto disponible. Por otro lado, tal heterogeneidad dificulta considerablemente la interconexión de equipos de fabricantes diferentes.

La interconexión de redes, a su vez, contribuye a hacer más difícil el problema, ya que: puede haber redes diferentes con servicios de transmisión diferentes, que requieran interfases diferentes. Es necesario, pues, una manera por la cual, el problema de las heterogeneidades no haga inviable la interconexión de sistemas distintos.

La incompatibilidad de equipos y/o redes fue inicialmente resuelta

a través del uso de convertidores, como se muestra en la figura 5.1.

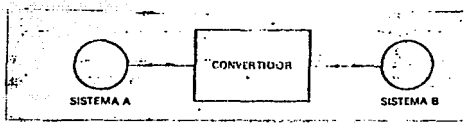


Figura 5.1 Interconexion de los sistemas A y B

En esta figura, los sistemas A y B son incompatibles. El convertidor interpreta la información originaria de uno de los sistemas y transfiere la información al sistema destinatario, traduciendo a una forma entendible por éste. Por lo tanto, el uso de convertidores es deficiente. Son lentos e inadecuados para solucionar incompatibilidades a nivel de aplicaciones ya que sería necesario su integración en el propio sistema operativo de cada uno de los dos equipos involucrados.

En 1977, la Organización Internacional de Normalizaciones (ISO) vio la necesidad de normalizar la interconexión de sistemas heterogéneos y creó un subcomité (SC16) para estudiar el problema. El objetivo del SC16 era definir normas para la interconexión de sistemas abiertos (Open System Interconnection,OSI).

Ya en 1978 el SC16 sugirió una arquitectura estratificada en categorías para que se desarrollase a partir de ahí una norma para el modelo de arquitectura que sirviera de soporte para el desarrollo de protocolos normalizados. A mediados de 1979 el desarrollo del modelo de arquitectura estaba terminado y recibió

el nombre de modelo de referencia para la interconexión de sistemas abiertos (RM-OSI). A finales de 1979 el comité técnico 97 (de procesamiento de datos) de la ISO al cual estaba subordinado el SC16 acato al RM-OSI como base para el desarrollo de protocolos. En torno a mayo de 1983, el RM-OSI era oficialmente aprobado por la ISO como una norma internacional para la interconexión de sistemas abiertos a través del documento ISO 7498.

El término abierto no se aplica a ninguna implementación, tecnología o interconexion particular de sistemas, pero si a la adopción de normas, es decir, cualquier sistema que adoptando las normas del SC16 pueda interconectar con cualquier otro sistema que obedezca a las mismas normas. El término OSI se refiere, pues, a las normas para la transferencia de información entre terminales, computadoras, personas, redes, procesos, etc., que esten abiertos a los demás, con el propósito de transferir información a través del uso de las normas aplicables. Se dice que un sistema que obedece a las normas OSI en su comunicación con otros sistemas, es un sistema abierto.

Estructura en capas.

Cualesquiera que sea el tipo de comunicación entre sistemas, es necesaria la observación de un grupo de reglas. Así, en una conversación telefónica usted "oye y habla" lo que su interlocutor "habla y oye". Si usted no entiende lo que le hablan, interrumpe y pide que le "repitan" lo que le "hablaron". Todo este es una serie de reglas implícitas que norman nuestra comunicación. En la terminología de las redes de computadoras, este conjunto de reglas

recibe el nombre de *protocolo*.

En la elaboración de protocolos para redes, hay varios aspectos técnicos y operacionales que dificultan un poco su diseño y entendimiento. Todo tiene que ser cuidadosa y correctamente especificado para que los diferentes procesos de aplicacion puedan cooperar de forma armónica y compatible en el procesamiento de tareas distribuidas por la red.

De acuerdo a Andrew Tanenbaum, Julio César fue el primero en enunciar la clave para reducir la complejidad de diseño de redes de computadoras: "divide y conquista". El principio es proyectar una red con un conjunto jerárquico de capas o niveles, cada una superpuesta en la capa inferior. Reduciendo el diseño global de una red al diseño de cada una de las capas, se simplifica considerablemente el trabajo de desarrollo y de mantenimiento. El diseño de una capa se restringe al contexto de esa capa y supone que los problemas externos a ese contexto ya están debidamente resueltos.

La arquitectura del RM-OSI está construida siguiendo un proceso jerárquico donde cada capa utiliza los servicios suministrados por la capa inmediatamente inferior para dar un servicio de "mejor calidad" a la capa superior. No interesa a una determinada capa cómo las demás realizan o implementan sus servicios; sólo importa lo que la capa ofrece como servicio, es decir, las demás capas son verdaderas "cajas negras". En la arquitectura jerárquica una capa N apenas sabe que existe una capa N - 1 prestadora de determinados servicios y, una capa N + 1 que le solicita servicios. La capa N no se apercibe de las capas N + 2, N + 3, etc.

La capa N solo se preocupa de utilizar los servicios de la capa N - 1 y de realizar sus servicios a la capa N + 1 independientemente de su protocolo. Es así que una capa puede ser alterada sin cambiar a las demas (facilitando el mantenimiento) sin que los servicios que se prestan sean modificados. Y ocurre también que otras (o nuevas) aplicaciones puedan ser implementadas, en la capa apropiada, aprovechando los mismos servicios ya efectuados por las otras capas.

La arquitectura del RM-OSI fue desarrollada a partir de tres elementos básicos:

a) Los procesos de aplicación existentes en el entorno OSI.

b) Las conexiones que unen los procesos de aplicación y que les permiten transferir informaciones.

c) Los sistemas.

La figura 5.2 muestra estos tres elementos.

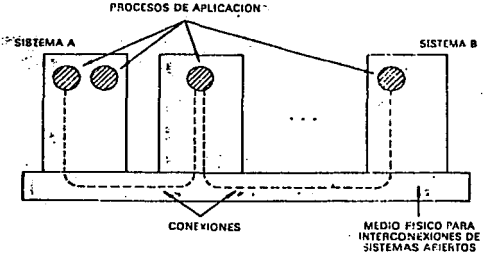


Figura 5.2 Elementos basicos del OSI

La representación de la arquitectura de RM-OSI utilizada por el SC16 es mostrada en la figura 5.3, donde las capas sucesivas son representadas con una secuencia vertical, con los medios físicos para la interconexión de sistemas abiertos (OSI) debajo.

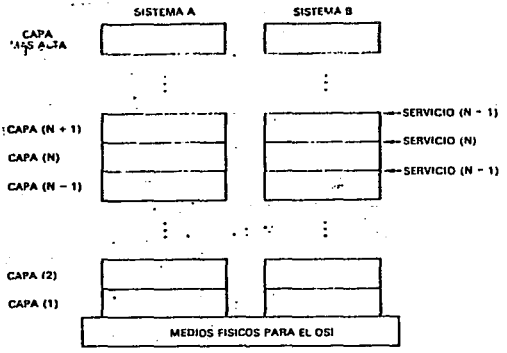


Figura 5.3 Método del SC16 de la ISO para la representación de la arquitectura jerárquica de capas.

Las siete capas del RM-OSI de la ISO.

La propia ISO afirma que sería difícil probar que son siete capas

las que forman la "mejor" arquitectura para una interconexion de sistemas abiertos. Pero por otro lado la ISO describe en la cláusula 5 del documento "Computer Communications Review", trece principios "arquitectónicos" que se aplicaron para llegar a las siete capas de la arquitectura del RM-OSI. Esos principios son:

i) no crear un número muy grande de capa a fin de no dificultar el trabajo de descripción e integración de esas capas.

ii) demarcar dos capas adyacentes en un punto donde la descripción de servicios pueda ser pequeña y minimice las interacciones entre las capas.

iii) cerrar capas separadas para trato de funciones que sean claramente diferentes en el proceso ejecutado o con la tecnología utilizada;

iv) las funciones similares deben ser agrupadas en una misma capa;

v) demarcar dos capas adyacentes en un punto donde la experiencia haya demostrado ser satisfactoria.

vi) crear una capa de funciones fácilmente localizadas (en la capa) a fin de que una capa pueda ser totalmente rediseñada y sus protocolos alterados sustancialmente para aprovecharse de los nuevos avances en la tecnología de software y hardware, sin alterar los servicios e interfases con las capas adyacentes;

vii) crear una capa que pueda ser de utilidad, en el futuro, para la normalización de la interfaz correspondiente.

viii) crear una capa donde exista un nivel diferente de abstracción en el manejo de datos, por ejemplo, morfología, sintaxis, semantica.

ix) posibilitar la modificación de funciones o protocolos dentro de una capa sin afectar a las otras capas;

x) crear para cada capa interfaces sólo con las capas inferior y superior.

xi) subagrupar y organizar las funciones para formar subcapas dentro de una capa en los casos en los que sea necesario para los distintos servicios de comunicación;

xii) crear, donde sea necesario, dos o más subcapas con

funcionalidad comun, y por tanto minima, para permitir el funcionamiento de la interfaz con capas adyacentes:

(iii) posibilitar la adopcion de alguna(s) subcapa(s).

La figura 3.4 muestra un esquema de las siete capas de la arquitectura OSI.

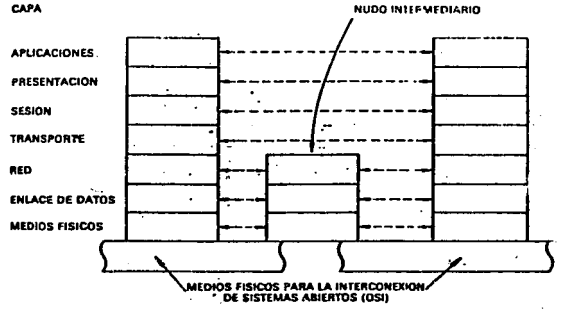


figura 3.4 Las siete capas de la arquitectura OSI.

5.2 LA CAPA FISICA

El propósito de la capa física consiste en transportar el flujo original de bits de una máquina a otra. Los métodos físicos más utilizados son los vistos anteriormente: cable coaxial, telefónico y fibra óptica. Así como también los conectores, interfases, etc. Las bases matemáticas para la comprensión y el diseño de estos medios físicos de transmisión, así como la norma que rige a los mismos es lo que trataremos más adelante.

Bases teoricas para la comunicacion de datos.

La información puede transmitirse por medio de cables, este proceso tiene lugar cuando se varían algunas de las propiedades físicas como su voltaje o corriente; al representar el valor de este voltaje o corriente únicamente como una función del tiempo f(t), puede entonces modelarse el comportamiento de la señal y analizarse en forma matemática.

Analisis de Fourier.

A principios del siglo XIX, el gran matemático francés Jean Fourier demostró que cualquier función que se comporte de forma razonablemente periodica, como por ejemplo g(t), de periodo T, puede construirse mediante la suma de un número posiblemente infinito de senos y cosenos:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \operatorname{sen}(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t) \qquad \ldots\ldots (5.1)$$

en donde f = 1/T representa la frecuencia fundamental y "a" y "b" son las amplitudes correspondientes al seno y coseno de los armonicos enésimos. A esta composición se le conoce como Serie de

Fourier. Una función puede reconstruirse a partir de la serie de Fourier: es decir, si se conoce el periodo T y se dan las amplitudes, la función original, con respecto al tiempo, puede calcularse realizando las sumas de la ecuación 5.1.

Una señal de datos que tiene una duración finita, puede manejarse suponiendo que aquella se repite una y otra vez.

Las amplitudes "a" para una g(t) dada pueden calcularse al multiplicar los dos lados de la ecuación 5.1 por el término sen(2πkft) y después integrarlo desde 0 hasta T. Dado que:

$$\int \text{sen}(2\pi kft)\ \text{sen}(2\pi nft)\ dt = \begin{cases} 0 \Rightarrow n \neq k \\ \\ T/2 \text{ para } k = n \end{cases}$$

sólo un término de la ecuación sobrevive: y éste es "a". La suma "b" desaparece por completo. De la misma manera, al multiplicar la ecuación 5.1 por cos(2πkft) e integrandola entre 0 y T, se puede obtener el valor de b . El valor de c se obtiene, precisamente, al integrar ambos lados de la ecuación tal y como aparece. El resultado de la realización de estas operaciones es el siguiente:

$$a_n = \frac{2}{T}\int_0^T g(t)\,\text{sen}(2\pi nft)\,dt,\quad b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi nft)\,dt;\quad c = \frac{2}{T}\int_0^T g(t)\,dt$$

Senales limitadas por ancho de banda.

Con objeto de ver la relación de estos conceptos con la comunicación de datos, consideremos el siguiente ejemplo concreto que toma en consideración la transmisión del carácter ASCII "b", codificado en un octeto. El patrón de bits que debe transmitirse

en serie es 01100010. La parte de la izquierda de la figura 5.5 muestra la señal de salida de la computadora que esta transmitiendo. El analisis de Fourier de esta señal genera los siguientes coeficientes:

$$C = \frac{3}{8}$$

$$a_n = \frac{1}{\pi n}\left[\cos(\pi n/4) - \cos(3\pi n/4) + \cos(6\pi n/4) - \cos(7\pi n/4)\right]$$

$$b_n = \frac{1}{\pi n}\left[\operatorname{sen}(3\pi n/4) - \operatorname{sen}(\pi n/4) + \operatorname{sen}(7\pi n/4) - \operatorname{sen}(6\pi n/4)\right]$$

El valor cuadrático medio de las amplitudes $\sqrt{a_n^2 + b_n^2}$, para los primeros términos se muestra en la parte de la derecha de la figura 5.5. Estos valores son de interes porque el cuadrado de ellos es proporcional a la energia transmitida a la frecuencia correspondiente.

Ningún medio de transmisión puede efectuar la transmisión de señales sin dejar de perder potencia durante la realización de dicho proceso. Si todas las componentes de Fourier fueran igualmente disminuidas o degradadas, la señal resultante se reduciria en amplitud, pero no sufriria distorsión alguna. Desafortunadamente, cualquier medio de transmisión degrada varias componentes de Fourier en forma diferente, por lo que se produce distorsión. En general, las amplitudes se transmiten sin degradación de frecuencia en una escala que va desde 0 hasta fc [Hz], observandose que todas las frecuencias que caen por arriba de esta frecuencia de corte son frecuentemente atenuadas. En algunos casos, esta es una propiedad fisica del medio de transmision, en tanto que en otros este efecto se introduce intencionalmente en el circuito mediante un filtro cuyo objeto consiste en limitar el ancho de banda que se encuentra disponible

para cada usuario.

Considérese ahora la señal representada por la figura 5.5a e imaginense como se veria ésta si el ancho de banda fuera tan pequeño que solo se pudieran transmitir las frecuencias mas bajas. En la figura 5.5b se muestra la señal resultante de un canal que sólo permite que el primer armonico pasa a traves de el. De la misma manera, en la figura 5.5c-e se muestran los espectros y las funciones reconstruidas de los canales para anchos de banda mayores.

El tiempo T que se necesita para transmitir un carácter depende del metodo de codificacion y de la velocidad de la señal [definida como el número de veces que la señal cambia de valor en un segundo (es decir, la forma en que varia su voltaje)]. El número de cambios por segundo se mide en baudios. No se puede decir que una linea de *b* baudios necesariamente transmite *b* bits/s, dado que la señal podria enviar varios bits. Si se utilizaran los canales 0,1,2,3,4,5,6 y 7, cada uno de los niveles de la señal serviria para enviar 3 bits, de tal forma que la rapidez de envio de los bits seria tres veces la velocidad en baudios. En nuestro ejemplo, sólo el 0 y 1 se utilizan como niveles de señal, asi que la velocidad en bits es igual a la velocidad en baudios.

Dada una velocidad en bits, de *b* bits/s, el tiempo necesario para enviar 8 bits es 8/*b* s, de tal forma que la frecuencia del primer armonico es *b*/8 HZ. Una linea telefónonica comun, tiene una freceuncia de corte alrededor de los 3000 Hz, la cual se introduce en forma artificial. Esta restriccion significa que el valor de

las frecuencias mas altas que pasan a traves de ella es de aproximadamente 3000/(6/8) ó 24000/6. Los valores tipicos resultantes despues de considerar las velocidades de datos de mayor uso, son las que se listan a continuación:

Bps	*T(mseg)*	*Primer armonico(Hz)*	*# de armonicos*
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

De acuerdo con los numeros anteriores, resulta claro que cuando se trata de enviar datos a una velocidad de 9600 bps sobre una linea de calidad telefónica, la figura 5.5a se transformará en algo parecido a lo que se muestra en la figura 5.5c, haciendo que la recepción correcta del flujo de bits binario original sea improbable. Será obvio que para velocidades de envio de datos superiores a los 38.4 Kbps, no hay ninguna seguridad de recibir las señales binarias, aún cuando los equipos y medios de transmisión estén totalmente libres de ruido. En otras palabras, la restricción del ancho de banda limita la velocidad de envio de los datos, incluso en los casos de canales de transmisión perfectos. Sin embargo, existen nuevos esquemas sofisticados de codificación que utilizan varios niveles de voltaje con los cuales se puede llegar a alcanzar velocidades de transmisión superiores.

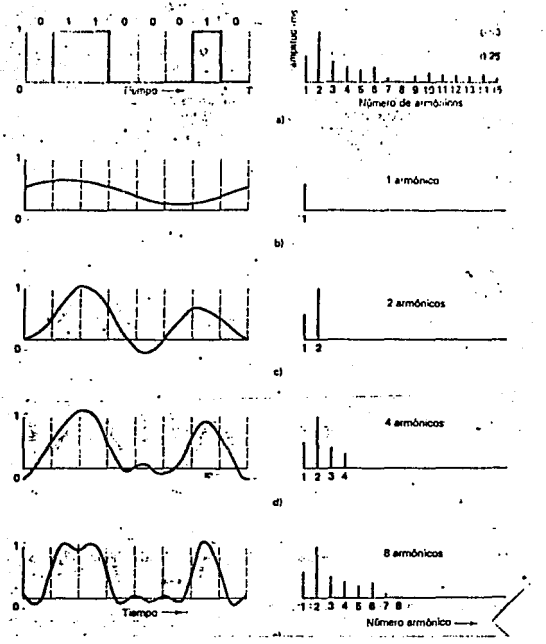


Fig 5.5 a) Una señal binaria y sus valores rms de las amplitudes de Fourier. b)-e) Aproximaciones sucesivas a la señal original.

Maxima capacidad de transferencia de datos de un canal.

En 1924. H. Nyquist comprendió la existencia de esta limitación fundamental y derivó una ecuacion que expresaba la velocidad maxima de datos a traves de un canal sin ruido. con un ancho de banda finito. En 1948. Claude Shannon llevo a cabo un trabajo más extenso sobre lo desarrollado por Nyquist. y lo amplió para el caso de un canal sujeto a ruido aleatorio. Enseguida se hará un resumen. muy breve. de los resultados clásicos sobre dicho problema.

Nyquist demostro que si una señal arbitraria se hace pasar a traves de un filtro pasa bajas. con un ancho de banda H. la señal filtrada puede reconstruirse por completo mediante la obtención simple y sencilla de 2H muestras por segundo. El llevar a cabo un muestreo de la línea a una frecuencia superior de 2H no tiene ningún sentido porque los componentes de frecuencias más altas de dicho muestreo no pueden recuperarse. pues han sido filtrados. Si la señal consiste de V niveles discretos. el teorema de Nyquist establece que:

La velocidad máxima de datos = 2Hlog V bits/s

Por ejemplo. un canal sin ruido de 3 kHz no puede transmitir señales binarias a una velocidad que exceda los 6000 bps.

Hasta aquí sólo se han considerado canales sin ruido. de tal manera que si estuviera presente ruido aleatorio. la situación llegaria a deteriorarse rápidamente. La cantidad de ruido presente se mide por la relacion que existe entre la potencia de la señal y la potencia del ruido. a la cual se le conoce como relación

señal-ruido. Si se denota por S a la potencia de la señal y por N a la potencia del ruido, la relación señal-ruido es S/N. Por lo general, no es común citar la relación misma, en su lugar, lo que se hace es indicarla mediante la cantidad 10 log S/N. La unidad de esta expresión está dada en decibelios (dB). Una relación S/N de 10 es 10 dB, una relación de 100 es 20 dB, una relación de 1000 es 30 dB, y así sucesivamente.

El resultado mas importante del teorema de Shannon establece que la máxima velocidad de datos sobre un canal ruidoso, cuyo ancho de banda es H Hz y cuya relación señal-ruido es S/N, está dado por

número máximo de bits/s = Hlog (1 + S/N)

Por ejemplo, un canal con ancho de banda de 3000 Hz, y una relación señal-ruido de 30 dB (parámetros típicos del sistema telefónico), nunca podrá transmitir a una velocidad superior a los 30 000 bps, sin importar el número de niveles de la señal o la frecuencia de muestreo que se tome. El resultado del teorema de Shannon se demostró mediante el uso de la teoría de la información y tiene una validez muy general.

Como se menciono anteriormente, los medios físicos de transmisión que comprenden esta primer capa del modelo OSI, son primordialmente: Cable coaxial, par trenzado y fibra óptica. Existen otros medios físicos de transmisión como pueden ser vía satélite, rayos infrarojos, etc.

5.1.a. SUBCAPA DE ACCESO AL MEDIO

El proposito de esta subcapa es controlar el flujo de informacion entre las diferentes computadoras y evitar "choques" y "desorden". Para ilustrar mejor lo anterior, veamos el siguiente ejemplo: considéreso una conversacion en la que seis personas, en seis teléfonos diferentes estan todas conectadas unas a otras, de tal forma que cada una de ellas puede oir y hablar a todas las demás. Es muy probable que cuando una de ellas deje de hablar, dos o más comenzaran a hablar al mismo tiempo, produciendose asi un caos. Dentro de esta subcapa se veran los medio y protocolos para evitar este caos.

Protocolos de red de area local.

A aquellos protocolos en los que las estaciones escuchan a una portadora (es decir, a una transmisión), y actúan en consecuencia, se les llama protocolos de detección de portadora.

El primer protocolo de detección de portadora es el CSMA 1 (acceso múltiple por detección de portadora). Cuando alguna estación desea enviar alguna información, primero escucha el canal para saber si alguien está transmitiendo; si el canal está efectivamente ocupado, la estación espera hasta que quede libre. Cuando la estación detecta un canal libre, empieza a transmitir la información. Si llega a ocurrir una colisión, la estación espera durante un intervalo de tiempo aleatorio, para después empezar todo de nuevo.

El retardo de propagación tiene un efecto muy importante en el comportamiento del protocolo. Existe una pequeña posibilidad de

que. justo después de que una estación empiece a transmitir otra estación llegue a estar lista para hacerlo y escuche el canal. Si la señal correspondiente a la primera estación todavia no ha alcanzado a la segunda, esta última detectará un canal desocupado. y también empezará a transmitir, dando como resultado una colisión. Cuanto mayor sea el retardo de propagación, más importante llegará a ser este efecto y, por consiguiente el protocolo, tendrá un rendimiento menor.

Basándose en el principio anterior de "escuchar" y transmitir, se crearon los diferentes protocolos, cada uno de los cuales fue mejorando la posibilidad de lograr una transmisión exitosa. la figura 5.8 muestra la relación de número de transmisiones por unidad de tiempo [S] y probabilidad de intentos de transmisión por unidad de tiempo [G].

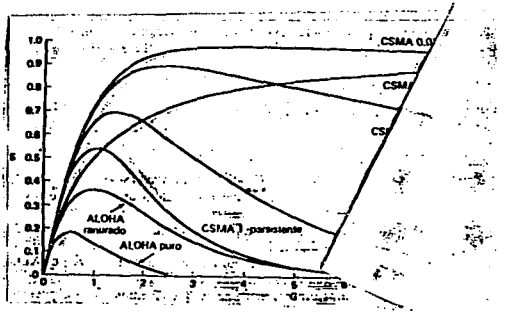


Fig. 5.5. Comparacion de la utilizacion de un canal versus la carga para varios protocolos de acceso aleatorio.

Protocolo por polling

Este protocolo está asociado regularmente con la topología tipo estrella. Su funcionamiento puede ser comprendido si imaginamos un reloj con 12 numeros y una manecilla. La manecilla está girando rápidamente alrededor de los 12 numeros y cada vez que pasa por un número pregunta si ese número tiene información que mandar. si es asi el mensaje es leido. Si no existe mensaje la manecilla pasa al siguiente número. Si el file server tiene información para alguna estación de trabajo. la manecilla se coloca en el número adecuado y el mensaje es enviado. Este protocolo elimina la posibilidad de que una estación de trabajo interfiera la comunicación de otra estación de trabajo.

Protocolo CSMA/CD

Este protocolo esta asociado con la topología lineal. Este protocolo puede ser entendido si se compara con una carretera. Cuando existe poco tráfico. la carretera es segura y fácil de utilizar; un conductor se para en la entrada. echa un vistazo. si la carretera esta libre entonces entra. Pero si la carretera está congestionada con tráfico. el conductor tiene que esperar para poder entrar en la carretera.

El protocolo CSMA/CD tiene a las estaciones de trabajo y al servidor escuchando la linea de comunicación todo el tiempo. Una estación de trabajo sólo se puede comunicar cuando la linea esta libre. Si una estación trata de enviar un mensaje mientras la

línea está ocupada, esta tiene que esperar hasta que la línea quede libre. La terminación CD quiere decir detector de colisiones (Colision detector) y es una mejora al protocolo original mencionado anteriormente. Esta mejora permite no solo escuchar la línea sino también a las otras estaciones y así evitar transmisiones simultáneas y el consiguiente choque de informaciones.

Protocolo Token Passing

Este protocolo es usado en la topología de anillo y anillo modificado. Un "TOKEN" es un sistema especial de acarreo de información que es transmitida en la red y que circula de una estación de trabajo a la siguiente de una manera controlada semejante a como lo hace un trenecito de juguete en una vía circular. Las estaciones de trabajo que no tienen ningún mensaje que enviar lo dejan circular por su camino. Las estaciones que sí tienen mensaje lo agregan al token y éste continua a la siguiente estación.

Estandares de red.

Los estandares de red de una de las organizaciones más importantes son los del IEEE a través del comite 802 de estándares.

802.3 .- Estándar para una topología de bus lineal (CSMA/CD)

802.4 .- Estándar para una topología de anillo modificado (Token Bus)

802.5 .- Estándar para una topología de anillo modificado (Token Passing)

5.3 CAPA DE ENLACE

La tarea primordial de la capa de enlace consiste en, a partir de un medio de transmisión común y corriente, transformarlo en una línea sin errores de transmisión para la capa de red.

Al principio se podría pensar que es un problema trivial en el que la máquina A pone los datos en la línea de transmisión (cable) y la máquina B sólo se encarga de leerlos. Desafortunadamente, los circuitos de comunicación cometen errores de cuando en cuando. Además, sólo tienen una velocidad de transmisión de datos finita y hay un retardo de propagación diferente de cero, entre el tiempo que transcurre desde que un bit se envía hasta que se recibe. Estas limitaciones, asociadas con la velocidad finita de las máquinas para procesar los datos, tienen implicaciones muy importantes en la eficiencia de la transferencia de datos. Los protocolos que se utilizan para las comunicaciones deberán tomar en consideración todos estos factores y es lo que veremos más adelante.

La función de la capa de enlace consiste en proporcionar servicios a la capa de red. El principal servicio es el de transferir datos de la capa de red de la máquina de origen, a la capa de red de la máquina destino. En la capa de red de la máquina de origen hay una entidad, llamada proceso, que entrega algunos bits a la capa de enlace para su transmisión a la máquina destino.

El trabajo que realiza la capa de enlace consiste en transmitir los bits a la máquina destino, de tal modo que puedan entregarse a la capa de red en el otro extremo, como muestra la figura 5.7a. La

transmisión real sigue la trayectoria que se muestra en la figura 5.7b, pero resulta más sencillo pensar en términos de dos procesos de capa de enlace, comunicandose por medio de un protocolo de enlace.

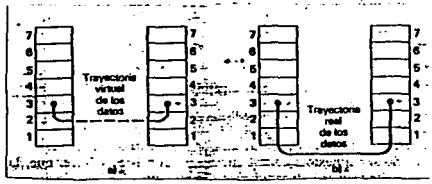


Figura 3.7 a)Comunicacion virtual b)Comunicacion real

La capa de enlace puede diseñarse para que pueda ofrecer varios servicios. Los servicios que realmente se ofrecen pueden variar de sistema a sistema, hay tres posibilidades razonables:

1.- Servico sin conexión y sin asentimiento.
2.- Servicio sin conexión y con asentimiento.
3.- Servicio orientado a conexión.

El servicio sin conexión y sin asentamiento consiste en hacer que, la máquina origen transmita tramas o "trozos" de información independientes a la máquina destino, sin que ésta proporcione un asentimiento o confirmación. No se establece ninguna conexión

previa, ni tampoco se libera posteriormente. Si la trama se llega a perder, como consecuencia de ruido en la línea, no se realiza ningún intento por recuperarla en la capa de enlace. Este tipo de servicio es muy conveniente cuando la tasa de error muy baja y la recuperación se delega a las capas mas altas. También resulta apropiado para los casos de tráfico en tiempo real, como en el caso de la voz, en la que la tardanza en la llegada de datos es peor que tener datos erróneos. Muchas redes de tipo LAN, cuentan con un servicio sin conexión y sin asentimiento en la capa de enlace.

El siguiente paso, en términos de fiabilidad, es el servicio sin conexión y con asentimiento. Cuando se ofrece este servicio, no se utiliza todavía la conexión, pero cada una de las tramas transmitidas se asiente en forma individual. De esta manera, el transmisor sabe cuando la trama llega bien al otro extremo. Si la trama no llega dentro de un intervalo de tiempo especificado, entonces puede comenzar a transmitirla nuevamente.

El servicio más sofisticado que la capa de enlace puede ofrecer a una red, es el servicio orientado a conexión. Con este tipo de servicio, las máquinas origen y destino establecen una conexión antes de transmitir ningún dato. Cada una de las tramas transmitidas a través de la conexión se enumera, y la capa de enlace garantiza que cada una de las tramas se reciba. Además garantiza que se reciba una vez y en el orden correcto.

Cuando se emplea el servicio orientado a conexión, las transferencias tienen tres fases distintas. En la primera fase, la

conexión se establece cuando los dos lados han iniciado las variables y los contadores necesarios para mantener el seguimiento de qué tramas se han recibido y cuales son. En la segunda fase, una o más tramas se transmiten realmente. En la tercera y última fase, la conexión se libera, dejando libres a las variables, a las memorias temporales, así como a otros recursos que se emplean para mantener la conexión.

La comunicación entre la capa de red y la capa de enlace utiliza las primitivas de servicio de OSI. Las primitivas son: *solicitud*, *indicación*, *respuesta* y *confirmación*. La capa de red utiliza las primitivas de solicitud para pedirle a la capa de enlace que haga algo, como por ejemplo, establecer o liberar una conexión, o transmitir una trama. Se utilizan las primitivas de indicación para indicarle a la capa de red que se ha producido un evento, por ejemplo, el hecho de que otra máquina desea establecer o liberar una conexión, o bien, avisar de la llegada de una trama. La capa de red utiliza las primitivas de respuesta, en el extremo de recepción, para contestar a una indicación anterior. Las primitivas de confirmación proporcionan una manera de saber en el extremo solicitante, si la solicitud fue realizada con éxito y si no, la razón por la cual no se llevó a cabo.

Existen diferentes protocolos para la detección de errores de la línea de transmisión. Si se desea profundizar en este tema, puede consultar el material de referencia.

5.4 CAPA DE RED

La capa de red se ocupa del control de la operacion de la subred. Un punto de suma importancia en su diseño es la determinacion sobre cómo encaminar los paquetes del origen al destino. Las rutas podrian basarse en tablas estáticas que se encuentran "cableadas" en la red y que dificilmente podrian cambiarse. También, podrian determinarse al inicio de cada conversación. por ejemplo en una sesión de terminal. Por último, podrian ser de tipo dinámico, determinandose en forma diferente para cada paquete, reflejando la carga real de la red.

Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruiran mutuamente y darán lugar a un cuello de botella. El control de tal congestión depende también de la capa de red.

Otra tarea importante de la capa de red es cuando se desea intercambiar paquetes en dos redes. El direccionamiento utilizado en la segunda red puede ser diferente al empleado en la primera. La segunda podría no aceptar el paquete en su totalidad, por ser demasiado grande. Los protocolos podrían ser diferentes, etc. La responsabilidad de la capa d red es resolver estos problemas de interconexión de redes heterogéneas.

Se diferencia de la capa de enlace en que ésta es más modesta y solo conecta a dos maquinas a traves del cable, mientras que la capa de red direciona o encamina a través quizá de varios nodos y trayectorias.

5.5 CAPA DE TRANSPORTE

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. Además todo este trabajo se debe hacer de manera eficiente, de tal manera que aisle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.

Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexion de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones de la red con objeto de mejorar dicho caudal. Por otra parte, si la creación o mantenimiento de la conexión de una red resulta costoso, la capa de transporte podría multiplexar varias conexiones de transporte sobre la misma conexión de red para reducir dicho costo. En todos los casos, la capa de transporte se necesita para hacer el trabajo de multiplexión transparente a la capa de sesión.

La capa de transporte determina que tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red. El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes en el mismo orden en que fueron enviados. Sin embargo, el transporte de mensajes aislados sin garantizar el orden de

distribución y la difusión de mensajes a destinos múltiples es otra posibilidad de servicio de transporte. El tipo de servicio se determina cuando se establece la conexión.

La capa de transporte es una capa del tipo origen-destino o extremo a extremo. Es decir, un programa en la máquina origen lleva una conversación con un programa parecido que se encuentra en la maquina destino, utilizando las cabeceras de los mensajes y los mensajes de control. Los protocolos, de las capas inferiores, son entre cada máquina y su vecino inmediato, y no entre las máquinas origen y destino, las cuales podrían estar separadas por varios elementos de conmutación. La figura 5.8 ilustra la diferencia entre las capas 1 a 3, que están encadenadas, y las capas 4 a 7, que son de extremo a extremo.

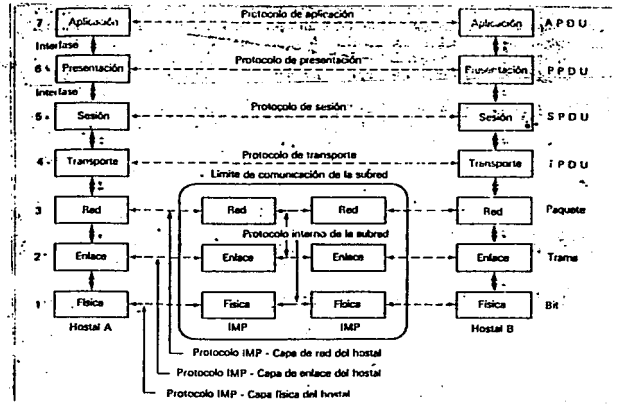


Figura 5.8 Arquitectura de red basada en el modelo OSI

5.6 CAPA DE SESION

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utilizan en algunas aplicaciones. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia o transferir un archivo entre dos máquinas. Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo, o bien, en una sóla dirección en un instante dado. Si el tráfico sólo puede ir en una dirección en un momento dado, la capa de sesión ayudará en el seguimiento de quien tiene el turno.

La administración del testigo es otro de los servicios relacionados con la capa de sesión. Para el caso de algunos protocolos resulta esencial que ambos lados no traten de realizar la misma operación en el mismo instante. Para manejar estas actividades, la capa de sesión proporciona testigos que pueden ser intercambiados. Solamente el extremo con el testigo puede realizar la operación crítica.

Otro de los servicios de la capa de sesión es la sincronización. Considérese, por ejemplo, los problemas que podrían ocurrir cuando se tratara de hacer una transferencia de archivo de dos horas entre dos máquinas en una red con un tiempo medio de una hora

entre caídas. Después de abortar cada archivo, la transferencia completa tendría que iniciarse de nuevo y probablemente, se encontraría de nuevo con la siguiente caída de la red. para eliminar este problema, la capa de sesión proporciona una forma para insertar puntos de verificación en el flujo de datos, con objeto de que, después de cada caída, solamente tengan que repetirse los datos que se encuentren después del último punto de verificación.

5.7 CAPA DE PRESENTACION

La capa de presentación realiza ciertas funciones que se necesitan bastante a menudo como para buscar una solución general para ellas, más que dejar que cada uno de los usuarios resuelva los problemas. En particular y, a diferencia de las capas inferiores, que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

Un ejemplo típico de servicio de la capa de presentación es el relacionado con la codificación de datos conforme a lo acordado previamente. La mayor parte de los programas de usuario no intercambian partes de bits binarios aleatorios, sino, más bien, cosas como nombres de personas, datos, cantidades de dinero y facturas. estos artículos están representados por caracteres, números enteros, números de punto flotante, así como por estructuras de datos constituidas por varios elementos más sencillos. Las computadoras pueden tener diferentes códigos para representar los caracteres (por ejemplo ASCII y EBCDIC), enteros (complemento a uno o complemento a dos), etcetera. Para posibilitar la comunicación de computadoras con diferentes representaciones, la estructura de los datos que se va a intercambiar puede difinirse en forma abstracta, junto con una norma de codificación que se utilice "en el cable". El trabajo de manejar estas estructuras de datos abstractas y la conversión de

la representación utilizada en el interior de la computadora a la representación normal de la red, se lleva a cabo a traves de la capa de presentación.

La capa de presentación está relacionada también con otros aspectos de representación de la información. Por ejemplo, la compresión de datos se puede utilizar aquí para reducir el número de bits que tienen que transmitirse, y el concepto de criptografía se necesita utilizar frecuentemente por razones de privacidad y de autentificación.

5.8 CAPA DE APLICACION

La capa de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos de terminales incompatibles en el mundo. Considérese la situación de un editor orientado a pantalla que desea trabajr en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de pantallas, de secuencias de escape para insertar y borrar texto, de movimiento de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracta, con el que los editores y otros programas pueden ser escritos para trabajar en ella. Con objeto de transferir funciones de una terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho sotfware deberá emitir la secuencia de comandos apropiados para que la terminal real también ubique su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Distintos sistemas de archivos tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las lineas de texto, etc. La transferencia de archivos entre dos sistemas diferentes requiere de la resolución

de éstas y de otras incompatibilidades. Este trabajo, así como el correo electrónico, la entrada de trabajo a distancia, el servicio de directorio y otros servicios de propósito general y específico, también corresponden a la capa de aplicación.

CAPITULO VI

SISTEMAS OPERATIVOS

El sistema operativo de redes, es la plataforma sobre la cual "corren" todas las aplicaciones de la red.

Como se dijo anteriormente, al iniciar el desarrollo del concepto de red local, cada fabricante desarrolló su equipo propio y requirió de desarrolladores de software también propio para poder funcionar en sus equipos. Fue así como se crearon varios sistemas operativos con aplicaciones propias y muy específicas.

Con la creación del modelo OSI y viendo la tendencia del mercado hacia la homogeniedad o al menos a poder utilizar diferentes equipos con diferente software, los fabricantes se hicieron a la tarea de desarrollar un software que cumpliera con el modelo OSI y fuera compatible con la mayoría de equipos.

Sin embargo, aún cumpliendo con los estándares del modelo OSI, cada sistema operativo tiene sus características propias que le permiten o lo limitan a usar cierto tipo de hardware: tarjetas de interfase, puentes, ruteadores, cable, etc. También una característica propia de cada sistema operativo es el número de estaciones de trabajo que soporta y su habilidad para integrarse a otros ambientes o sea su conectividad. Obviamente el precio va en función directa de la versatilidad de cada sistema operativo.

Dentro de todos los sistemas operativos que hay en el mercado, existen tres que por sus características abarcan gran parte de éste. Ellos son: LANTASTIC, LAN MANAGER y NETWARE.

LANTASTIC es una muy buena opción para instalar una red pequeña. de 2 a 4 estaciones. y muy económica.

LAN MANAGER y NETWARE, principalmente este último, son los sistemas operativos de mayor uso en la actualidad. Esto se debe principalmente al cuidado que han puesto en su diseño, cubriendo niveles de seguridad, capacidad de comunicación y conectividad con otros ambientes.

Este caputulo presenta una reseña de cada uno de estos sistemas operativos, más algunos otros existentes en el mercado. He puesto un énfasis especial en LANTASTIC como un sistema operativo ideal para redes pequeñas, LAN Manager como un sistema que corre sobre OS/2 y Netware como el sistema de mayor uso y con mayor número de opciones.

6.1 LANTASTIC

Suponga que usted cuenta con una PC 386 con una impresora laser y desea compartir información con su asistente el cual cuenta con una PC 286 y una impresora de matriz de puntos.

Se requiere entonces instalar una pequeña red de dos nodos que nos permita enviar mensajes entre si por medio del correo electrónico, compartir archivos y compartir impresoras. El paquete LANTASTIC para este proposito es una muy buena opción. Este paquete viene completo con hardware y software y es relativamente fácil de instalar.

Paso 1. El primer paso es instalar las tarjetas de red en ambas computadoras. Las tarjetas LANtastic tienen un sólo banco de interruptores que muy probablemente no necesite tocar; en la mayoría de los casos la configuración de fábrica funcionará en sus máquinas.

La mayoria de los conflictos que surgan entre su PC y el software pueden ser resueltos a nivel comandos de software. Los problemas más comunes surgen cuando las tarjetas de red tratan de usar la misma interrupcion (IRQ) de otra tarjeta o dispositivo en su PC, como un "mouse", un modem o un puerto serie. En algunas ocasiones estos dispositivos tienen pequeñas anotaciones que nos indican que interrupción están usando, otra opción es consultar los manuales. Si ninguna opción anterior es posible, se puede conseguir un programa de análisis de sistema que nos indica las interrupciones. Las tarjetas LANtastic usan el IRQ 3. Si existe algún conflicto, no es necesario sacar la tarjeta y reconfigurarla. Es suficiente

con utilizar un comando que le indique que IRQ usar. Si existe un modem que utilice el IRQ 3, por ejemplo, cambie la interrupción en la tarjeta dando el siguiente comando.

LANBIOS2 IRQ=4

Paso 2. Cableado y software de instalación. Después de instalar las tarjetas en ambas PC's, conectelas con el cable que viene en el paquete. Una vez hecho esto corra el software de instalación en ambos discos duros. Por el momento es conveniente utilizar los "defaults". El programa le pedirá que proporcione el nombre de las computadoras y el "password" para cada una de ellas.
Aegúrese de especificar que desea utilizar amabas computadoras como servidor y estación de trabajo a la vez. LANtastic es un sistema operativo que nos permite lo anterior.

Paso 3. Establezca recursos compartidos y niveles de acceso.
Cambiese al directorio LANtastic de la 386 y teclee NET_MGR. El menú de administrador de red aparecerá en pantalla. Seleccione la opción "Shared Resource Management" (administración de recursos compartidos). La pantalla mostrará una lista de recursos compartidos que el programa detectó durante la instalación. Por ejemplo puede aparecer lo siguiente: Floppy drives A: y B:, disco duro con particiones C: y D: e impresora laser.
Al principio, todos los dispositivos son enlistados como recursos compartidos. Para hacer un dispositivo privado, sólo elimínelo del

menú. Si no quiere que su asistente tenga acceso a sus floppy drives, puede eliminarlos: mueva el cursor a donde se encuentran los floppy drives y presione la tecla [Del]. También puede borrar una partición de su disco duro para hacerla privada y dejar como recurso compartido la(s) otras particiones.

Repita el procedimiento en la otra computadora para seleccionar los recursos a compartir de ésta.

El procedimiento para los niveles de acceso es muy similar. Al instalar LANtastic se crea el drive F: por default y en este drive se puede accesar a todos los archivos que se especifiquen. (aún cuando estos se encuentren en una partición privada). Al compartir un archivo también aparecerá en pantalla una lista de privilegios para cada uno de ellos. Suponga que tiene un archivo llamado "agenda" y desea que sólo su asistente realice cambios en él. Usted debe poder ejecutarlo y leerlo. Usted puede tener los siguiente privilegios sobre este archivo: "E" para poder ejecutarlo, "R" (Read access) para poder leerlo y "L" (File Lookups) para poder consultar sus subdirectorios. Su asistente deberá tener además el privilegio "M" (modify) para realizar cambios.

Paso 4. Carge el software de red. Ahora el siguiente paso es cargar el software LANtastic. Ya que deseamos que ambas máquinas funcionen como servidor y estación a la vez, debe poner el software de servidor y de estación en ambas.

Primero, debe crear un archivo batch como el siguiente para cargar

el sotfware necesario:

```
\DOS\FASTOPEN C: D: E:
\DOS\SHARE
LANBIOS2
REDIR 386 LOGINS=2
SERVER
```

FASTOPEN carga el programa fastopen de DOS para los drives físicos de la máquina C: D: y E: los cuales acelerarán algunas tareas de la red. El comando SHARE de DOS habilita el poder compartir archivos o bloquearlos. El comando LANBIOS carga el sistema operativo LANtastic, el comando REDIR instala el sotfware de estación de trabajo, y los parámetros de LOGINS le permiten realizar dos tareas de red a la vez. SERVER carga el software de servidor.

El archivo batch de la computadora de su asistente deberá de ser igual.

A diferencia de otras redes, LANtastic no es un glotón de memoria. El sistema operativo toma 1.5 K. Si configura su máquina como estación de trabajo se lleva 11 K, como servidor de 23 a 27 K; y si quiere que funcionen como ambos, se necesitan de 34 a 38 K.

Paso 5. Escriba Login Scripts para accesar a sus recursos compartidos. Una vez cargado el sotfware de red en ambas máquinas, necesita "log in" o entrar a la red y accesar los recursos que dió de alta en el paso 3. Para hacer eso, necesita escribir un Login Script (el login script es el equivalente al autoexec.bat en MS-DOS) Para la 386 suponga que su nombre de usuario es JEFE y su

password es NUM1. Puede tener el siguiente Login Script:

```
NET LOGIN \\386 JEFE NUM1
NET LOGIN/WAIT\\AT JEFE NUM1
NET ATTACH/VERBOSE\\AT
NET USE LPT2\\AT\@PRINTER
NET QUEUE START\\AT
NET LPT TIMEOUT 1
:END
```

El primer comando accesa la máquina 386 a la red (por seguridad puede excluir este comando y accesar a la red manualmente contestando a las preguntas de usuario y password).

La segunda instrucción permite acceso a la AT de su asistente. La opción /WAIT para la ejecución del batch si no localiza a la AT en la red. Su PC espera un tiempo antes de volver a intertar acceso a la AT. Puede cancelar el proceso teclendo [Esc].

Una vez encontrada la AT, el comando ATTACH enlaza ambas computadoras. La opción VERBBOSE despliega un listado de todos los recursos compartidos. NET USE LPT2\\AT\@PRINTER le permite acceso a la computadora de su asistente. Note que usamos LPT2 debido a que ya existe una impresora conectada a su LPT1. NET QUEUE START\\AT inicia una cola de impresión para la impresora conectada a la AT.

NET LPT TIMEOUT 1 asegura que todos sus programas puedan imprimir en la red.(Algunas aplicaciones no permiten mandar a impresión, en una red, directamente del programa -primero debe salir del programa.) El comando TIMEOUT ayuda un poco ya que envia la orden de impresión con un tiempo de retraso. En este ejemplo el tiempo es 1 segundo pero puede ser de hasta una hora.

El Login Script de la otra máquina es muy similar. Solo es necesario cambiar el nombre de usuario y su password correspondiente.

Paso 6. Trabajar en red. Una vez completados los pasos anteriores, ya está todo listo para trabajar en red. Pude compartir recursos, enviar mensajes, intercambiar archivos.

LANtastic usa sotfware con menus que le van a orientar paso a paso lo que debe realizar. Teclee NET y aparecerá un menú de red en la pantalla. Desde este menú usted puede crear, enviar y recibir correo electrónico, controlar trabajos de impresión, cambiar las passwords, etc.

Ambas PC's pueden seguir funcionando de manera ordinaria y los comandos de DOS son reconocidos. Puede utilizar el comando copy para transferir archivos de una PC a otra, leer información, enviar mensajes o archivos binarios o en código como pudiera ser una hoja de cálculo.

6.2 LAN MANAGER

LAN MANAGER es un sistema operativo de red que se instala sobre OS/2 y es esto quizá lo que ha limitado su popularidad ya que la mayoría de usuarios está más familiarizado con MS-DOS.

Sin embargo, LAN MANAGER desarrollado por MICROSOFT es un muy buen sistema operativo cuyas características enunciaremos a continuación.

La versión más reciente de LAN MANAGER es la 2.0. Esta versión requiere la instalación del sistema operativo OS/2 en el servidor de la red (y no es necesario en las estaciones de trabajo).

Lan Manager 2.0 instala HPFS (Sistema de archivos de alto desempeño) que inmediatamente representa dos grandes mejoras.

La primera de ellas se refiere a la seguridad. HPFS se instala automáticamente en los servidores con procesador 386 ó 486 y trae consigo su propio sistema de seguridad sobre los archivos que administra. Para ello la información de control de acceso se almacena como parte de la estructura del archivo y es necesario su permiso y contraseña especiales para acceder cualquier archivo, aún si la red no está operando.

La segunda ventaja ofrecida por HPFS es el desempeño de la red a través de multiples rasgos distintivos. Citaré solamente unos cuantos:

HPFS explota las posibilidades de los procesadores 386 para acceder mucho más rápidamente los archivos. Además permite que los nombres de los archivos puedan tener más de 11 caracteres.

En este ambiente se pueden tener 254 caracteres en el nombre, con

la posibilidad de signos de ortografía y espacios en blanco. lo que permite un nombre mucho más significativo de lo que contiene el archivo.

Los atributos de cada archivo pueden extenderse hasta ocupar 64 K. Además HPFS hace la distribución de los archivos de una manera mucho más eficiente. DOS los distribuye de modo tal que las ampliaciones de los archivos son colocadas según el espacio que está disponible en disco. Este proceso provoca la fragmentación en los archivos.

El HPFS usa el algoritmo de colocación de archivos por banda. así los archivos se guardan en directorios de bandas de información de 8 Megabytes. Esta técnica mantiene los directorios cerca de los datos a los que hace referencia y se minimiza el movimiento de cabezas en el disco, el resultado es un mayor desempeño de la red.

El espacio en disco se distribuye ocupando incrementos de un sector de modo que, en promedio, sólo 256 bytes por cada archivo se pueden llegar a desperdiciar (DOS usa incrementos de un cluster y puede dejar 4096 bytes sin ocupar).

En HPFS se ha eliminado la búsqueda secuencial de los nombres de los archivos y en su lugar se tiene un árbol binario indexado para acceder directamente el nombre del archivo.

Mayor seguridad

La seguridad en las versiones anteriores de Lan Manager se habia tratado en tres formas distintas.

La primera, es la seguridad de ingreso a la red (Net-Logon Security) en la cual se pide al presunto usuario teclear una

identificación de usuario (password) dada de alta por el administrador y, opcionalmente, una contraseña válida unicamente para ese nombre del usuario.

En segunda cada servidor en la red, además de tener la seguridad de ingreso, puede ser designado con seguridad de usuario o seguridad de recursos compartidos.

El tipo de seguridad de usuario es el más común y el más recomendable, la clave de usuario es clasificada como perteneciente a uno o más grupos a los cuales se les ha concedido ciertos privilegios (lectura,escritura, creación, etc.) con respecto a algunos de los recursos de la red (subdirectorios de archivos, colas de impresión, puertos de comunicación, etc.)

De esta forma el administrador puede conferir privilegios a cada usuario en particular, sobre cada uno de los recursos. El tercer tipo, la seguridad de recursos compartidos, tiene un funcionamiento más sencillo. Simplemente cada recurso en la Red es protegido por medio de una contraseña o password. Así el procesador de palabras tendrá un password, el sistema de base de datos otro y habrá un tercero para las hojas de cálculo, etc.

Algunos usuarios tienden a confundirse con la proliferación de contraseñas y el dar aviso de cambios complica las cosas un poco más y esto no ha favorecido mucho a Lan Manager.

Con la versión 2.0 de Lan Manager se siguen soportando estos tipos de seguridad. Sin embargo, el HPFS protege todos los archivos de usuarios no autorizados, del propio administrador de la red o de alguien que llegue a tener acceso a la consola. Es todo un reto

aún para programadores expertos el romper la seguridad de HPFS.

Mayor aprovechamiento de la memoria en las estaciones de trabajo. Las estaciones de red pueden estar operando bajo DOS o bien bajo OS/2. En esta versión el consumo de memoria es sumamente pequeño. Una estación DOS con servicios básicos sólo dedica 60 K al almacenamiento de los drives (con Lan Manager). Esta memoria aumenta si se usa la configuración de servicios extendida (Enhaced) en la que se puede tener:

a) Servicios de mensajería con estaciones de este tipo y estaciones OS/2

b) Interfase y posibilidad de instalar y controlar recursos de red, como en las estaciones OS/2.

La versión 3.0 de Microsoft Windows puede instalarse en las estaciones DOS con los beneficios que trae este ambiente en lo referente a redes.

Las estaciones OS/2, en realidad son servidores limitados, ya que pueden compartir recursos con cualquier otra estación (aún la DOS) y realizar funciones de administración.

Esta serie de servicios que pueden correrse en las estaciones OS/2 hacen que las necesidades de RAM crezcan, como mínimo se requiere 2 Megas.

Otras características. Desde su primera versión Lan Manager tuvo gran número de características especiales que ganaron la aprobación del mercado en general. De acuerdo a pruebas de campo realizados por Info World Lan Manager es la red más rápida.

Además de su velocidad el dispositivo de desconexión automática de

los usuarios, cuando su sesión ha sido dada muestras de actividad por un período de tiempo prefijado, habilita a Lan Manager para manejar grandes grupos de trabajo en ambientes de oficina. Desde luego, si el usuario intenta hacer uso de los recursos de la red. Lan Manager le restablece su sesión, también de modo automático.

Esta característica de auto conexión se extiende hasta elementos de la red con fallas y al mismo servidor. Con esto, el administrador puede apagar un servidor en la red, instalarle una tarjeta de uso especial y reconectarlo a la red sin interrumpir el trabajo de los usuarios.

El servidor de respaldo sobre los archivos de DOS puede ser cualquiera existente en el mercado. Para respaldar archivos HPFS existen sistemas tales como Sytos Plus de Sytron Corp.

Lan Manager incorpora en su versión 2.0 accesorios para tener la admistración de las cuentas de usuario. Por ejemplo, se puede forzar al usuario a conectarse desde determinada estación (o grupo de estaciones), se puede cambiar la contraseña de entrada cada determinado tiempo o permitir a un usuario conectarse sólo durante una ventana de tiempo prefijada.

También existe el servidor de perfil de usuario muy conveniente para guardar una configuración de la red (todos los nombres lógicos de los subdirectorios, colas de impresión, puertos de comunicación, etc. de todos los servidores requeridos para una aplicación) y generarla automáticamente al necesitarla. El perfil puede compartirse con otros usuarios.

Lan Manager cuenta con un Script de inicio que puede hacer las

funciones de autoexec.bat del DOS. El script se guarda en el servidor de manera que puede compartirse.

En grandes redes, se pueden definir "dominios" o grupos de servidores y entre ellos se designa a uno como el controlador primario del grupo. Hay dos caracteristicas que provee Lan Manager para facilitar la labor administrativa:

1a. La función de administración de todo el dominio puede hacerse en el controlador primario. Este actúa como exportador de todos los datos de cuentas y privilegios que se le suministren y los exporta a cada uno de los servidores dentro del dominio.

2a. Se puede definir otro servidor dentro del dominio como el suplente del servidor primario. Así, en el caso de que el controlador primario llegara a faltar, el servidor suplente entrará en funciones impidiendo se suspenda el servicio de la Red y de la administración centralizada. Ya en esta versión, Lan Manager cuenta con los servicios de duplicación de disco y de imagen espejo de disco (estos términos se explicarán mejor en el siguiente capitulo) como sistemas de tolerancia a fallas. También se ha incluido el poder conversacional con UPS (Fuente de poder ininterrumpida) inteligentes a fin de dar a conocer a los usuarios las condiciones de trabajo sel sistema de fuerza ininterrumpida.

La posibilidad de exportar información de un servidor a otros, no está limitada a ser únicamente de naturaleza administrativa. Cualquier archivo directorio se puede exportar a todos los servidores de dominio.

El nuevo sistema operativo Lan Manager 2.0 es una sólida opción

para aquellos administradores que tengan la necesidad de enfrentarse a grandes redes, con un gran número de usuarios multidisciplinarios con necesidades de interconexión a otros ambientes.

6.3 VINES 386

VENTAJAS

* Buen manejo de tráfico pesado multiusuario
* Fácil de instalar
* Soporta buen número de topologías
* Soporta acceso de PC remota
* Buen nivel de seguridad
* Buen nivel de auditoria de usuario

DESVENTAJAS

* Pobre manejo de impresoras
* No tiene posibilidad de duplicar en espejo
* Protección contra copias complicada

6.4 3 + OPEN (3COM INC)

VENTAJAS

- Soporta estaciones OS/2
- Rápido con pocas estaciones
- Fácil de instalar
- Soporta colas de impresión
- Ha anunciado productos buenos de conectividad
- Buena auditoria de usuarios
- Ejecución remota de programas OS/2

DESVENTAJAS

- Alto requerimiento de memoria
- Bajo rendimiento con tráfico multiusuario
- Soporta sólo topologías 3COM e IBM
- No se administra el server desde estación
- Bajo nivel de seguridad
- No tiene posibilidad de duplicar en espejo
- Muchas opciones sólo anunciadas no disponibles

6.5 OS/2 LAN SERVER (IBM)

VENTAJAS

* Soporta estaciones OS/2
* Fácil de instalar
* Soporta colas de impresión con prioridad
* Ejecución remota de programa OS/2
* Buena auditoria de usuarios

DESVENTAJAS

* Bajo rendimiento de impresoras
* Bajo rendimiento con tráfico multiusuario
* Requiere programa PC LAN en cada estación DOS
* Difícil de afinar adecuadamente
* Soporta sólo topologías IBM
* No se administra el server desde estación
* No tiene posibilidad de duplicar en espejo

La figura 6.1 muestra una gráfica de poder contra usabilidad como una manera de evaluar a los distintos sistemas operativos.

Poder = (Rendimiento + versatilidad)/ 2

Usabilidad = ((2 x Facilidad de aprendizaje) + (2 x Facilidad de uso) + (evaluación del usuario))/ 5

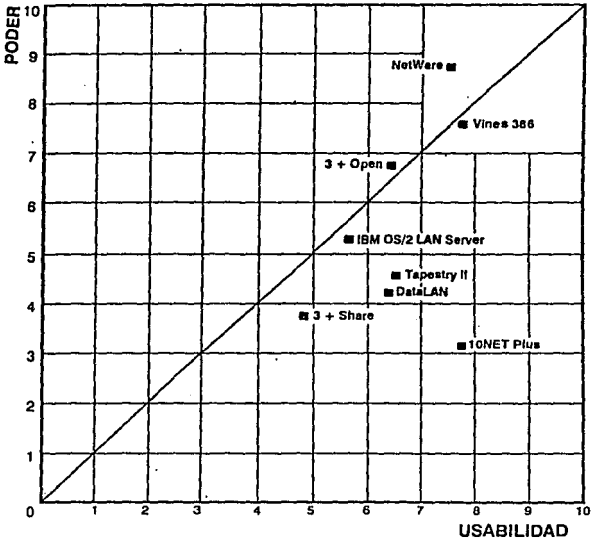


Figura 6.1 Comparacion de s.o. de red. Evaluacion realizada por Novellco de Mexico S.A. de C.V.

6.6 NETWARE

Netware es el sistema operativo de redes más popular en la actualidad. Este sistema fue introducido por primera vez en el mercado en el año de 1983 como Novell-NETWARE.

Según estadísticas realizadas por diferentes revistas dedicadas a la computación, Netware abarca más del 53 % del mercado de redes. Una de las razones del éxito de Novell es mantenerse a la vanguardia en tecnología y la versatilidad de sus productos. Existe una versión para casi cualquier necesidad, para pequeñas redes de 4 u 8 usuarios o hasta grandes redes heterogeneas con equipos muy diversos.

En forma general, existen cuatro características particularmente importantes que distinguen a Netware de sus competidores:

1.- Tecnología de File Server

2.- Tolerancia a fallas

3.- Tecnología de protocolo abierto

4.- Administración de la red

La tecnología de File Server comprende cuatro componentes básicos:

- Servicios de archivos de alta velocidad utilizados por los protocolos del núcleo de Netware. Estos servicios incluyen la capacidad de compartir archivos remotos, impresoras y herramientas de manejo de la red.

- Capacidad de base de datos distribuida (razón por la cual se creó el Netware SQL) que permite a los usuarios usar los paquetes estandar que usa SQL para dar acceso a la información por vía de Netware.

- Servicio de manejo de mensajes (MHS). Tecnología que almacena y dirige, mediante el procesamiento de datos distribuidos. Ayuda a los desarrolladores líderes a llegar a la siguiente generación de aplicaciones.

- Subsistema de comunicación. Permite que las LANs geográficamente dispersas se comuniquen utilizando protocolos asíncronos y tecnología X.25

Netware proporciona integridad de la información por medio de tres niveles de tolerancia de Fallas del Sistema (SFT)

- Todos los sistemas de Netware utilizan el nivel I, el cual incluye el Hot Fix e información de archivo duplicada.
- Netware SFT proporciona un reflejo de disco y rastreo de transacción.
- Las nuevas generaciones de Netware, permitirán hacer operaciones sin parar.

Ya que los usuarios requieren de un acceso transparente desde medios ambientes heterogéneos, la tecnología de protocolo abierto (OPT) es un paso natural en el desarrollo de las redes de proceso abierto. Netware ofrece lo siguiente:

- Cinco medios ambientes claves que requieren acceso tranparente incluyen DOS, OS/2, Sistema Operativo Macintosh, UNIX y VMS
- Dos productos OTP son el Netware para Macintosh y el Netware para VMS.

El manejo de la red llega a ser crítico, conforme las redes se incrementan en tamaño y complejidad.

La estrategia de Novell para mejorar el manejo de la red incluye cuatro fases:

- La primera fase de Novell proporciona herramientas y capacidad dentro del Netware para manejar las instalaciones tales como, la configuración del sistema operativo, la seguridad, el análisis del funcionamiento y el aislamiento de falla.
- La segunda fase asegura que estas capacidades puedan tener acceso remotamente a través de las Netware Application Program Interfaces (APIs).

- La tercera fase permite que los usuarios del Netware se conecten a otros sistemas huéspedes.

- La cuarta fase permite que los usuarios de Netware "mapeen" a otros sistemas centralizados del manejo de la red de los vendedores, tales como la Netview de IBM.

6.6.a VERSIONES DE NETWARE

Productos Tradiconales

ELS NETWARE I V2.0A
ELS NETWARE II v2.15
ADVANCED NETWARE V2.15
SFT NETWARE V2.15

Características generales de Netware:

1.- Interacción con MS-DOS.

2.- Comparte disco duro e impresoras.

3.- Soporta hasta cuatro tarjetas de red permitiendo usar diferentes tipos de hardware.

4.- Cuenta con el software necesario para que un microcomputador se conecte vía modem.

5.- Maneja una excelente administración de cola de impresión.

6.- Administración de recursos a través de la consola del servidor.

7.- Cuenta con gran cantidad de utilerías y ordenes del sistema.

8.- Consola virtual.

9.- Contabilidad de uso de recursos.

10.- Permite limitar la cantidad de almacenamiento en disco.

11.- Absoluto control sobre el acceso de los usuarios a la red a través de cuatro niveles.

* Login y Password
* Derechos de usuario
* Derechos de directorio
* Atributos de los archivos

Netware funciona en modo dedicado y no dedicado.

6.6.b ELS Netware 286 V2.0a Nivel I

- Versión para un número máximo de 4 usuarios activos en la red aunque más de cuatro usuarios pueden ser dados de alta en la red.

- Diseñado para correr en servidores tipo PC-AT.

- Es una versión No Dedicada.

- Corre en el modo protegido de los equipos ATs por lo que tiene capacidad para direccionar hasta 16 MB de memoria RAM (dependiendo del equipo AT) y hasta 2 GB en disco duro.

- No permite la formación de puentes internos, así como tampoco la formación de puentes remotos.

- Puede instalarse también en equipos del tipo 386 o equipos del tipo PS/2 de IBM modelos 50,60 y 80.

Niveles de seguridad de acceso con cuatro niveles:

a) Password de acceso
b) Derechos de usuario
c) Derechos de directorio
d) Atributos de los archivos

- Por ser una versión del tipo 286 Nivel I, cuenta con la utileria HOT FIX, que se encarga de detectar sectores que pudieran estar dañados del disco duro para no ser utilizados.

- Esta es la versión de Netware más económica.

6.6.c ELS Netware 286 V2.15 Nivel II

- Presenta todas las ventajas señaladas en caracteristicas generales.

- Versión para un número máximo de 8 usuarios al mismo tiempo aún cuando se pueden dar de alta más de ocho usuarios.

- Diseñada para correr en servidores tipo 286, 386 y PS/2.

- Es una versión Dedicada (en máquinas 8088 y 8086) y No dedicada (en máquinas 286 y 386).

- Corre en el modo protegido de los equipos ATs por lo que tiene capacidad para direccionar hasta 16 MB de memoria RAM y hasta 2 GB en disco duro.

- No permite la formación de puente internos ni externos con otras redes, pero si tiene una opción de comunicación remota.

Niveles de seguridad de acceso con cuatro niveles:

a) Password de acceso
b) Derechos de usuario
c) Derechos de directorio
d) Atributos de los archivos.

- Operando en equipos AT y PS/2 (50 en adelante) es una versión del tipo 286 Nivel I, cuenta con la utilería HOT FIX, que se encarga de detectar sectores que pudieran estar dañados del disco duro para no ser utilizados.

- ELS Netware 286 V2.15 Nivel II povee servicios de red a PC's, Macintosh y estaciones de trabajo OS/2.

- Se requiere el Netware para Macintosh, para soportar las estaciones de trabajo Macintosh, para las estaciones de trabajo OS/2 se necesita el Netware Requestor.

6.6.d Advanced Netware V 2.15

- Presenta todas las ventajas señaladas en caracteristicas generales.

- Esta versión es para un número grande de usuarios.

- Puede instalarse en forma dedicada o No dedicada, para equipos del tipo PC-AT y 386 o para equipos PS/2 IBM modelos 50,60 y 80.

- Permite la formación de cualquier cantidad de puentes internos y externos.

- Operando en equipos AT y PS/2 (50 en adelante) es una versión del tipo 286 Nivel I, cuenta con la utileria HOT FIX, que se encarga de detectar sectores que pudieran estar dañados en el disco duro para no ser utilizados.

- Advanced Netware V2.15 provée servicios de red a PC's, Macintosh y estaciones de trabajo OS/2.

- Se requiere el Netware para Macintosh, para soportar las estaciones de trabajo Macintosh, para las estaciones de trabajo OS/2 se necesita el Netware Requestor.

6.6.e System Fault Tolerant (Novell SFT Netware 2.15)

Sistema tolerante a fallas de Novell.
Además de contar con las características generales de Netware, este es el sistema operativo tolerante a fallas cuyas ventajas principales son:

- Manejo de dicos en espejo: Capacidad para manejar dos unidades con disco duro de capacidades similares en forma de espejo, evitándonos caídas del sistema por fallas en disco. Todo ésto en forma automática y transparente para el usuario.

- Duplicidad de discos: Se refiere a la capacidad de manejar dos unidades de disco duro en espejo, cada uno de ellos conectado a su tarjeta controladora. Dicha capacidad no protege de caídas en el sistema debidas a fallas de disco o tarjeta controladora. Todas las escrituras a disco se harán por duplicado, pero las lecturas las hará la cabeza del disco que se encuentre más cercana.

- Transaction Tracking System: (Sistema de Registro de Transacciones). Esta facilidad permite evitar que algún desperfecto en el equipo, ya sea por pérdida o falla de corriente, afecte a una serie de archivos relacionados entre sí en el momento de la interrupción. Si la transacción no se hizo completa no se efectúa la actualización de los archivos en ningún caso.

- Monitoreo de Unidades de Potencia ininterrumpible (UPS): el UPS se conecta al servidor y le ordena que de de baja la red si la energia externa se mantiene fuera de rango por un tiempo largo.

- SFT Netware V2.15 provee servicos de red a PC's, Macintosh y estaciones de trabajo OS/2.

La figura 7.1 es un cuadro de especificaciones técnicas de los productos tradicionales Netware de Novell.

CARACTERISTICAS / NETWARE	ELS I V2.0A	ELS II V2.15	ADVANCED NETWARE V2.15	SFT NETWARE V2.15	NETWARE 386 V3.0
PARA PROCESADORES	286,386	286,386	286,386	286,386	386
MODO DE OPERACION	NO DEDICADO	DEDICADO NO DEDICADO	DEDICADO NO DEDICADO	DEDICADO	DEDICADO
No. USUARIOS / SERVIDOR	4	8	100	100	250
SERVIDORES MULTIPLES	NO	NO	SI	SI	SI
CONEXION ENTRE REDES (No DE TARJETAS)	NO (0)	NO (0)	SI (4)	SI (4)	SI
CAPACIDAD DE COMUNICACION	NO	SI (1 CONEXION REMOTA)	SI (MULTIPLES)	SI (MULTIPLES)	SI (MULTIPLES)
HARDWARE SOPORTADO	3	48	48	48	48
HOT FIX	SI	SI	SI	SI	SI
ESPEJO EN DISCOS	NO	NO	NO	SI	SI
DUPLICIDAD DE DISCOS DUROS	NO	NO	NO	SI	SI
TTS	NO	NO	NO	SI	SI
MONITOREO UPS	NO	SI	SI	SI	SI
REQ. MINIMOS DE MEMORIA	640 Kb. BASE 512 Kb. EXT.	1Mb DEDICADO 2 Mb NO DEDICADO	1 Mb DEDICADO 2 Mb NO DEDICADO	1 MB DEDICADO	2 MB DEDICADO
SOPORTE A MACINTOSH	NO	SI	SI	SI	SI

6.6.f Netware 386 V3.0

- Séptima generación del producto
- Para procesadores 386 y 486
- 250 usuarios
- Soporte a DOS, OS/2, MAC, VAX, UNIX, etc.
- Capacidad muy grande en disco (32 Tera Bytes)
- Archivos de hasta 4 Gigabytes
- Niveles de seguridad a nivel archivo
- 16 impresoras locales o del server

Productos avanzados

Netware para OS/2
Netware para Macintosh
Netware para VMS (VAX)
Netware para UNIX
Netware Transportable

Estrategia de Novell:

- Soporte a múltiples protocolos estándar (Arcnet, Ethernet, Token Ring, otros)
- Soporte a múltiples sistemas operativos de la estación de trabajo (DOS, OS/2, Macintosh, XENIX/UNIX)
- Soporte a diferentes plataformas de servidor (286, 386, Mini, mainframe)
- Soporte a diferentes estándares de comunicaciones (IPX, TCP/IP, OSI, X.25, SNA, asincrono)

CAPITULO VII
SOFTWARE PARA REDES

El software de aplicaciones es como la sangre de las PC. Las hojas de cálculo, los procesadores de palabra, las bases de datos y otras aplicaciones hacen de la PC una potente herramienta. Al conectar su PC a una red las aplicaciones más comúnes instaladas en su PC monousuario sufren algunos cambios que vere a continuación.

7.1 Hoja de calculo.

La hoja de cálculo más popular en la actualidad es LOTUS 1-2-3 y es la que tratare en este punto. La primera pregunta que surge al instalar una red es ¿Puedo usar este mismo paquete en la red?. Desafortunadamente, la utilización de software monousuario en un entorno en el que varios usuarios intentan acceder simultáneamente a la aplicación, puede ocasionar problemas inesperados. Por lo general la mayoria de los fabricantes de los paquetes más populares ya ofrecen versiones para LAN. Como la versión LOTUS para LAN, la cual puede ser utilizada por varios usuarios. En este punto tratare la versión de LOTUS 2.01 para monousurio instalada en un entorno LAN. Independientemente de los aspectos legales que se derivan de la violación de la licencia al utilizar un paquete autorizado para un usuario con varios usuarios, veremos los problemas que pueden surgir prácticamente al usar la red.

Puede copiar Lotus 1-2-3, versión 2.01, en el servidor y permitir que varios usuarios tengan acceso a una copia del paquete. Esto funcinará debido a la forma en que los archivos de programas de

1-2-3 son manejados en el servidor.

En cuanto se copian en el servidor, los archivos de programas se marcan como normales: como archivos no-compartibles, lectura y escritura. Cuando escribe 1-2-3 en el indicador de órdenes y pulsa [Enter], Netware procede de esta forma.

1. Va al disco duro del servidor por una copia de los archivos de órdenes y ejecutables de 1-2-3.

2. Copia los archivos en la RAM del servidor (y cierra los archivos del disco duro).

3. Transmite los archivos a través de la LAN a la estación de trabajo desde la que fueron requeridos.

4. Cierra los archivos 1-2-3 en la RAM del servidor.

Desde que los archivos se cierran, cualquier otro usuario de la red podrá abrirlos de nuevo siempre que disponga de los derechos de búsqueda, Apertura y Lectura en el directorio correspondiente.

En esencia, cada estación de trabajo recibe y ejecuta 1-2-3 como una aplicación monousuario. Sólo ocurre que es la misma copia de los archivos de programas. netware gestiona la apertura y cierre de archivos de forma fiable. El inconveniente es que se experimenta un ligero retraso al acceder a 1-2-3. Así pues, usted y otro usuario, digamos VANESA, pueden estar contentos. Sin embargo, aparecerán algunos inconvenientes.

Suponga que usted entra a una hoja de cálculo para realizar algunas modificaciones y unos minutos después el usuario VANESA entra a la misma hoja de calculo para realizar SUS modificaciones. Si usted salva su hoja antes que VANESA, al volver a accesarla encontrará la hoja que modificó VANESA y no la suya.

La versión 2.2. de Lotus 1-2-2 ya implementa un sistema de *reserva de archivo* que evita reescribir inadvertidamente los cambios de un usuario sobre los realizados por otro. Desafortunadamente la versión 2.01 es únicamente monousuario y no multiusuario.

Existen otros inconvenientes como son la unidad de disco que 1-2-3 apunta al iniciar una sesión y que en una red puede resulta muy confuso. Otro problema podría ser el direccionamiento a la impresora. Estos problemas son relativamente fáciles de resolver, más no se puede decir lo mismo respecto al primer problema.

Como conclusión podemos decir que aunque se puede utilizar un paquete monousuario en un ambiente LAN lo mejor es no hacerlo sino adquirir uno específico.

7.2 Base de Datos.

Las bases de datos son quizá la aplicación más importante en una red y por lo mismo se debe tener especial cuidado en su manejo y seguridad. En una base de datos grande no querrá que todos los usuarios tengan acceso a toda la información. En este punto trataré uno de los paquetes más populares en México de manejo de base de datos. El Dbase III Plus.

En un ambiente de red, donde varios usuarios deben compartir la misma copia de dBase III PLUS y almacenar archivos en el mismo disco duro, es necesario prevenir que ciertos usuarios puedan correr algunos programas, leerlos o actualizar determinados archivos.

Otro problema de seguridad al usar dBase III Plus es la protección de archivos en disco, proteger contra el daño que causaría el que dos usuarias actualizaran los datos simultáneamente. Cuando un usuario ejecuta una operación que implica actualización en gran escala de la base de datos, el archivo entero debe cerrarse a otros usuarios. Cuando los registros se actualizan uno por uno, con los comandos de edición de pantalla completa o con un programa de actualización, sólo es neceario asegurar que dos usuarios no podrán escribir en el mismo registro al mismo tiempo.

Como en el caso de Lotus 1-2-3, dBase III Plus en su versión monousuario puede ser cargado en un servidor en ser utilizado en un ambiente LAN. De hecho, existen comandos de programación en dBase que nos permiten tener cierto control y seguridad. Sin embargo, es más conveniente contar con paquetes para aplicación en

red.

7.2.a Structured Query Language.

Usando en programa de base de datos del punto anterior implica una carga grande para el servidor y entre más crecen nuestros datos mayor será la carga.

El surgimiento del servidor de base de datos, representa una nueva tecnología en la administración de datos. Los servidores de base de datos introducen un concepto operativo del servidor del cliente (front end/back end). Esto significa que un nodo de la red maneja las solicitudes de base de datos en el back end del sistema, en su mayor parte en un servidor de archivo y genera resultados en las estaciones de trabajo del front end. El servidor de base de datos integra las solicitudes desde todas las estaciones de trabajo, como reducción de números, transacciones de datos, acceso de archivos e implementaciones de datos. Los resultados computados son enviados de regreso a las estaciones de trabajo.

El Structured Query Language (SQL) es un lenguaje universal, compuesto de 18 comandos para los sistemas de Administración de Base de Datos Relacionales (RDBMS). El SQL no solamente simplifica los procedimientos de recuparación de datos, sino que también proporciona un estándar de lenguaje de base de datos. Además, el SQL hace que la información sea intercambiable entre los archivos de base de datos bajo diferentes medios ambientes operativos.

El SQL es un lenguaje de alto nivel capaz de procesar un paquete de comandos con un solo mandato. Una sola línea de comando del SQL puede producir el mismo resultado que el generado hasta por 15 declaraciones de dBase.

IBM fue el primero en introducir el SQL para su RDBMS DB2 bajo la plataforma de la Arquitectura de Aplicaciones de Sistemas (SAA) de IBM. Ahora está teniendo un papel importante en la industria de las redes. El TCP/IP conecta a los host Unix y Xenix junto con los servidores de archivo DOS y OS/2. En dicho ambiente el SQL hace que los datos puedan ser compartidos entre los host.

Un servidor de base de datos SQL proporciona una solución basada en el servidor cliente, así como todos los servicios de SQL. En un medio ambiente de red heterogeneo, el servidor SQL no sólo trata con las solicitudes SQL de los usuarios de redes locales, sino que también actúa como un coordinador de datos con otras bases de datos SQL de la red. Las solicitudes de las estaciones de trabajo basadas en el cliente, pueden extenderse para tener acceso a los datos de SQL, almacenados bajo otros ambientes operativos. Por ejemplo, Una hoja de cálculo Excel de Microsoft controlada por archivo de escritura, integra los datos automáticamente desde una base de datos Oracle bajo Unix, un archivo de datos SQL de FoxBase bajo Xenix, un archivo de dBase bajo DOS y un archivo Paradox SQL bajo OS/2. Hace todos los trabajos de reducción de números en la hoja por sí mismo, traza gáficas y envía resultados actualizados a cada archivo de datos SQL individual. Todo gracias a la magia de los servidores de base de datos SQL.

Integridad de los datos. Los desastres como discos duros o archivos de datos dañados ya no son un problema para los administradores de datos de red SQL. Una base de datos SQL automáticamente crea registros diarios que salvan las imágenes de transacciones de datos completas. El comando integrado ROLLBACK

ayuda a rastrear los datos hasta el punto de la falla del sistema. El comando COMMIT WORK protege los datos de los daños causados por una operación inapropiada, por ejemplo, un paro del sistema con los archivos abiertos.

Además del archivo automático y del seguro de registro para el medio ambiente de multiusuario, se ofrece un seguro de servidor de base de datos, para hacer que el contro de procesamiento SQL sea inmune a todos los errores creados por los usuarios y los programadores.

Virtualmente todos los fabricantes de RDBMS están comprometidos con el desarrollo de productos de SQL. Microsoft y Ashton-Tate conjuntamente lanzaron su producto de servidor SQL. Apoyando a las aplicaciones de fornt end, están el dBase IV, Paradox, DataEase, Clipper y Advanced Revelation. Existen muchos más paquetes SQL apoyados por diversos fabricantes y para aplicaciones en diversos sistemas operativos. Mi intención en este punto es sólo dar a conocer una parte del potennciai de las LANs y el desarrollo que está surgiendo en la industria de la computación a raíz de esto.

La tecnología SQL es un tema muy amplio y complejo que se puede consultar más a fondo en los libros de referencia.

7.3 Programacion en redes.

En este punto pretendo presentar los comandos a utilizar cuando se programa en un ambiente de redes utilizando dBase III Plus y/o Clipper. Se supone un conocimiento previo de programación. No prentendo presentar una guia de programación ni mucho menos ya que eso seria muy largo. Por otro lado, siendo dBase III Plus y Clipper bastante populares en nuestro pais y una muy buena herramienta de programación, es importante consideración su aplicación en un ambiente multiusuario.

Como comenté anteriormente, el principal problema al trabajar en red una base de datos, es mantener la integridad de nuestros archivos. Imaginen el problema de dos o más personas tratando de modificar la misma base de datos al mismo tiempo. ¿Cuáles datos serian los que finalmente se mantendrian presentes? Y si alguien quisiera consultar información en ese momento, ¿Qué le mostraria la pantalla?

Para evitar estos problemas, existen una serie de comandos en dBase y en Clipper los cuales podemos y debemos usuar al programar en red.

El primer aspecto a considerar en la programación en redes es el modo de funcionamiento del archivo. Si vamos a utilizar un archivo para escritura su modo es EXCLUSIVO. Si se va a accesar para lectura, consulta, etc. su modo es COMPARTIDO. De esta manera debemos de considerar si una instrucción debe ser exlusiva o compartida. Por ejemplo, la instrucción INDEX, debe ser usada en modo exclusivo ya que no se podria indexar la misma base al mismo

tiempo con dos parámetros distintos.

Cuando se trabaja en red y no se toman las precauciones debidas, será muy común el encontrarse con mensajes de error debidos a los conflictos creados. Para evitar esos errores, nuestro programa debe incluir mensajes como el siguiente:

" Archivo en uso.....[opción] "

Dentro de las opciones podemos considerar:

- Reintentar
- buscar otros datos
- Regresar a un menu de opciones

Los tipos de reintentos pueden ser:

- Una vez
- Un tiempo fijo
- Hasta que se interrumpa
- Combinación de 2 y 3
- Hasta lograr el acceso (FOREVER)

Comandos Principales.

Comandos que requieren exclusividad:

1) Nivel registro

REPLACE	Al utilizar estos comandos
DELETE	previamente debe de indicar
RECALL	su exclusividad. De no hacerlo
@...GET...Campo	aparece el siguiente mensaje:
APPEND BLANK	"System Error Not Locked"

El comando que nos da la exlusividad de un solo registro es

RLOCK()	
REC_LOCK()	Funciones logicas que retornan un valor F o T.

El comando que nos da exclusividad cuando se manejan multiples resgistros es

FLOCK()
FIL_LOCK()

2) Nivel archivo

```
PACK
REINDEX
INDEX ON
ZAP
```

El comando que nos da exclusividad del archivo es

```
USE archivo EXCLUSIVE
```

Comandos que no requieren exclusividad:

```
SEEK
LIST
REPORT FORM
LABEL FORM
GO TOP
GO BOTTOM
GO RECNO()
```

Otros comandos:

UNLOCK — se utiliza para desbloquear el registro o el archivo.

Nota: Es muy importante utilizar este comando inmediatamente después de utilizar nuestro registro o archivo para así permitir el acceso a los demás usuarios de la red.

NETERR() — Determina si fallo un USE o USE ...EXCLUSIVE Si es así retorna un valor verdadero .T.

APPEND BLANK — En un ambiente de red intenta agregar un registro en blanco y si lo consigue lo bloquea. Ya no es necesario utilizar un RLOCK().

NETNAME() — Devuelve el identificador de la terminal, es de 15 caracteres.

SER EXCLUSIVE ON — Cualquier archivo que abra después de ejecutar este comando será de modo exclusivo.

CAPITULO VIII

CONECTIVIDAD

8.1 MINIS Y MAINFRAMES

Las minicomputadoras y los mainframes son máquinas con una mayor capacidad de procesamiento y almacenamiento de información. Aunque la tecnología de las PC's está acortando cada vez más la diferencia entre las PC's y las minis y mainframes, estos últimos siguen siendo muy utilizados sobre todo para el manejo de grandes volúmenes de información. Su integración como parte de una red local es importante y lo trataré a continuación.

El principal fabricante de mainframes es IBM y como sabemos lo que hace IBM tiene gran impacto en la industria de la computación. No obstante que las PC's surgieron a partir de IBM y se han convertido en un estandar mundial, IBM sigue diseñado y fabricando equipo que lo diferencie de los demás aunque en ocasiones la única diferencia es el nombre y el precio. Sin embargo, la inflencia de IBM no puede pasar desapercibida.

Cuando se habla de IBM y su conectividad siempre surgen dos palabras fundamentales: SNA y SAA. Por esta razón, empezaré haciendo un breve análisis del significado de cada una de estas palabras.

SNA. System Network Architecture. Es el esquema global de comunicaciones y redes de IBM. Creado en 1974, SNA define diversos protocolos actuando en 7 capas superpuestas, equivalentes en gran medida a las 7 capas del modelo OSI.

SNA no es un producto en sí mismo, sino toda una arquitectura que siguen diversos productos de software y hardware. Por ejemplo, SNA

define en el nivel 2 un protocolo denominado SDLC (Synchronous Data Link Control), de manera que las conexiones de hardware que se establecen dentro de SNA, deben respetar dicho protocolo.

La figura 8.1 ilustra los 7 niveles de SNA.

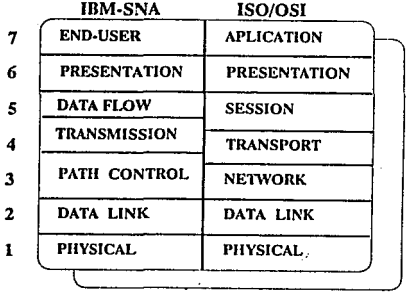


Fig. 8.1 Estructura general de SNA y su comparacion con OSI.

Dado que SNA fue creado en 1974 y a partir de entonces la tecnologia de comunicaciones ha evolucionado en gran manera, lógicamente SNA ha tenido que evolucionar y modificarse en algunos sentidos. Tal es el caso de la incorporación de nuevos protocolos como el APPC o de nuevas formas de enlace como Token Ring.

SNA fue creado con una visión arquitectónica netamente jerárquica: Un procesador central (nivel 5) platicando con controladores de comunicaciones (nivel 4), los cuales a su vez dialogan con controladores de terminales (nivel 3), que tienen conectadas diversas terminales (nivel 2). Los elementos más importantes en esta jerarquía, así como la numeración típica de cada uno de ellos

son: Controladores de comunicaciones 3725 ó 3745, genéricamente 37XX. Cluster controllers 3274 ó 3174. Terminales 3278, 3279, 3178, etc. todas pertenecientes a la llamada familia de terminales 3270. En una terminología común en lugar de decir controlador de comunicaciones XXXX le llamaríamos Procesador Frontal.

Dentro del mundo SNA, existen tres términos muy importantes para entenderlo: Unidades Físicas o PUs, Unidades Lógicas o LUsy sesiones. En palabras sencillas, una unidad física es un cierto tipo de hardware. Una unidad lógica se puede ver como un "puerto" de software, o como la categoría de software que puede tener un dispositivo. Y una sesión es la plática que se establece entre dos unidades lógicas.

SAA. En 1987, IBM lanzó al mercado SAA. Pero contrario a lo que muchas personas piensan, SAA no es ningún producto concreto, sino el compendio de diversos estándares, normas y documentos, enfocados a que las aplicaciones desarrolladas en un ambiente, puedan ser migradas a otros ambientes prácticamente sin cambios. De ahí su nombre SAA o System Application Architecture.

Así por ejemplo, una aplicación desarrollada en PC's bajo la normatividad que sugiere SAA, podrá ser tranpostada prácticamente sin cambios a una mini o mainframe. Lo que a veces IBM se olvida de comentar es que aunque las especificaciones de SAA se hayan publicado, no significa que al día siguiente ya sean utilizadas. En otras palabras, muchas de las promesas de SAA apenas están siendo realidad.

Para que una aplicación sea tranportable, deben existir "elementos comúnes" en los diversos ambientes: El mismo lenguaje de

programación, el mismo tipo de base de datos así como su lenguaje de acceso, la misma forma de utilizar el teclado y la pantalla, los mismos protocolos de comunicación, etc. Todos estos elementos comúnes son los que forman SAA. La figura 8.2 muestra una red local que integra PC's y minframes IBM.

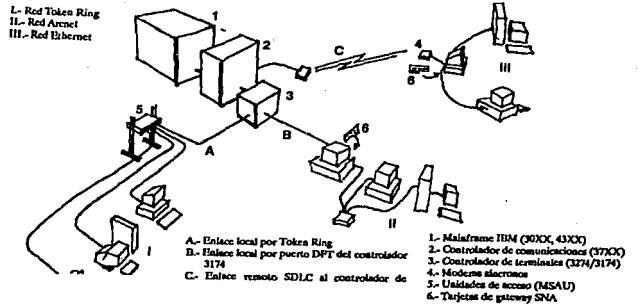


Fig. 8.2 Red local con Pc's y mainframes IBM

Vale la pena comentar que como SAA no es un producto marca IBM, cualquier empresa de hardware y/o software, puede decidir adherirse a dichos estándares y fabricas sus productos basados en éste. Es importante también decir que entre los ambientes de IBM (micros, minis y mainframes) la disparidad total que existía y todavía existe entre las aplicaciones de uno a otro ambiente, hacían muy complicado el transportarlas entre ellos mismos. Incluso dentro de la misma familia IBM no existía compatibilidad total. Por lo tanto, el compromiso de IBM fue SAA.

Token Ring y APPC. IBM basa su estrategia de enlazar equipos en la utilización de Token Ring si se trata de hacer la conexión local y

en líneas SDLC si es remota. Lo relativamente nuevo es tener puertos Token Ring directamente en las minis y mainframes IBM, sin tener que utilizar los enlaces normales de terminales.

Este tipo de enlaces directos presentan ventajas importantes pero también un nuevo reto: Por una parte tenemos un enlace rápido (4 ó 16 Mbit/seg.) y no tenemos que estar "engañando" al mainframe al conectar PC's como terminales ordinarias, sino más bien el mainframe se torna en un nodo más de la red. En concepto el enlace es DEMOCRATICO. Pero por otra parte, para aprovechar esta democracia requerimos del mismo tipo desoftware en ambas partes: En las PC's y en el mainframe.

El concepto de DEMOCRATICO, se explica de la siguiente manera. Si ya tenemos un medio físico de enlace (Token Ring) que no establece distinción entre un nodo PC y un nodo mainframe, los nodos pueden comunicarse entre sí a cualquier momento y sin distinciones. Lo que se requiere ahora es el mismo protocolo superior, que permita que la democracia no se quede sólo en el hardware, sino que se extienda al software para que el flujo de datos e información sea constante. Dicho protocolo equivaldría a que los programas de aplicación pudieran utilizar una serie de comandos tales como: Envia-información, Espera-a-recibir, verifica, etc. para enviar y recibir información y algunos más de control que permitan establecer y terminar la comunicación.

Lo anterior es precisamente lo que hace APPC (Advanced Program to Program Communication), permite que un programa común lo llame a través de comandos tales como SEND o RECEIVE AND WAIT y establezca comunicación con otro programa en otra máquina. No importando en

que ambiente se encuentre el otro programa.

8.1.a Niveles de conectividad.

Nivel 1. Emulación de terminales: Si bien ésta es la forma más común de conexión, también es la menos avanzada. Bajo esta modalidad, el usuario mediante una serie de comandos, invoca a un programa que hace que la PC se comporten como una terminal. (Terminal tonta).

En ambientes IBM-mainframes, el tipo de terminal que se emula es generalmente una 3278 (familia 3270). La desventaja real para los usuarios, es tener que cambiar de ambiente, en vez de usar comandos de MS-DOS, ahora tendrán que utilizar comandos bajo MVS o VM, que son los sistemas operativos de los mainframes de IBM. Y si tienen suerte y casi todo es a través de opciones de menú, entonces al menos tendrán que pelearse un rato con el teclado que ahora se comportará como el de una 3278.

El proceso que sigue una terminal al comunicarse con el mainframe es el siguiente:

Cuando el usuario escribe un carácter en la terminal, ésta lo envía al CPU interrumpiendo el proceso ejecutado en ese monento. El CPU le responderá a la terminal, haciendo eco del carácter enviado, es decir, recibirá un carácter para comparar el 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. (Figura 8.3)

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, en ese 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 o fracaso del comando del usuario. En este caso el trabajo del CPU se multiplica por cada terminal, tienen que hacer el 100 % de las vadilaciones y cambios en la pantalla necesarios para que el proceso funcione.

Si la terminal tonta es una computadora personal con un programa de emulación de terminal su capacidad se desperdiciará en su totalidad, quedaria prácticamente reducida a teclado y monitor, el CPU no tiene ningún papel en este caso.

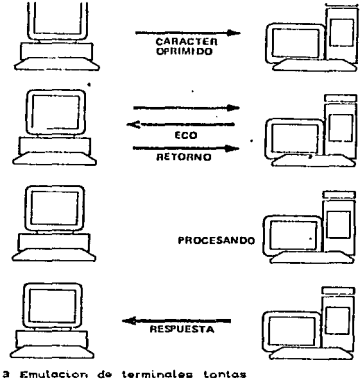


Fig. 8.3 Emulacion de terminales tontas

Nivel 2. Utilización de Interfases de Programación (APIs): Bajo este nivel, en vez de que el usuario platique con el mainframe emulando una terminal, es nuestro programa que corre en PC quien hace esas funciones, evitando que el usuario tenga que "ver" otro

ambiente que no sea MS-DOS. Imaginese que decide modificar una aplicación de dBase, ahora será el mismo programa de dBase, el que se conecte al mainframe, extraiga los datos y los utilice en la aplicación, sin que el usuario se ocupe de nada. Para realizar lo anterior, lo único que hicieron los programadores de dBase, fue revisar y utilizar una serie de funciones que casi todos los emuladores tienen, denominadas genéricamente Interfases de Programación o APIs (Application Program Interface). Es importante hacer notar que los APIs solo evitan que el usuario vea una terminal. Esto es, del lado del mainframe las cosas suceden exactamente igual que en el nivel 1.

Nivel 3. Comunicación programa a programa: Aunque el nivel 2 es un avance para el usuario, no presenta una mejora del lado del mainframe. En ambos casos la comunicación es de tipo jerárquica: estamos sujetos a que corra un programa en el mainframe y en la PC sólo se corre un emulador de terminal, por lo que el mainframe nos ve siempre como una terminal tonta.

A diferencia de lo anterior, cuando utilizamos alguna forma de comunicación programa a programa (Peer to Peer), el mainframe nos reconoce como "nodos inteligentes", capaces de iniciar una conversación.

Bajo este tipo de comunicación, en vez de emular una terminal, en cada PC corre un programa que platica con otro del mainframe y se dice entonces que se establece una conversación. Al establecer una conversación, la PC se olvida por completo de tener una emulación de terminal, ni siquiera a través de los APIs lo que viajará ahora por el canal serán comandos o datos entre los programas. APPC es

el protocolo propuesto por IBM para realizar conversaciones entre programas.

El modo de operacion es como sigue: (Fig. 8.4)

En la PC el usuario escribe todos los caracteres deseados sin ser enviados uno a uno al CPU, el envio al CPU de toda la cadena de caracteres se realiza hasta el momento en que se oprime [Enter].

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.

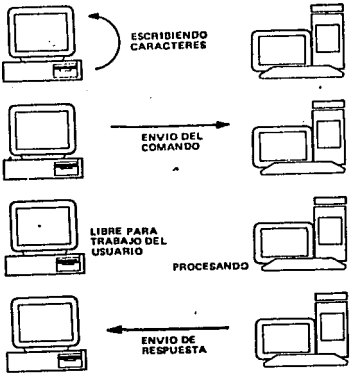


Fig. 8.4 Terminales inteligentes

8.1.b Formas de enlace.

Una forma de enlazar mainframes y PC's es a través del uso de Gateways. En forma sencilla, un Gateway es el enlace de una red local a otro ambiente, como puede ser el mainframe.

Dependiendo del tipo de conexión entre redes, ya sean locales o remotas será la instalación.

Conexiones locales. Se utiliza cuando la red de micros y el mainframe se encuentran relativamente cercanos y no es necesario utilizar ningún dispositivo adicional como modems. Existen dos formas básicas de conectar una red en forma local al mainframe:

Utilizar uno o varios puertos de un controlador de terminales

(3174) conectando a éste la tarjeta de Gateway que se montará dentro de una PC, o bien directamente teniendo el mainframe en Token Ring. Bajo esta última forma, se tiene un puerto Token Ring en el mainframe que se conecta a los MSAUs (MultiStation Access Units) igual que cualquier otro nodo de la red.

La diferencia entre estas dos formas, radica en el costo y la velocidad asociadas, como lo ilustra el cuadro de la figura 8.5.

	Sesiones	costo	Velocidad
Conexión al controlador de comunicaciones 37XX Líneas SDLC	16	bajo	baja
Conexión al controlador de comunicaciones 37XX (usando tarjetas con más memoria y procesador integrado) para líneas de alta velocidad	32-128	medio	media

Fig. 8.5 Resumen de enlaces locales.

Conexiones remotas. A diferencia de las locales, las conexiones remotas requieren de la utilización de módems y típicamente se conectan directamente al procesador frontal, por ejemplo a un controlador 3745.

El cuadro de la figura 8.6 resume los principales tipos de conexiones remotas.

	sesiones	costo	velocidad
Conexión a puerto DFT de controlador 3174	5	bajo	media
Conexión a puertos DFT de controlador 3174 usando MUX 3299	40	medio	media
Conexión TOKEN RING a controlador 3174	128	medio alto	alta
Conexión TOKEN RING a controlador de comun. 3725 ó 3745	128	alto	muy alta

Fig. 8.6 Resumen de enlaces remotos

Nota: Velocidad baja entre 2,400 y 9,600 bps.
Velocidad media entre 19,200 y 100,000 bps.
Velocidad alta entre 150,000 y 1 Mbps
Velocidad muy alta superior a 1 Mbps

8.2 UNIX Y MACINTOSH

Antes de iniciar a hablar de la forma en que se puede integrar el sitema operativo UNIX a una red local de computadoras PC, presento una breve introducción de lo que es UNIX.

UNIX es un sistema operativo ideal para aquellos que desean desarrollo de programas en una forma profesional y sin problemas pero, sin embargo tiene el inconveniente de ser un ambiente muy poco amigable. Unix es un sistema multiusuario y multitareas sumamente confiable y con varios años de existencia lo que lo hace más ventajoso en cierto sentido a, por ejemplo, Windows (que no es un sistema operativo sino una opción multitareas).

A primera vista Unix puede parecer similar a cualquier sistema operativo multiusuario: Se requiere una clave de usuario y un código de acceso para comenzar una sesión de trabajo; sin embargo, eso es todo lo que tienen en común.

Una sesión de trabajo puede consistir de la ejecución de un programa de aplicación, comunicación con sistemas remotos, o el uso de las herramientas del sistema operativo para procesamiento de textos y programación simple de aplicaciones.

Conceptualmente los sistemas Unix fueron diseñados para programadores y todas las herramientas disponibles en él están diseñadas con un grado muy alto de especialización, por ejemplo: en lugar de proveer un sofisticado editor de textos que permita dar formato a documentos, ordenar columnas, consultar y anexar el contenido de un directorio y mandarlo a la impresora, Unix provée un programa especifico a cada uno de estos requerimientos, y puede ser combinado en conjunto con otros para satisfacer la necesidad

del usuario. Unix es adecuado para que cada usuario puede configurarlo de acuerdo a sus necesidades y prioridades, y esto se puede lograr con o sin la ayuda del administrador del sistema.

Nadie niega que los comandos de Unix tienen nombres un tanto extraños, por ejemplo: Para ver el contenido de un directorio, el usuario "normal" ejecutará un comando DIR o CAT. Sin embargo Unix utiliza el comando "ls" que quiere decir "listar directorio". La brevedad de ese comando y otros de Unix permite re-teclearlo más rápidamente. Unix también permite ser utilizado por medio de Shells para generar menús más amigables e inclusive hay usuarios que no les interesa conocer en sí al sistema operativo sino simplemente correr su aplicación y listo.

Unix destaca también por su flexibilidad de programación y el manejo de aplicaciones que requieren gran volúmen de memoria y de procesamiento lo cual hace su integración a una red local, sobre todo en compañías grandes con grandes volúmenes de información, una muy buena opción.

El protocolo que permite la comunicación entre redes y Unix es el TCP/IP y Unix funciona con todos los productos bajo TCP/IP. Otra alternativa es Netware tranportable para Unix, que permite a los usuarios de un sistema operativo Netware ver al equipo Unix como servidor de archivos.

Existen otra gran variedad de productos que nos permiten la conectividad entre redes PC y ambiente Unix siendo algunos de ellos: HP LAN Manager/X HP-UX, POWERfusion with POWERfusion, Extras for DOS, Ported Netware, StarGroup LAN Manager Server, Atlantix Axcess y PC-NFS.

8.2.a Macintosh

Macintosh es otro tipo de computadora y sistema operativo propio que tiene una importancia relevante en el mercado de la computación. Por esta razón, es indispensable considerarlo como parte de una red local heterogenea.

Novell nos proporciona el Netware para Macintosh como un medio ideal para conectar Macibtosh con PC's. Sin entrar mucho en detalle, presentare las caracteristicas más importantes de Netware para Macintosh y la forma de instalarlo.

Existen diferentes versiones de Netware para Macintosh, siendo las más recientes las versiones 2.2 y 3.0 con caracteristicas adicionales. En forma general, todas las versiones permiten a los usuarios de la red trabajan en el ambiente que más les acomode sin necesidad de preocuparse que sistema está utilizando su compañero. Netware para Macintosh le proporciona al administrador la habilidad de tener usuarios de Macintosh como si fueran usuarios de MS DOS.

Netware para Macintosh convierte el servidor de archivo en un servidor Appleshare. Netware es compatible con protocolos AppleTalk (AFP) y el protocolo de acceso a impresión (PAP). Por lo tanto, el software AFP del cliente o usuario que forma parte del sistema operativo Macintosh puede arrancar o inicar su sesión directamente en el servidor Netware.

Las principales caracteristicas de Netware para Macintosh son:

* La habilidad para los usuarios Macintosh de accesar un servicios de archivo e impresión Netware de una manera consistente con la interfase de usuario Macintosh. Esto incluye integración de

archivo Netware dentro del menú de Macintosh.

* Compatibilidad con el sistema operativo Macintosh lo cual incluye el sistema de ventanas o archivos característico de Macintosh.

* La habilidad de aplicaciones AFP lo que permite a los usuarios intercambiar archivos de forma transparente.

* Compatibilidad total con los servicios de impresión de Macintosh. Netware toma las peticiones de impresión de Macintosh, saca los archivos de los paquetes, y direcciona la información a las colas de impresión de Netware.

* Usuarios de DOS y OS/2 tienen acceso a las impresoras MAcintosh.

* Compatibilidad total con seguridad AppleShare. Los usuarios Macintosh pueden limitar el acceso a folders y archivos y puden restringir la habilidad de otros usuarios de hacer cambios en ellos.

* Acceso de Macintosh a muchas de las características de funcionamiento de Netware incluyendo SFT, contabilidad y restricciones de login.

La transparencia entre Netware y AppleTalk en Netware para Macintosh 2.X y anteriores se obtiene por medio del servicio de puertas de protocolos SPG o Service Protocol Gateway. SPG convierte el protocolo AppleTalk como por ejemplo el AFP en un protocolo Netware y viceversa.

Para entender SPG, debemos examinar primero los componentes básicos de la red cliente-servidor. La figura 9.1 compara el modelo servidor-cliente con el modelo OSI. Los servicios

requeridos en una red pueden incluir archivos, impresoras y llamadas de acceso a gateways. Para que un cliente pueda solicitar apropiadamente un servicio y el servidor responda de igual manera, deben estar presentes tres capas de protocolos de comunicación. Estas son protocolos de medio y de acceso, protocolos de subred, y protocolos cliente-servidor. Los protocolos de medio y acceso se equiparan a las capas física y de enlace del modelo OSI. Netware es compatible con más topologías de red que AppleTalk la cual es compatible con topologías LocalTalk, Ethernet y token ring. El protocolo de subred se equipara a las capas de sesión, transporte y red del modelo OSI. Estas capas incluyen las reglas básicas que usan los nodos de red para comunicarse a través de la red, tales como el manejo de mensajes de error en caso de una falla del sistema. Otros ejemplos de protocolos de subred son Novell's Internet Packet Exchange (IPX), IBM's NetBIOS, and Apple's AppleTalk Transport Protocol (ATP) and AppleTalk Session Protocol (ASP). Los protocolos cliente-servidor son lineamientos que los clientes usan para hacer peticiones de servicio, tales como una petición para abrir o copiar un archivo, correr un programa o listar un directorio. Ellos corresponden a la capa de presentación del modelo OSI.

La capa de servicios de red corresponde a la capa de aplicaciones del modelo OSI. Aquí donde de hecho corren las aplicaciones. Cientos de aplicaciones compiladas en Netware o AppleShare corren en este nivel.

Con esto en mente, los gateways de protocolo de servicios trabajan de la siguiente manera. Netware para Macintosh trabaja entre el

protocolo cliente-servidor y la capa de servicios Netware del modelo cliente-servidor. Convierten la petición AFP del cliente Mac a NCP. Una vez que el servidor Netware atiende la petición (por ejemplo, abrir un archivo en particular y mandar un trabajo a la cola de impresión), el SPG convierte la respuesta de nuevo en AFP. El SPG puede residir en un servidor Netware o puente externo (figura 9.2).

Usando SPG, Netware para Macintosh une dos ambientes totalmente diferentes. Novell sigue a la vanguardia de sistema operativos para redes y con el concepto de conectividad cada día es más fácil conectar diferentes computadoras. Debemos estar al pendiente de las nuevas versiones de Netware y la serie de productos que salgan al mercado.

8.3 PUENTES Y RUTEADORES

Los puentes y ruteadores son dispositivos que nos permiten el crecimiento de una red local y su conectividad con otras redes locales u otros ambientes.

Al hablar de puentes y ruteadores se corre el riesgo de entrar en confusiones, muchas de ellas debidas al lenguaje, debido a la gran cantidad de dispositivos que cumplen con las características de ellos. En este punto trataré de definir con mayor claridad cada uno de estos dispositivos y sus características principales. Aparte de los puentes y ruteadores, existen los repetidores y los gateways. Los primeros nos sirven para amplificar la señal y así poder enviarla a distancias mayores. Muchos puentes y ruteadores ya tienen integrado un repetidor. Por gateways podemos entender que son puentes que conectan una red local con un mainframe con con una red con un ambiente diferente, en la literatura de redes podemos encontrar que se usa indistintamente el término puente (bridge) y gateway (sin traducción exacta al español).

Los puentes fueron diseñados en un principio como un dispositivo que permitiera el mejor manejo de una red local grande al poder dividirla en varios segmentos, es decir, el puente es el enlace entre varias redes locales. Los puentes superaron la limitación de distancia inherente en las topologías de red.

Por otro lado, el ruteador fue diseñado para conectividad de área amplia, direcciona paquetes de información basándose en capa de red del modelo OSI. Un ruteador selecciona el camino más eficiente de un dispositivo a otro disponible y dirige el tráfico. Los ruteadores ofrecen más características de control y administración

que los puentes, porque ellos están al pendiente de todo el movimiento en la red inclusive en otros ruteadores. Sin embargo, en la actualidad se pueden encontrar en el mercado, puentes que ofrecen las caracteristicas de los ruteadores y bisceversa. Es por eso que aparecieron nuevos términos como "brouters", "bridging routers" y "routing bridges".

Un puente, en su forma más simple, compara la dirección destino del paquete de datos con una tabla de direcciones de los nodos locales. Si el puente no encuentra la dirección en su tabla, sabe que la dirección destino es remota y la manda al siguiente segmento. Un puente Ethernet construye su propia tabla a partir de examinar la identificación de los paquetes enviados por todos los nodos activos de la red. Este es un puente "inteligente" y puede asimilar todos los cambios, bajas y altas que se den en la red.

Los puentes más sofisticados filtran los paquetes de información usando otros criterios además de la dirección destino, la dirección fuente, paquete de tramsmisión sencilla o multitransmisión y criterios definidos por el usuario.

Algunos puentes Ethernet son compatibles con el algoritmo del árbol, un algoritmo IEEE 802.1, el cual es indispensable en los puentes Ethernet que van a ser usados para construir WANs tolerantes a fallas ya que permiten enlaces reduntantes. Esto quiere decir que en una topología de bus Ethernet se pueden hacer círculos usando estos puentes. El algoritmo del árbol determina un camino único entre cada par de nodos, permitiendo que los puentes se coloquen en paralelo. Si el puente primario falla, el puente secundario se encarga de que no haya interrupción en el servicio.

Otros dispositivos de interconección proporcionan una mezcla de

puenteo y ruteo. Algunos permiten que el gerente de la red determine si trabajan como puente o como ruteador, pero sin la posibilidad de realizar ambas funciones simultaneamente. Otros rutearan o puentearan dependiendo de como se configuren. Los dispositivos con más caraterísticas deciden cual función realizar dependiendo de una especificación predefinida por el administrador de la red. Si se ha designado un tipo de protocolo específico, el dispositivo lo ruteara de acuerdo a ese protocolo. De otra manera sólo puenteara la información basándose en su nodo destino.

La habilidad para puentear o rutear es indispensable en ciertas redes multiprotocolo, como por ejemplo las que usan TCP/IP y LAT. TCP/IP es un protocolo de la capa de red y puede ser ruteado. Local Area Transport (LAT) es un protocolo que no opera en la capa de red y sólo puede ser puenteado.

Una vez más, dependiendo de las necesidades de la empresa y de su presupuesto se verá el equipo necesario para la red. Pero siempre debemos tener presentes a los puentes y ruteadores ya que son una opción de crecimiento y conectividad hacia otros ambientes.

CAPITULO IX

MANTENIMIENTO DE LA RED

9.1 EQUIPOS DE PRUEBA

Existen una gran variedad de dispositivos y equipos para mantenimiento de la red. En este punto consideraré los más importantes y de uso más común. Por otro lado, no debemos perder de vista el rápido crecimiento tecnológico en materia de redes locales y los equipos necesarios para mantenerse actualizados.

La gran mayoría de los problemas en redes proviene del cableado. Dividiendo el tipo de cable en dos: cobre (par trenzado y coaxial) y fibra óptica, discutiremos primero las herramientas para el cable de cobre.

Generador de tonos y detector.

Las figura 9.1 y 9.2 muestran el generador de tonos modelo 77M y el amplificador inductivo modelo 200B de Progressive Electronics, Inc. Ambos instrumentos han sido usados extensivamente en la industria telefónica para rastrear cableado de par trenzado entre campos enterconectados en habitaciones de equipo telefónico.

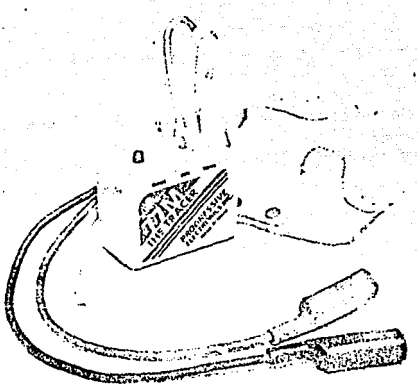


Fig. 9.1 genrador de tonos modelo 77M

Para identificar correctamente un cable, el generador de tonos es conectado a un extremo del cable. En el otro extremo, se conecta el amplificador inductivo el cual recibe la señal audible cuando este en el cable correcto. Estas herramientas son muy útiles para verificar la continuidad de un cable o para identificar un cable en particular.

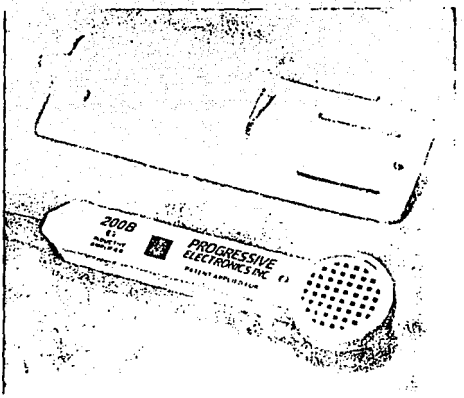


Fig. 9.2 amplificador inductivo modelo 2008

Rastreadores de cable.

Un problema primordial cuando se utiliza cable de par trenzado ya instalado en un edificio es localizar la trayectoria de cada uno de estos cables. El "enviador de cable" y "rastreador de cable" mostrados en la figura 9.3 proporcionan una solución a ese problema. El "enviador de cable" transmite una señal que puede ser recibida por el rastreador de cable a lo largo de un cable de hasta 30 metros de longitud. El cable oculto puede estar localizado dentro de cualquier piso, pared o cubierta y aún ser identificado por el rastreador si está localizado a 30 cm. de distancia del cable.

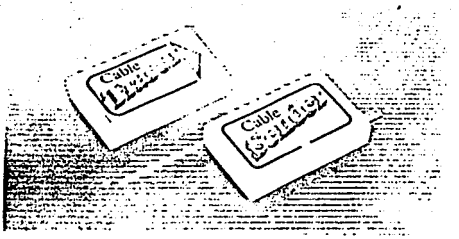


Fig. 9.3 enviador y rastreador de cable.

Probadores de continuidad.

La figura 9.4 muestra dos dispositivos llamados "checadores de cable". Estos dispositivos son muy simples y únicamente indican la continuidad o circuito abierto de un cable.

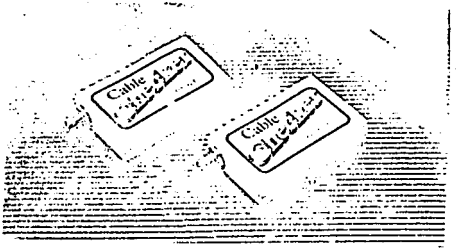


Fig. 9.4 Checadores de cable

Refectometro en dominio del tiempo (TDR)

Un TDR opera transmitiendo un pulso corto de amplitud y duración conocida a través de un cable, y midiendo la amplitud correspondiente y el tiempo de retardo asociado con cualquier señal reflejada. Circuitos abiertos y corto circuitos, impedancias incompatibles, torceduras, dobleces e imperfecciones en el cable tienen diferentes señales reflejadas que son analizadas y medidas por el TDR.

La figura 9.5 muestra un TDR. Además de corto circuitos y circuitos abiertos, el "Cable Scanner" puede medir resistencia terminal, nivel de ruido o interferencia en el cable de la red y tráfico de la red. Se puede conectar a un impresora y un osciloscopio.

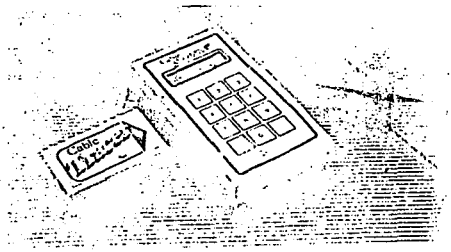


Fig. 9.5 TDR "Cable Scanner"

Fuente de poder optico y medidor.

Los cables de fibra óptica experimentan problemas similares a los de cobre con la diferencia que que la fibra óptica maneja señales

ópticas en vez de eléctricas. El equipo de prueba es necesariamente más complejo y costoso. Por ejemplo, un TDR para fibra óptica puede costar desde 10,000 hasta 50,000 dólares. Una solución más económica puede ser una fuente de poder óptica y un medidor óptico. El equipo se muestra en la figura 9.6 de Wilcom Products, Inc.. Su manejo es similar al generador de tonos mencionado anteriormente, con la fuente de poder conectada en un extremo y el medidor en el otro.

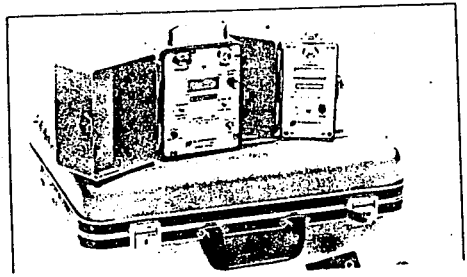


Fig. 9.6 Equipo de prueba para fibra optica.

Probador de voltaje.

La figura 9.7 muestra un dispositivo muy sencillo de usar, el monitor de CA. Cuando se conecta, el monitor indica la magnitud del voltaje de la linea de CA y lleva un registro de picos, condiciones de alto o bajo voltaje y fallas de voltaje. Una alarma audible nos previene de situaciones potencialmente dañinas para el equipo.

Un dispositivo más complejo es el mostrado en la figura 9.8. Con este instrumento se pueden hacer otras pruebas, medir la magnitud de la línea a neutro, ruido de neutro a tierra, los LEDs de diagnóstico indican que medida correctiva se debe tomar.

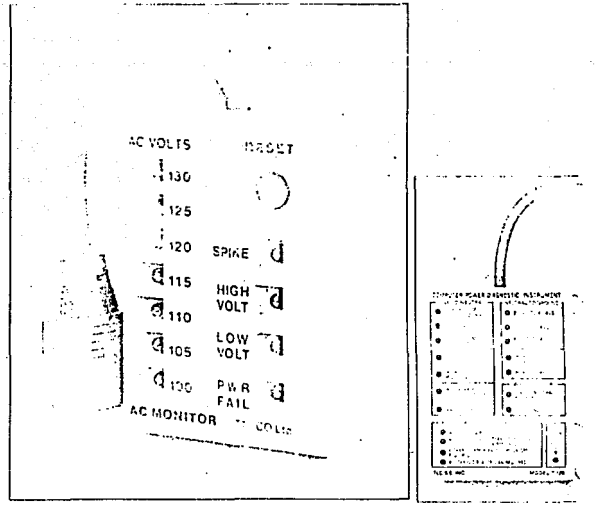


Fig. 9.7 y 9.8 dispositivos para el voltaje

Herramientas de prueba de interfases analogas.

Dada la naturaleza digital de las redes locales, puede facilmente pasarse por alto la necesidad de un equipo análogo de prueba. Tres dispositivos son valiosos y necesarios: un multimetro, . el osciloscopio, y el sistema de medición de fallas de transmisión (TIMS), la figura 9.9 muestra los puntos donde se deben usar equipos analógicos.

El TIMS se usa en la interfase entre la red y una linea telefónica análoga, el osciloscopio es usado para medir el ruido de la fuente de alimentación al servidor de la red o en el mismo cable de la red, y el multimetro se usa para varios propositos, como medir la resistencia de un terminador de cable o la salida de voltaje de la fuente interna de la PC.

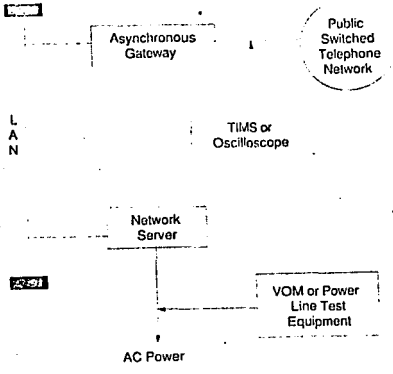


Fig. 9.9 Puntos de prueba para equipos analogicos.

Herramientas de prueba de interfases digitales.

Las señales digitales presentes en las interfases de una red a las PC's, impresoras, modems, y otros periféricos son los puntos de prueba más comunes. La figura 9.10 muestra una variedad de estos puntos y donde se deben conectar las herramientas. Analizaremos cada una de ellas.

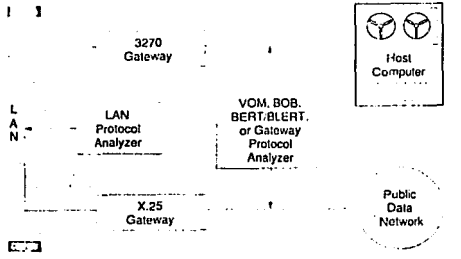


Fig. 9.10 Puentos de prueba para equipos digitales

Breakout Box (BOB)

Esta caja permite que el estatus de la interfase EIA-232-D entre el equipo terminal de datos (DTE) y el equipo terminador de circuitos (DCE) sea monitoreada. Su mayor importancia radica es su habilidad para reconfigurar la interfase abriendo un camino entre los pins correspondientes de los conectores de la interfase y reacomodandolos. De esta manera, un BOB puede ser usado para rápidamente configurar el cable de un modem. La figura 9.11 es muestra un ejemplo de un BOB que permite la reconfiguración de

todas las terminales de la interfase EIA-232-D.

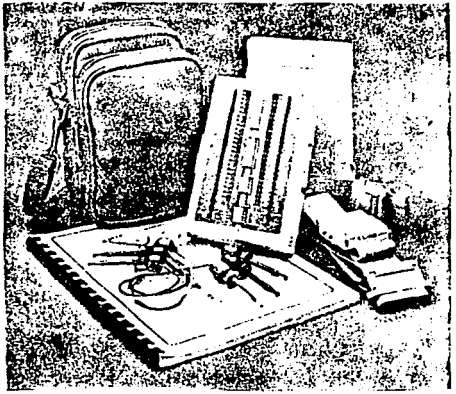


Fig. 9.11 BOB modelo DT-4

Trampa de pulsos (Pulse trap)

De conección similar al BOB, la trampa de pulsos monitorea las terminales seleccionadas de una interfase y visualmente lleva un registro de cualquier actividad (transiciones de alto a bajo o bajo a alto) que ocurran en esas terminales. Esto puede ser muy útil para registrar pulsos extremadamente rápidos que serían imposibles de visualizar en un BOB. La figura 9.12 muestra un dispositivo de este tipo fabricado por Datatran Corporation.

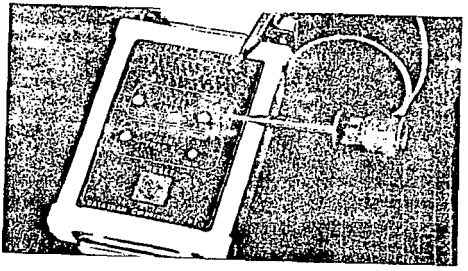


Fig. P.12 Rastreador de pulsos modelo PT-1

Cable inteligente 821 Plus (Smart Cable 821 Plus)

Existen tres productos fabricados por IQ technologies, Inc. que son muy buenos ahorradores de tiempo para una red. El cable inteligente 821 Plus, que se muestra en la figura 9.13, automáticamente configura una conección EIA-232-D entre dos dispositivos asincronos. Tres interruptores con LEDs indicativos, controlan las conecciones internas de la SC821. El primer interruptor selecciona el tipo de envio de información, en trayectoria recta o cruzada, el segundo interruptor configura las líneas de control y el tercero establece las líneas de conección. Un banco adicional de interruptores sirve para configuraciones especificas. Usando este dispositivo, se puede configurar un modem en menos de un minuto.

Medidor de datos inteligente 931 (Smart Data Meter 931)

Este dispositivo se muestra en la figura 9.14 y sirve para determinar los parámetros de la tranmisión de datos. Cualquier dispositivo compatible con EIA-232 puede tranmitir información al medidor de datos, y la pantalla nos dará el rango de bits, número

de bits de datos, paridad, y número de bits de alto. Este dispositivo también puede determinar los parámetros adecuados para un dispositivo únicamente receptor, como las impresoras, enviando diferentes combinaciones de parámetros hasta encontrar el adecuado. De esta manera, es relativamente sencillo determinar la configuración de un ainterfase server-impresora.

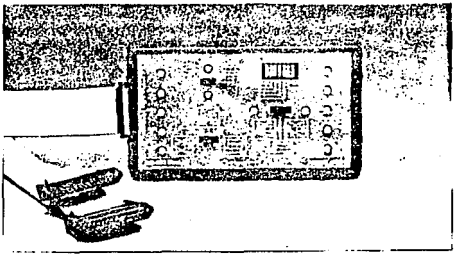


Fig. P.13 Cable inteligente D21 Plus

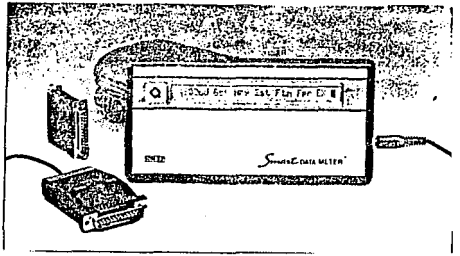


Fig. P.14 Medidor de datos inteligente D31

Medidor de datos asincrono inteligente (Smart Asynchronus Data Meter).

La figura 9.15 muestra el medidor de datos asincrono inteligente. Este modelo incluye la capacidad del cable inteligente y el medidor de datos inteligente, además de las caracteristicas del BOB y un probador de errores en Bits y Blocks (BERT/BLERT). El BERT/BLERT es un dispositivo de prueba de interfases digitales que compara la señal recibida con una señal de transmisión conocida para determinar si algún bit o block tiene errores. Un BERT/BLERT típico opera a varios rangos de información. También puedo que lleve incluidos paquetes de aplicación (en ROM) para varios protocolos de las capas 2 y 3, por ejemplo, asincrono, SDLC, X.25, etc.

Datatran Micropatch

Otra herramienta muy útil es el "Datatran Micropatch" de la figura 9.16 el cual puede ser usado para "cablear" un modem en un dispostivo compacto. Una vez que la configuración del modem ha sido verificada con un BOB, puede ser "cableado" dentro de esta pequeña caja logrando una conección directa entre DTE y DCE usando un mínimo de espacio. La unidad se cierra para evitar desconecciones accidentales.

Convertidores de interfase.

Similar en tamaño al microptach, el convertidor de interfase como el mostrado en la figura 9.17 proporciona un medio económico para usar equipo diseñado para cierta interfase en otra diferente. El modelo mostrado convierte de RS-232 a RS-422.

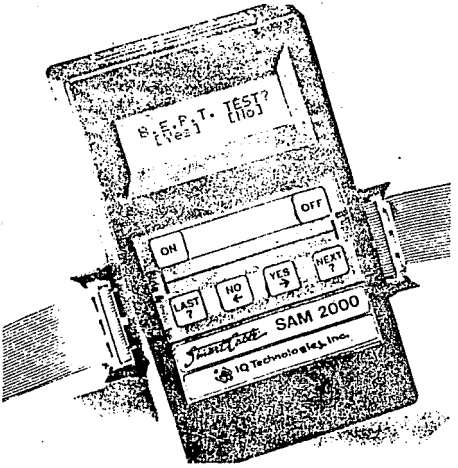


Fig. P.15 Medidor de datos sincronos inteligente

Fig. P.16 Datatran Micropatch

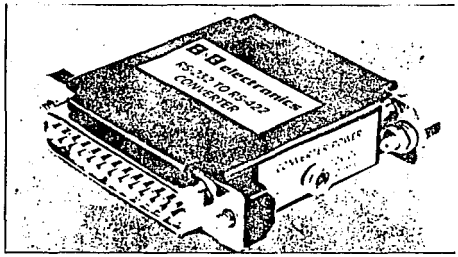


Fig. 9.17 Convertidor de interfase

Analizadores de protocolo.

Hasta el momento sólo hemos discutido equipos para prueba de hardware. Ahora veremos las herramientas que nos ayudan a resolver problemas de software.

Dos diferentes tipos de analizadores, mostrados en la figura 9.18, pueden ser usados con LANs. Un analizador de protocolo LAN conectado a una estación de trabajo de la red. Un analizador de protocolos "gateway" conectado a una interfase digital en el lado de salida de un X.25,3270 o gateway asincrona.

El analizador de protocolo de red puede capturar, registrar y analizar información transmitida en la red. Deben por lo tanto contener una tarjeta de interfase para una red en particular, y se conecta al cable de igual manera que cualquier estación de trabajo.

Los analizadores de Gateways realizan una función distinta a los analizadores de red. Los datos que van de una red a un gateway

pueden ser capturados por un analizador de red, pero esto no asegura la operación adecuada del gateway. Sólo un análisisa la salida del gateway puede hacerlo. Para una confirmación definitiva de la operación del gateway, la información que entra y sale puede ser capturada por ambos analizadores y luego ser comparada.

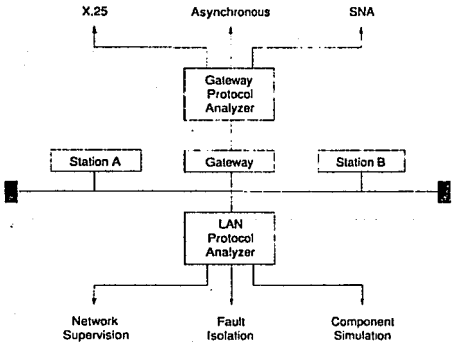


Fig. 9.18 Analizadores de protocolo

¿Que herramientas realmente necesito?

Como he dicho anteriormente, existen una gran variedad de herramientas de diagnostico, tanto para el hardware como el sofware. El tipo de herramientas con el que se cuente depende en gran parte del presupuesto de la empresa y de la importancia del buen funcionamiento de la red. En general debe de observarse lo siguiente:

1. Obtenga herramientas de diagnóstico directamente del fabricante que proporciona el equipo de red. Estas herramientas son más económicas y proporcionan una buena ayuda.

2. Este preparado para fallas en el cableado. La mayoria de los problemas en una red están relacionados con los cables.

3. Tenga equipo disponible o acceso a este para checar las distintas interfases que compongan su red.

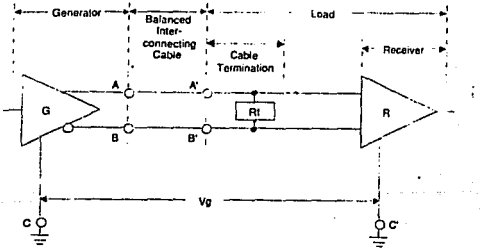
4. Si su red tiene multiples protocolos o gateways considere los analizadores de software. Si su red es muy grande (más de 100 nodos) un analizador de protocolos también será muy útil.

9.2 MANTENIMIENTO DEL CABLEADO

Como he mencionado anteriormente, la mayor parte de los problemas en una red tienen su origen en el cableado. Para analizar éste, primero veamos los antecedentes matemáticos.

Líneas de transmisión balanceadas y no balanaceadas.

Los términos "balanceado" y "no balanceado" se usan para describir las líneas de transmisión. Una línea balanceada es como la mostrada en la figura 9.19 y un ejemplo de una línea no balanceada es la figura 9.20.



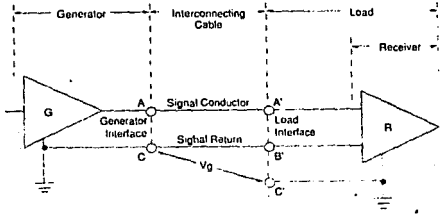
Rt = Resistencia terminal opcional
Vg = Diferencia de potencial a tierra
A, B = Puntos de interfase generador
A',B'= Puntos de interfase de carga
C = Tierra del circuito generador
C' = Carga del circuito a tierra

Fig. 9.19 circuito digital de intefase balanceado

En un diseño balanceado, las corrientes circulantes entre el generador y receptor en cada uno de los cables son iguales en

magnitud, pero de dirección opuesta. Los voltajes en estos conductores, con respecto a tierra, también son iguales en magnitud pero de polaridad opuesta. Una diferencia de potencial a tierra (Vg) puede existir entre el generador y el receptor. El cable de par trenzado es una ejemplo de una linea de transmisión balenceada.

El cable coaxial es una linea de transmisión no balanceada. La corriente circulante en el conductor de la señal regresa por medio de una conección a tierra que puede ser compartida por otros circuitos. Tanto la corriente como el voltaje en el conductor de la señal se mide con respecto a la señal del conductor de retorno.



A, C = Interfase generadora

A',B'= Interfase de carga

C' = Circuito de carga a tierra

C = Circuito generador a tierra

Vg = Diferencia de potencial a tierra

Fig 0.20 Circuito no balanceado

Para convertir una linea de transmisión no balanceada a balanceada, se utiliza un transformador llamado "balun". Usando baluns podemos utilizar cable coaxial dentro de una linea de par

trenzado. Los baluns son muy útiles en redes Ethernet y ARCnet ya que son una forma económica de reemplazar cable coaxial.

Diafonía

La diafonía es causada por el campo o efecto inductivo de una línea sobre otra. Este efecto es más pronunciado en cables con transmisión bidireccional, tal como el par trenzado. El efecto se muestra en la figura 9.21.

Fig. 9.21 Efecto inductivo

El efecto inductivo es medido en decibeles [dB], como sigue:

$$dB = 10 \log \quad Ps/Pe = 20 \log \quad Vs/Ve$$

donde las relaciones de Ps/Pe y Vs/Ve son potencias y voltajes respectivamente.

Este efecto se corrige manteneniendo los cables alejados de fuentes de interferencia conocidas como ruido.

El ruido se define como cualquier señal indeseable que entra a la línea de transmisión y perturba la señal comunicada. El ruido se clasifica de dos formas: Interferencia de radio frecuencia (RFI) producida por transmisiones de radio o televisión e Interferencia

electromagnética (EMI) producida por luces fluorescentes, motores, soldadores, etc. La figura 9.22 ilustra los efectos de RF y EMI en una línea de tranmisión.

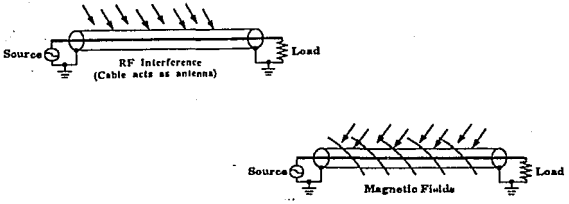


Fig. 9.22 Interferencia RF y MFI

Para medir los efectos del ruido tambien se utilizan los decibeles y es la relación entre la potencia de la señal y del ruido:

$$dB = 10 \log S/N$$

donde S y N son potencias de señal y de ruido, medidas en watts o miliwatts.

Efectos de diafonia y ruido.

La relación que tiene lo anterior con las redes locales radica en que tanta interferecia puede una red soportar y aún seguir funcionando adecuadamente. Dado que el ruido tiene un origen aleatorio es muy difícil determinar un posible problema, pero podemos hacer algunas generalizaciones.

El receptor ARCNET contiene un filtro muy sensistivo que pasa sólo las frecuencias de interés (5 MHz) y atenua otras frecuencias. Como resultado, ARCNET es muy tolerante a las fallas de ruido.

Los estándares IEEE 802.3 y 802.5 especifican las caracteristican que deben poseer los receptores y el nivel mínimo de señal recivida o de efecto inductivo (medido en milivolts o dB de atenuación). Dependiendo de que estándar usemos, las amplitudes máximas de ruido van de 50 a 300 milivolts. Cualquier señal de interferencia que exceda esos valores puede causar errores en los datos.

La mejor manera de evitar estos problemas, es mantener los cables lo más alejado posible de fuentes causantes de ruido como las mencionadas anteriormente.

Cable de par trenzado.

Las características eléctricas de los cables de par trenzado son básicamente cuatro: el calibre de los conductores, el cual determina la resistencia de CD en ohms por kilometro; la capacitancia mutua entre los dos conductores medida en picofarads por metro o por pie; la impedancia característica, Zo, medida en ohms a una frecuencia de referencia; y la atenuación en decibeles. La transmisión óptima se obtiene cuando la resistencia, capacitancia mutua y la atenuación del cable son mínimas. La impedancia característica se determina por la geometría y los materiales usados en el aislamiento y la constante del cable proporcionada por el fabricante.

Codigo de colores del cable de par trenzado.

La mayoría de los cables de par trenzado siguen los estándares de colores de la industria telefónica, el cual se basa en un grupo de 25 pares, conocido como grupo encuadernador. Para construir cables más grandes se añaden grupos de pares y así podemos tener cables

de 50 pares, 100 pares, etc.

El código de color está basado en los cinco colores primarios y cinco secundarios, los cuales proporcionan 25 combinaciones de color.

Color primario	Color secundario
Blanco	Azul
Rojo	Naranja
Negro	Verde
Amarillo	Cafe
Violeta	Pizarra

Por lo tanto, el par número 1 consiste de un conductor blanco con un trazado azul y un conductor azul con un trazado blanco. El par siete es rojo/naranja, el par 18 es amarillo/verde, etc.

Es muy importante indicar que las parejas de conductores deben de ser consistentes. Esto es, los dos conductores blanco/azul forman un par, pero un conductor blanco/azul con uno blanco/verde no lo forman.

Durante la instalación, en algún momento podrá necesitar determinar la distancia entre dos puntos de un cable de par trenzado. La manera más fácil de hacerlo es midiendo su resistencia con un multímetro. Conecte las terminales del multímetro a un par y cortocircuitue el mismo par en el otro extremo como se muestra en la figura 9.23. Esta medición puede hacerla inclusive con el cable ya colocado. Sin embargo, si ya está colocada, debe tener cuidado de que no contenga un circuito vivo. La resistencia en CD también puede obtenerse de una tabla como la siguiente:

Calibre	Resistencia CD (ohms/km)	Resistencia CD (ohms/kft)
22	53	16
24	84	26
26	134	41

Anote la resisntecia medida con el multimetro, y luego dividala entre el factor apropiado. Por ejemplo, 26 ohms/kft para un cable calibre 24. Esta medida será la distancia ida y vuelta del cable. Divida entre dos y tendrá la distancia de un extremo a otro.

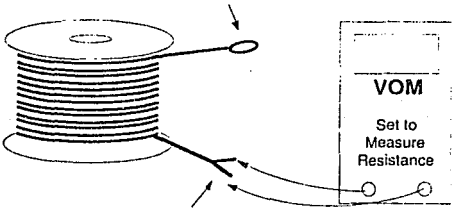


Fig. P. 23 Medicion de la longitud de un cable

Cable Coaxial

El cable coaxial tiene cinco caracteristicas eléctricas: la resistencia de CD, del conductor central y el externo; la

impedancia característica, Zo; la atenuación, la capacitancia entre el conductor central y el recubrimiento; la velocidad nominal de propagación (NVP) o velocidad de transmisión relativa a la velocidad de la luz en vacío; y finalmente el retardo de propagación medido en nanosegundos por pie (ns/ft). Como con el par trenzado, la operación óptima se obtiene cuando la atenuación y la capacitancia son mínimas. La impedancia característica, velocidad de propagación y retardo son usualmente parametros constantes determinados por los ingenieros en el diseño del circuito emisor y receptor.

Existen cuatro tipos de cable coaxial usados en redes locales.

Tipo de cable	Aplicación	Diametro	Zo (1 MHz)
Ethernet	IEEE 10BASE5	0.40 inch	50 ohms
RG-58A/U	IEEE 10BASE2	0.18 inch	50 ohms
RG-59/U	CATV, ARCNET	0.25 inch	75 ohms
RG-62/U	ARCNET, IBM	0.25 inch	93 ohms

Debido a la similitud en las fallas para los dos cables anteriores los consideraremos al mismo tiempo.

Todos los problemas de cable se pueden clasificar en dos categorias generales: aquellos causados por los conectores, terminadores o cualquier dispositivo mecánico; y aquellas fallas causadas por el cable en si tales como aberturas, cortocircuitos, torceduras, etc. En general los problemas causados por dispositivos mecánicos son más comunes. Veremos dos métodos para identificar estas fallas.

Prueba de continuidad o resistencia de CD.

Una prueba de continuidad simplemente mide la habilidad de una señal de CD para circular por una trayectoria continua, o un

circuito dentro del cable. Esta prueba es muy sencilla y se realiza con un multimetro. La continuidad o resistencia de los terminadores en una red son quizá lo más importante de esta prueba. Para terminadores con conección tipo N o BNC, se debe medir entre el conductor central del conector o su capa exterior. Para terminadores modulares (RJ-11 o RJ-45) se debe medir entre los pins o terminales adecuadas, usualmente las dos del centro. Consulte su manual de instalación para una prueba correcta.
La siguiente tabla muestra los resultados que se deben de obtener.

Tipo de cable	Resistencia del terminador
Ethernet	50 ohms
RG-58A/U	50 ohms
RG-59/U	75 ohms
RG-62/U	93 ohms
Par trenzado sin cubierta	100-120 ohms
Par trenzado con cubierta	150 ohms

La figura 9.24 muestra un cable Ethernet con terminadores de 50 ohms y un punto de acceso (que puede ser conector de terminal BNC "T"). Si se hace una medición de resistencia en el punto de acceso, se debe obtener un valor aproximado a los 25 ohms. Si la resistencia medida es muy diferente, digamos unos 80 ohms, que decir que un extremo del cable no está terminado adecuadamente. El circuito eléctrico equivalente se muestra en la misma figura, los terminadores colocados adecuadamente en paralelo proporcionan una medición de aproximadamente 25 ohms.

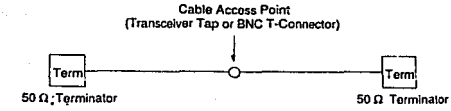


Fig. 9.24 Medición de terminadores Ethernet

Pruebas de reflectometros en el dominio del tiempo.

Un reflectómetro en el dominio del tiempo o TDR se construye como una combinación de un generador de pulsos, un probador de voltaje, y un amplificador de salida, alimentando una pantalla o un osciloscopio.

La operación del TDR es similar a un radar. Un pulso eléctrico de amplitud y duración conocida se transmite desde un extremo del cable. Cualquier cambio en la impedancia característica del cable causará una reflección del pulso transmitido. Si no existen fallas en el cable, y éste termina con su impedancia característica, no ocurre ninguna reflección.

Una gran variedad de problemas, como cortos, rupturas, terminadores inadecuados, dobleces, impedancias no compatibles (causadas al combinar dos tipos diferentes de cable) producen una gran variedad de pulsos o señales. La figura 9.25 muestra algunos ejemplos de estas fallas.

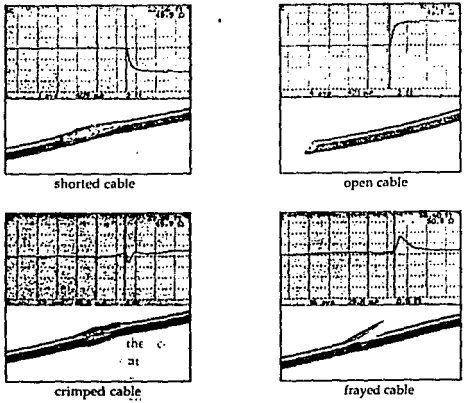


Fig. 9.25 Ejemplo de fallas detectadas con un TDR

Fibra optica.

Como he mecionado anteriormente, la fibra óptica es lo más reciente en cuanto a tecnología de comunicación y es una gran aportación al mundo de las redes locales.

Una conección simple de fibra óptica se muestra en la figura 9.26. En el transmisor, la señal de entrada conduce una fuente luminosa, ya sea un diodo laser o un LED. La fuente óptica opera en el espectro infrarojo, emitiendo luz en uno de los tres rangos de onda: 800-900 nonometros (nm), 1100-1300 nm, y alrededor de 1500 nm. La fuente óptica y el cable son diseñados para una transmisión óptima en uno de estos rangos.

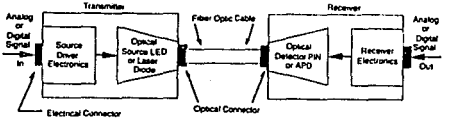


Fig. 9.26 Circuito de fibra óptica

En el receptor, un detector óptico consistente de un diodo positivo-intrinseco-negativo (PIN) o un fotodiodo avalancha (ADP) captura los pulsos de luz y los entrega al receptor electrónico. El enlace de transmisión óptica intermedio es de punto a punto y en este enlace lo más importante es considerar las posibles fallas. Un modelo de tres tipos de transmisión por fibra óptica se muestra en la figura 9.27. En el modo simple, la luz viaja a través de un sólo camino. Estos cables son usados para las aplicaciones de datos extremadamente altas como conversaciones telefónicas de larga distancia.. Los cables multimodo contienen muchos diferentes rayos de luz, y pueden ser índice tipo grada o índice graduado. En el cable de índice tipo grada, ocurre un cambio dramático entre el núcleo y el índice de refracción de la cubierta. En el índice graduado, ocurre un cambio más gradual. El primer cable emite un patrón de luz en forma de zigzag, y el segundo tipo de cable provee una luz más graduada.

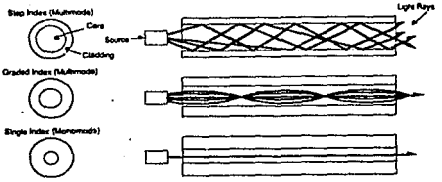


Fig. 9.27 Transmision por fibra optica

Para los dos cables multimodo, ocurre un fenómeno conocido como dispersión modal o esparcimiento del pulso de luz recivido. Cuando este esparcimiento de pulso ocurre, el receptor tiene dificultad para distinguir un pulso de otro. El efecto de esta dispersión es limitar la frecuencia efectiva del cable. Se mide en nanosegundos por kilómetro o em MHz/km. El producto de la más alta frecuencia (en MHz) y la distancia del cable (en Km) da por resultado el modelo de dispersión (o ancho de banda).

El núcleo del cable es el cilindro que proporciona un conducto para la luz, miesntras que el recubrimiento proporciona una superficie que causa reflexión de la luz. El diámetro del cable, medido en micrometros está dado por dos números separados. Por ejemplo, un 62.5/125 micron tiene un diámetro de núcleo de 62.5 microns, y un diámetro externo de 125 microns.

La atenuación de la fuente de poder óptica se mide en decibeles por kilómetro, en forma similar a los cables de cobre

dB = 10 log Potencia Salida/ P entrada

La potencia de entrada típica se encuentra en el rango de los miliwatts y la potencia de pérdida estaría a 30 dB arriba del rango del enlace de transmisión.

Los causantes de pérdidas al usar fibra óptica son el cable en sí mismo, más los conectores y empalmes los cuales tienen una pérdida de aproximadamente 0.15-0.5 dB. El cable de fibra óptica tiene una pérdida de alrededor de 5 dB/km a una onda de 85 nm. La atenuación es una constante proporcionada por el fabricante dependiendo del tipo de cable.

Existen dos estándares principalmente para el uso de fibra óptica en las redes locales. Uno es de AT&T y el otro de IBM. AT&T especifica un cable 62.5/125 micron, mientras que IBM utiliza un cable 100/140 micron.

Como vimos en los equipos para red, existe un reflectómetro (OTDR) para hacer pruebas al cable de fibra óptica pero debido a su alto costo se utiliza otra alternativa para hacer pruebas. Esta otra alternativa consiste en una fuente de poder óptica y un medidor de potencia óptica.

Hacer estas mediciones es un proceso muy directo. La fuente de poder óptico se verifica primero usando un pequeño trozo de fibra óptica proporcionado con la unidad.

El segundo paso es medir la atenuación (pérdida) de la fibra. Como se ve en la figura 9.28, la fuente se conecta en un extremo del cable y el medidor en el otro extremo. Para una red IBM Token Ring, una pérdida óptica que exceda los 13.0 dB indica una falla

en el cable. Un cable roto o conectores sucios son otros posibles problemas. Una vez más es importante tener alguien con quien recurrir en caso de problemas, ya sea el vendedor o alguna otra compañía de apoyo técnico.

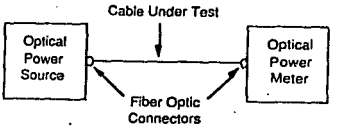


Fig. 9.28 medidas opticas

9.3 COMO MANTENER LA RED TRABAJANDO

En este punto final haré algunas consideraciones generales para evitar lo más posible "caidas de sistema" y otras fallas que impidan que nuestra red continue funcionando.

Si se ha decidido hacer una inversión en red, es porque ésta representa una utilidad y un beneficio a la empresa, cualquier caida o pérdida de tiempo va en contra de los interes de la misma y por lo tanto no se deben pasar por alto algunos detalles, que aunque parecen triviales son muy importantes.

No exceda los limites de diseño

Cada arquitectura de red tiene una variedad de parámetros asociados a su diseño. Por ejemplo, las redes IEEE 802.3 O 10BASE5 tiene una longitud máxima por segmento de 500 metros; ARCNET tiene un máximo de 255 nodos. El tratar de exceder esos limites por lo regular significa problemas. Con las redes Ethernet, un cable muy largo provoca colisiones excesivas.

Si por alguna razón su red llega al limite de diseño, puede que sea la arquitectura equivocada para sus necesidades o quizá sea necesario hacer crecer su red con elementos adicionales como repetidores, puentes y/o ruteadores.

Instale con cuidado.

Una instalación cuidadosa evita muchos problemas a futuro. Es mejor tardarse un poco más al momento de la instalación que tardar varias horas o días tratando de corregir una falla. Hay cuatro factores que debe de considerar en su plan de instalación:

1.- Verifique la continuidad eléctrica de todo el cableado y sus conectores y que todos los contactos esten colocados

adecuadamente.

2.- Identifique los requisitos de funcionamiento de su red desde el punto de vista del usuario. En otras palabras, póngase en el lugar del usuario y cheque toda la operación de la máquina y demás periféricos para la red.

3.- Verifique la operación de los periféricos, incluyendo impresoras de red y servidores de comunicación.

4.- Cheque todos sus dispositivos de energía como son los No breaks y UPS. No espere a que ocurre una falla para averiguiar si su aparato realmente funciona.

Sea paciente y tendrá mayores beneficios.

Documente su red.

Una documentación adecuada debe de cubrir las siguientes áreas:

1.- Detalles de la estación de trabajo- indicando la configuración de cada PC, incluyendo:

* El nombre del nodo y su dirección, ya sea ésta configurada con interruptores DIP o en ROM.
* Tipo de CPU, cantidad de memoria, etc.
* Otros dispositivos (tarjetas gráficas, tarjetas de emulasión, etc) también instaladas en la estación.
* Detalles específicos de cada tarjeta adicional en la PC, tales como el canal DMA y la línea IRQ, memoria compartida, etc.

Un modo conveniente de documentar estos parámetros es con una etiqueta adhesiva en la parte posterior de cada PC.

B. Detalles del cableado - Debo saber que estación, servidor, impresora, o periférico está al final de cada cable. En el momento de una crisis imagínese buscando a donde va cada cable.

C. Detalles del servidor - Incluyendo cuales usuarios y periféricos estan conectados a cada servidor. Si un usuario en su red se queja de no poder accesar el servidor, debe saber cual servidor verificar. Esto es especialmente útil entre más grande sea su red. Inclusive debe tener un mapa que le muestre la distribución total.

D. Dispositivos de conectividad - Tales como repetidores, puentes y gateways. Muchas fallas pueden ser aisladas en una sección particular de la red muchas veces separada por uno de estos dispositivos.

Anticipe las fallas

Existen tres mediciones de fallas que pueden ser aplicadas a la red y sus componentes y que proporcionan una advertencia en cuanto a un posible desastre.

A. Media del tiempo entre fallas (MTBF). Es una medida usualmente en miles de horas, del promedio (o media) del tiempo que un dispositivo debe operar adecuadamente antes de una falla. Los factores que influyen en la MTBF son la topología de red y el tiempo de conección de sus elementos, sea en serie o en paralelo, además de la confiabilidad de cada componente. Por ejemplo, la tarjeta madre de una PC puede tener una MTBF de 45,000 horas, lo cual quiere decir que puede existir alguna falla cada 5 años aproximadamente.

B. Media del tiempo de repación. (MTTR) Esta es una medida usualmente menor de 10 horas, del promedio de tiempo requerido para identificar y reparar o reemplacer el componente dañado. Dos

factores que afectan la MTTR incluyen la complejidad de la red y la disponibilidad de partes. Si la empresa cuenta con su propio servicio de mantenimiento de redes, se puede mejorar significativamente la MTTR teniendo manuales de servicio y partes listas para reemplazo. Por ejemplo, un sistema con una MTTR de ocho horas quiere decir que un dia laboral es suficiente para diagnosticar la falla, repararla y reinstalar la red.

C. Disponibilidad de la red. La disponibilidad es un porcentaje de la relación entre MTBF y el tiempo total (MTBF + MTTR):

$$\text{Disponibilidad} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})}$$

Obviamente una MTBF alta y una MTTR baja es lo óptimo, para obtener una disponibilidad mayor del 99%.

CONCLUSION

Como últimos comentarios quisiera mencionar el hecho de que vivimos en un proceso de constante evolución en todos las áreas. Si nos enfocamos concretamente a la computación, nos encotramos que el avance tecnológico revaza la capacidad de asimilación del hombre. Cada día surgen nuevas ideas y conceptos, algunos muy buenos y otros no tanto, pero que hacen de la computación un campo muy amplio de estudio y desarrollo.

Dentro de esta tecnologia en desarrollo, el concepto de Red Local o "LAN" ha tenido una extraordinaria aceptación y una comprobada utilidad en diversos campos como la industria, el comercio, la educación, etc.

De relativamente reciente incorpación en nuestro país, las redes locales cada día suman más usuarios y ya existen diversas compañías que cuentan no sólo con varias PC's aisladas, sino con una red local o inclusive una red internacional indispensable para el buen funcionamiento de sus operaciones.

En esta tesis he pretendido ilustrar de una manera sencilla y a la vez profunda los conceptos relacionados con las LAN's y su incorporación a un sistema más amplio de comunicación a nivel metropolitano e inclusive mundial.

Otro de los aspectos de gran importancia dentro de la computación es la plataforma o sistema operativo sobre el cual trabajan los equipos y la compatibilidad de unos con otros. Una vez más, debido al crecimiento acelarado, nos encontramos cada día con nuevas propuestas y cientos de asesores o vendedores de equipo de computo en especial de redes locales. Esto lejos de ser un inconveniente,

es una ventaja para el usuario final gracias a la creación de estándares y políticas de sistemas abiertos que permiten a todos los fabricantes seguir inovando y creando nuevos productos sin alejarse del concepto de compatbilidad. Es decir, el usuario final no sólo tiene una opción de compra sino varias.

En cuanto al problema que nos interesa, podemos concluir que la mejor opción para AFS México es la instalación de una red con topología de bus, usando cable coaxial y tarjetas Ethernet. Esta red tendrá en un principio un servidor 386 dedicado con al menos 100 Mb de disco duro y 4 Mb de memoria RAM, un mínimo de 4 estaciones de trabajo, 2 de las cuales pueden ser las XT's ya existentes y es conveniente que las otras dos sean AT's 286. El sistema debe ser diseñado de tal manera que se prevea un crecimiento de la red a mediano plazo. Se usará el sistema operativo Netware con capacidad de correo electrónico interno y el software necesario para la comunicación remota no sólo con los demás países como está planeado, sino también con el creciente número de voluntarios que ya cuentan con su propia P.C.

Finalmente, quiero mencionar que la persona interesada en el área de sistemas de computación debe estar en actualización constante para conocer los más recientes avances y así poder aplicarlos a su área de trabajo según las necesidades. Recuerden que no siempre lo más nuevo es lo mejor. Hay que hacer un análisis, como los mencionados en la tesis, de nuestras necesidades y en base a eso ser capaces de tomar una decisión.

APENDICE A

INSTALACION FISISCA

Por instalción física entendemos todo el hardware que compone nuestra red, esto es: computadoras, tarjetas de interfase, cables, impresoras, modem, etc.

Antes de hacer la instalación propiamente dicha, debemos hacer un bosquejo de esta, escoger la topología, el tipo de cable, las tarjetas de interfase, numero de estaciones y dispositivos periféricos. Dependiendo de la versión de Netware, podemos usar diferentes tarjetas (si soporta puentes internos), conectar varias redes (con puentes externos), tener una red de servidores dando servicio a un mayor numero de computadoras, o tener redes heterogenas con máquinas PC's, Macintosh, UNIX, minis o mainframes.

Cuando se compre el sistema operativo, el distribuidor o fabricante también proporciona la asesoria necesaria para la instalación de la red. Si se trata de una instalación mayor, la compañía debe contar con personal capacitado y un departamento de sistemas. Hay en la actualidad una variedad enorme de empresas que ofrecen sus servcios para la intalación de una red, desde el software y hardware necesario hasta el cableado completo de un edifico, sistemas de correo electrónico,etc.

Los capitulos anteriores nos dan la información referente a cada elemento de la red. Dependiendo de las necesidades y recursos de la empresa se debe diseñar esta. Hay dos factores de particular importancia que determinan el tipo de red a instalar:

* Aplicaciones

* Velocidad

Estos dos factores no son independientes, muy al contrario la velocidad de respuesta dependerá de la o las aplicaciones de la red. En base a estos factores debemos determinar si es necesario adquirir poderosas máquinas con procesador 486, utilizar cable coaxial o la más costosa fibra óptica. Determinar cuantas computadoras formarán parte de la red, cuantos servidores se requieren, posibilidades de crecimiento, etc.

Por lo general, al instalar una red ya se cuenta con computadoras que se han usado independientemente y lo unico que hace falta es conectarlas entre si. Un buen estudio de nuestras necesidades nos evitará comprar un Ferrari para recorrer 100 mts.

Cualquier combinación de Server-red tiene un máximo ancho de banda. Esto es, existe un limite máximo de cuantos datos pueden moverse a través de la red. Una vez que ese limite se ha alcanzado, la red ha llegado a su máximo de eficiencia.

Por lo tanto, el secreto para comprar una red es determinar cuanto ancho de banda necesito y combinarla con la opción de Server-red que me soporte esa necesidad.

Novell ha desarrollado un sistema que permite la evaluación de una red de una forma muy sencilla.

- Primero se estima el factor de carga de la red.
- Segundo, se busca en las gráficas de evaluación la combinación que cumpla con mi factor de carga.

Evaluación del factor de carga:

Para evaluar el factor de carga, hay que determinar los tipos de usuarios que van a utilizar la red. Estos usuarios se pueden clasificar en cinco tipos diferentes:

TIPO 1: Este tipo de usuario es el que el 100 % del tiempo usa un tipo de aplicación como procesamiento de palabra u hoja electrónica y no "carga" mucho a la red. A este tipo de usuario se le da un peso = 1.

TIPO 2: Este tipo de usuario es el que el 70 % del tiempo usa un tipo de aplicación como procesamiento de palabra u hoja electrónica y 30 % del tiempo usa aplicaciones del tipo base de datos. A este usuario se le da un peso = 5.

TIPO 3: Este tipo de usuario utiliza un 70 % del tiempo aplicaciones del tipo base de datos y un 30 % aplicaciones del tipo procesamiento de palabra. A este usuario se le da un peso = 15.

TIPO 4: El ususario que utiliza el 100 % del tiempo en una aplicación del tipo base de datos, que continuamente esta accesando al File Server. A este usuario se le da un peso = 30

TIPO 5: El usuario del tipo 5, es el que necesita el máximo ancho de banda de la red. Un programador que realiza compilaciones el 100 % del tiempo constituye este tipo de usuario al cual se le da un peso = 70.

Para determinar el factor de carga de la red, a cada usuario se le asigna un peso y al final se suman todos los pesos.

Para determinar como se aplica vamos a crear una situación y a encontrar el factor de carga.

Imaginemos una red con 15 usuarios:

	Número de usuarios	Tipo de usuario	Peso	Factor de carga
	7	1	1	7
	6	3	15	90
	2	5	70	140
TOTAL	15			237

Siete usuarios se clasifican como del tipo 1 ya que estos usuarios sólo utilizarán aplicaciones como procesamiento de palabras u hoja electrónica. Multiplicando el número de usuarios por el peso obtenemos el factor de carga de estos usuarios.

Supongamos que hay 6 usuarios del tipo 3 y dos usuarios del tipo 5, al sumar tendremos un factor de carga total de 237.

El segundo paso en la evaluación del sistema es encontrar la combinación server-red que cumpla con el factor de carga determinado anteriormente.

Para simplificar la evaluación Novell ha evaluado más de 40 combinaciones de Server-red, y las mejores las ha expresado en unas gráficas.

Como se puede observar en las gráficas en el eje X se refiere al factor de carga y el eje Y se grafica en Kilobytes por segundo. Para determinar la eficiencia de una red, se escoge una de las líneas rectas que representan el funcionamiento de una AT con disco duro y una PC con floppy's. Si el punto localizado está abajo de la línea de la AT, la estación de trabajo será más lenta que una AT. Si por el contrario, el punto de intersección se

encuentra por arriba la estacion de trabajo será mas rapida que una AT.

Cabe observar con detenimiento, la importancia que tiene el tipo de File Server que tengamos conectado en nuestra red. Un servidor mas rapido file server, se traduce en una mas eficiente red.

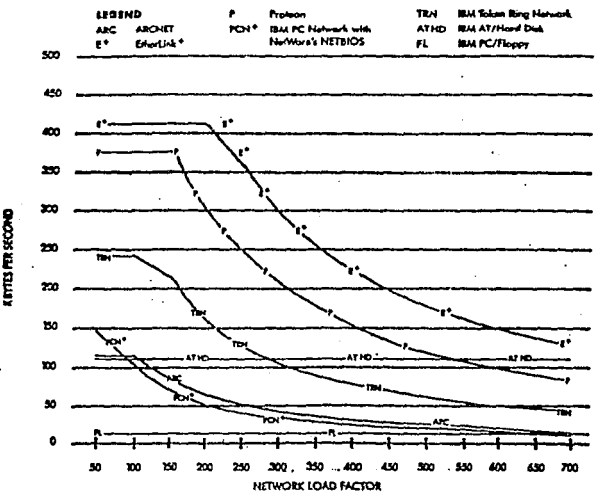


Figura A.1

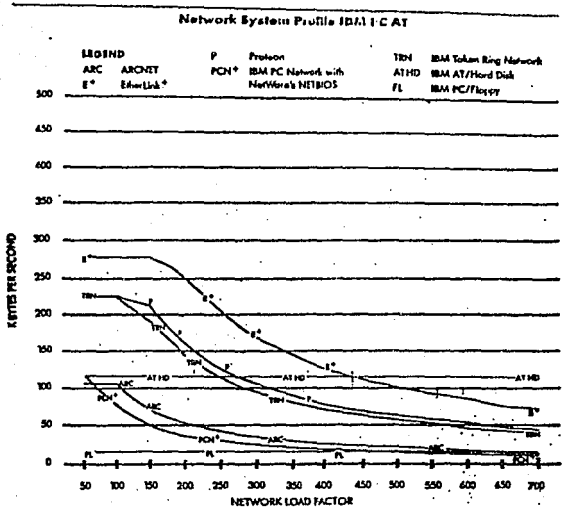

Network System Profile IBM PC AT
LEGEND
ARC ARCNET
E* EtherLink*
P Proteon
PCN* IBM PC Network with NetWare's NETBIOS
TRN IBM Token Ring Network
ATHD IBM AT/Hard Disk
FL IBM PC/Floppy
K BYTES PER SECOND
NETWORK LOAD FACTOR

Figure A.2

Network System Profile IBM PC XT

LEGEND					
ARC	ARCNET	P	Proteon	TRN	IBM Token Ring Network
E+	EtherLink+	PCN+	IBM PC Network with NetWare's NETBIOS	AT HD	IBM AT/Hard Disk
				FL	IBM PC/Floppy

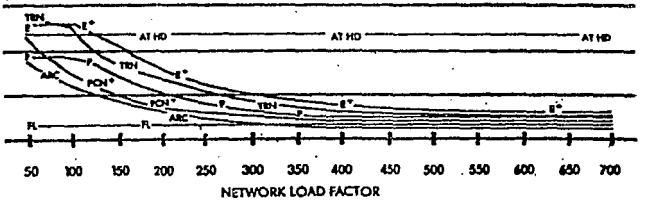


Figure A.3

Conexion de una estacion a la red

Para hacer este primer paso es necesario lo siguiente:

* Configurar adecuadamente la dirección y línea de interrupción de la tarjeta de interfase con la red (NIC) (Network Interface card).

* Connectar apropiadamente el cable a la NIC.

* Arrancar la estación de trabajo y cargar un shell configurado adecuadamente.

Redirecciones de las NIC (Network Interface card)

La NIC es la interfase primaria entre un nodo de red (una estación de trabajo o el servidor) y el cable de la LAN o cualquier otro medio de comunicación. Las NIC tienen topologías diferentes, pero en cualquier topología hay varios modelos y fabricantes de NIC. Se pueden tener instaladas NIC de diferentes fabricantes y modelos en diferentes estaciones de trabajo, siempre que la misma NIC este diseñada para la misma topología.

Sin embargo, cada NIC instalada debe tener una única dirección en la red. En una LAN pequeña con un servidor y una topología, la estación de trabajo es identificada inequivocamente por medio de las *direcciones de nodo* NIC. La figura A.4 muuestra donde están colocados los interruptores para definir una dirección de nodo NIC. Deberá consultar la documentación de la NIC como guía para colocar los interruptores y seleccionar una dirección en particular.

Si dos estaciones de trabajo NIC en el mismo sistema de cableado tienen la misma dirección de nodo, la información no puede ser distribuida con fiabilidad, ya que no pueden distinguirse una de

otra. Debido a esto debe mantenerse una lista con las direcciones de las NIC utilizadas en la red. Cuando se instala una nueva estación deberá consultarse esta lista y seleccionar una dirección NIC libre.

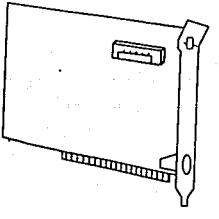


Fig. A.4 Especificacion de la direccion hardware de la red.

Algunas tarjetas vienen preconfiguradas de fábrica. A menos que sea un caso poco común, esta configuración trabajará sin ningún problema. Por otro lado, existen tarjetas cuya dirección puede ser cambiada a nivel software, evitando así el abrir la computadora.

Las NIC instaladas en el servidor deben tener también una dirección diferente en relación a las estaciones de trabajo. Si se hace un puente interno a través del servidor cada NIC debe tener una dirección diferente de nodo.

Las NIC instaladas en el servidor también tienen asociadas a ellas una *direccion de red*. A diferencia de las direcciones de nodo, que residen fisicamente en la NIC, las direcciones de red se definen en los procedimientos de generación del sistema de Netware que veremos más adelante. Un servidor puede tener hasta 4 NIC y cada

una de ellas está identificada individualmente por Netware. La figura A.5 ilustra como las direcciones de red y de nodo pueden usarse en una LAN que incluya dos servidores y tres topologías diferentes.

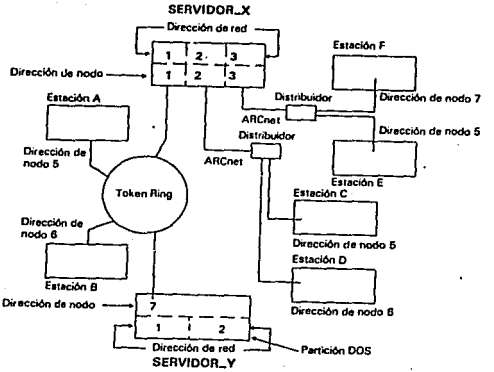


Fig. A.5 Direcciones de nodo y de red en servidores con puente interno.

En la figura A.5 el SERVIDOR_X está conectado a una red Token Ring y a dos redes ARCnet. Cada topología tiene asignada su propia dirección de red: 1, 2 ó 3 en este ejemplo. Debido a que el SERVIDOR_X y el SERVIDOR_Y participan en la misma topología Token Ring, la dirección de red para el SERVIDOR_Y es también fijada a 1 a través del proceso de generación del sistema Netware. Mientras comparten la misma dirección de red, el SERVIDOR_X y el SERVIDOR_Y están identificados individualmente en la red Token Ring mediante una dirección de nodo distinta en la NIC instalada en cada servidor así como mediante un nombre de servidor diferente.

Debido a que Netware usa una combinación de direcciones de red y de nodo para identificar las estaciones de trabajo, en la red multitopología dibujada en la figura A.5, la NIC en la estación A puede usarse con la misma dirección de nodo que la usada en la estación C. Estas dos estaciones están conectadas al SERVIDOR_X a través de NIC de servidor separadas, cada una con su dirección de red asociada; por tanto, están identificadas individualmente. Y debido a que las NIC Token Ring no funcionan en la topología ARCnet, y viceversa, no hay riesgo de que la estación A pueda ser trasladada a la topología ARCnet, ni que la estación C pueda serlo a la topología Token Ring.

Técnicamente, las estaciones C y F podrían compartir la misma especificación de nodo NIC, ya que cada estación está unidad al servidor a través de NIC de servidor distintas, y cada servidor tiene su propia y única dirección de red asignada. Sin embargo, las estaciones C y F comparten la misma topología, no el mismo

sistema de cableado físico en la red. Si se cambiara la estación C al mismo sistema de cableado de la estación F, que es tan sencillo como desconectar un cable y conectar otro en la estación C, estas dos estaciones podrían estar compartiendo el mismo nodo NIC y la misma dirección de red, y no estarían identificadas individualmente.

Como regla, se debe establecer una dirección diferente para cada NIC de la red, aunque en caso de estar en sistemas de cableado distintos no sea estrictamente necesario.

Elección de la IRQ en una NIC

Los dispositivos físicos de una máquina basada en el DOS, tales como los puertos serie, puertos paralelo, controladores de disco, etc. son accesibles mediante peticiones de interrupción o IRQ (Interrupt ReQuest). Las IRQ son canales, o líneas, usadas entre la unidad central de proceso (CPU) y otros componentes del hardware para transmitir peticiones de comienzo y finalización de tareas. Hay que tener cuidado con la selección de las IRQ usados por los dispositivos hardware, como las tarjetas NIC, para que no se produzcan colisiones cuando se acepten estas peticiones de interrupción del CPU.

Las tarjetas NIC vienen de fábrica generalmente con una especificación IRQ. No es recomendable cambiar esta especificación a menos que sea absolutamente necesario.

INSTALACION DEL SISTEMA OPERATIVO

La instalación de Netware implica generar y cargar el software del sistema operativo en el servidor y generar los diskettes de arranque de las estaciones.La primera tarea se lleva a cabo mediante la utilidad NETGEN de Netware; la otra, a través de la utilidad SHGEN.

Una vez instalado y configurado el hardware de las máquinas y demás dispositivos periféricos, el siguiente paso es instalar el sistema operativo. Netware viene acompañado de varios manuales que se deben de leer para obtener una información más detallada del proceso de instalación. En este punto sólo tratare los puntos más importantes y diferentes opciones de instalación.

Anteriormente, Netware estaba protegido contra copia mediante un número de serie instalado en el software del sistema operativo Netware y en un dispositivo hardware instalado en el servidor llamado *tarjeta llave (keycard)*. Ni siquiera se podía hacer una copia de seguridad del diskette GENDATA de Netware que contenía el número de serie.

Las tarjetas de llave ya no son necesarias aunque algunas equipos ya la tienen instalada y pueden ser usadas para otros propósitos. Todavía se incluye un número de serie que identifica cada copia de Netware en el diskette GENDATA. Ahora sí puede hacerse una copia de seguridad del diskette GENDATA, y el proceso de instalción del número de serie se realizará automaticamente mediante una rutina de NETGEN.

Normalmente, el numero de serie está impreso tambien en la cubierta del diskette. Durante el proceso de instalacion o al consultar a Novell es muy importante tener a la mano este número. Se puede generar más de un sistema operativo y si su maquina no tiene tarjeta llave puede correr en diferentes servidores pero esto es una acción ilegal y viola la licencia de software de Novell. Por otro lado, si trata de instalar el sistema operativo con el mismo numero de serie en dos servidores conectados en la misma red provocan conflictos y mensajes de error que hacen inutilizable la red. Por lo tanto si desea instalar una red de servidores o cumicación entre ellos es necesario un paquete de Netware para cada servidor.

Para asegurarse de no borrar accidentalmente los diskettes, debe protegerlos contra escritura antes de copiarlos. A continuación debe hacerse una copia de seguridad del software, con la que se realizará la configuracion e instalación del paquete. Hay que disponer de un buen número de diskettes. Son muchos los programas que componen Netware, aún sin configurar, pero no es necesario formatear los diskettes antes de hacer las copias de seguridad. Novell recomienda para esta tarea el uso de la orden DISKCOPY del DOS.

Con la computadora funcionando bajo DOS, escriba en el indicador

```
DISKCOPY A: A:
```

al presionar [Enter], se pedirá la colocación del diskette Origen en la unidad A: y que se pulse cualquier tecla. El diskette origen

es cualquiera de los diskettes originales de Netware, que han sido previamente protegidos contra escritura. Posteriormente se pide que introdusca el diskette destino donde se copiará el contenido del diskette origen.

Hay varios modos de generar el sistema operativo Netware. Para comprender bien las distintas opciones, es bueno saber que algunas partes del proceso de instalación y generación del sistema operativo pueden realizarse sobre cualquier computadora personal que funcione bajo DOS, mientras que otras partes deben realizarse en el servidor en el que el sistema operativo Netware se va a instalar.

Metodos de NETGEN

Las posibilidades para ejecutar NETGEN son:

* El método estándar de discos flexibles
* el método del disco RAM
* el método del disco fijo
* el método de la unidad de red

EL METODO ESTANDAR DE DISCOS FLEXIBLES. Con este método es fácil la instalación y generación de Netware. Si se dispone de al menos dos unidades de disco flexible, esto reduce el número de veces que hay que intercambiar los diskettes. De este modo, las rutinas de NETGEN escribiran la configuración del sistema directamente en las copias de seguridad de los diskettes Netware.

EL METODO DEL DISCO RAM. Para evitar el intercambio de discos y conseguir mayor velocidad en el proceso de acceso a los archivos

de configuración de Netware, se puede crear en la computadora un disco RAM del DOS, copiar los archivos Netware de diskettes de seguridad en el disco RAM, y ejecutar NETGEN desde ese disco. El inconveniente es que el disco RAM desaparece si apaga la computadora.

Si antes de apagar no se terminan completamente todas las fases del proceso generacion, copiar de nuevo los archivos en la RAM supondrá haber empleado tanto tiempo como si inicialmente se hubiera utilizado el método anterior.

EL METODO DEL DISCO FIJO. Si se dispone de un disco fijo en una computadora que no sea el servidor, es posible crear en el un directorio de trabajo Netware. NETGEN carga los archivos que necesita desde las copias de seguridad de los diskettes de instalación al disco fijo local.

Este método requiere una cantidad de espacio libre considerable (8 Megabytes); debe arrancar con DOS 3.0 o mayor, y el archivo CONFIG.SYS del DOS debe tener FILES = 20 y BUFFERS = 15.

EL METODO DE LA UNIDAD DE RED. Este método es una variación del anterior. Se utiliza el disco rigido del servidor de una red ya existente. Como antes de crearse un directorio de trabajo en el disco fijo del servidor (el disco debe de tener al menos 10 megabytes de espacio disponible). También se debe entrar en el servidor, desde la máquina en la que se va a instalar, y que se utiliza por el momento como una estación más de la red. Con este método, puede completarse totalmente el proceso de instalación y generación desde la estación, sin tener que copiar los archivos

temporalmente en sus diskettes de copia de seguridad.

Si se usa uno de estos dos ultimos métodos, pueden generarse sistemas Netware una y otra vez. Sin embargo, se debe tener cuidado al insertar el diskette GENDATA, con el número de serie correcto, cuando se indique. De otro modo, se duplicarian los número de serie.

Niveles de NETGEN

NETGEN puede ejecutarse para crear una configuración del sistema por omisión, o para crear una configuración del sistema especifica. Si no se tiene conocimientos profundos de software y hardware es preferible realizar la configuración por omisión. Si no se cambiaron los IRQ's por omisión al instalar las tarjetas no hay ningún motivo de incompatibilidad.

Se debe evitar no ejecutar NETGEN como nueva configuración. Si selecciona new NETGEN ingnorará cualquier configuración previa y se deberá comenzar de nuevo la configuración. Normalmente, ejecutará NETGEN para una nueva configuración una sola vez.

Una peculiaridad de NETGEN consiste en que para aceptar o validar una configuración particular del sistema operativo, a veces se debe pulsar la tecla [Esc]. En cambio, para abandonar la configuración y volver al menu del nivel anterior se debe seleccionar en el menú la opción "leave" o "abandon" o intentar completar la configuración y entonces decirle a NETGEN que la configuración no es correcta.

Es posible que no se pueda presionar [Esc] para volver a un menú anterior.

A medida que se van completando las distintas fases de la instalación, aparecen nuevas opciones en los menús. Por este motivo, cada vez que se entra en los menús de NETGEN, pueden parecer distintos.

A veces, es difícil seguir los menús. Sin embargo, NETGEN le permite hacer las selecciones con cierta seguridad. Si lee atentamente las pantallas, y sigue adelante seleccionando opciones, lo peor que le puede ocurrir es que necesite comenzar de nuevo.

Ejecucion de NETGEN

El método de NETGEN explicado aquí es el estándar de disco flexible. Se desarrollará una nueva configuración del sistema por omisión. Debe comenzarse por arrancar su computadora personal con el sistema operativo DOS.

Para entrar en NETGEN se debe colocar el diskette de copia de seguridad NETGEN en la unidad A:, escribir NETGEN y pulsar [Enter]. Aparecerá lo siguiente:

```
Insert disk SUPPORT in any drive.
Strike any key when ready....

(Inserte el disco SUPPORT en cualquier unidad.
Pulse una tecla para continuar...)
```

Si es posible, debe colocarse el disco de copia de seguridad SUPPORT, sin protector de escritura, en la unidad B:, mientras se mantiene el disco NETGEN (También sin proteger contra escritura)

en la unidad A:.(Se puede utilizar una sola unidad, pero los cambios de disco serán en este caso muy frecuentes.) Despues de que NETGEN cargue la información que necesita del disco SYSTEM, se visualizará en la pantalla el menú "System Configuration Level" (Niveles de configuración del sistema), ilustrado en la figura A.6. Ahora podria terminarse fácilmente la sesión de NETGEN presionando la tecla [Esc] una vez, y confirmando con "Yes" el deseo de salir.

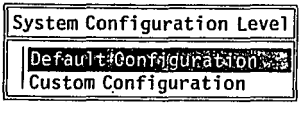


Fig. A.6 NETGEN Menu de niveles de configuracion del sistema

Debe mantenerse la barra de selección en "Default Configuration" y presionar [Enter]. Si se ha iniciado NETGEN, sin ningún parámetro aparecerá en pantalla el menu de opciones de ejecución de NETGEN, como se muestra en la figura A.7. Seleccione "Standard (floppy disks)", pulse [Enter] y se visualizará un menú de opciones de generación (figura A.8)

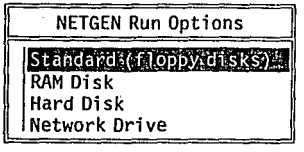


Fig. A.7 NETGEN Menu de opciones de ejecucion

A través del submenú "Network Generation Options" (Opciones de generación de la red) se puede hacer lo siguiente:

* Iniciar la primera fase mediante la opción "Select Network Configuration" (Selección de la Configuración de la Red), para entrar en el submenú "Topics Available", donde se selecciona o introduce la información que NETGEN necesita para adaptar Netware a nuestra red.

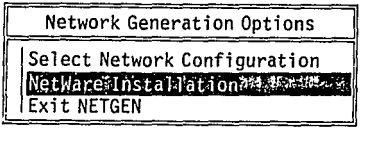


Fig. A.8 NETGEN Menu de opciones de generación de la red.

* Iniciar la segunda fase, dedicada a la instalación de Netware, que debe realizarse en la máquina que actuará como servidor.

Seleccion de la configuracion de la red

El siguiente paso es seleccionar la opción "Select Network configuration" dentro del submenú "Network Generation Options".

Se verá el siguiente mensaje:

```
Loading Program Files. Please Wait
(Cargando los archivos del programa. Espere, por favor)
```

A continuación aparecerá:

```
Insert disk AUXGEN in any drive
Strike any key when ready...
(Inserte el disco AUXGEN en cualquier unidad.
Pulse una tecla para continuar...)
```

Simplemente deben seguirse las instrucciones que aparezcan en la pantalla. Si se realiza una nueva instalación por omisión, aparecerá el menú "Available Options" (Opciones disponibles), que se ilustra en la figura A.9.

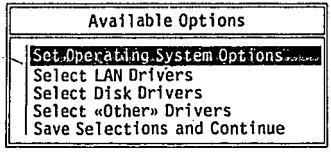


Fig. A.9 NETGEN submenu de opciones disponibles para configurar la red.

El menú "Available Options" irá conduciendo al usuario en el proceso de selección de numerosas opciones necesarias para describir a NETGEN las características del hardware de nuestro

servidor y nuestra red. Novell llama a este proceso "selección de los recursos del servidor". Mencionare algunas decisiones importantes en este proceso.

Manteniendo la barra de selección en "Set Operating System Options" y pulsando [Enter], se verá uno o dos submenús de opciones del sistema operativo.

Si se está instalando Advanced Netware 286, versión 2.15, aparecerá la pantalla ilustrada en la figura A.10.Está versión no incluye las caracteristicas de tolerancia a fallos del SFT Netware

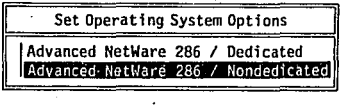


Fig. A.10 NETGEN: opciones del sistema operativo para Advanced Netware 286.

Con estas opciones únicamente podrá decidir la instalación de Netware en modo dedicado o no dedicado. Si se está instalando SFT Advanced Netware 286, las opciones disponibles serán:

SFT Netware Level II+TTS

SFT Netware Level II

Si se va a ejecutar cualquier aplicación de base de datos en el servidor, está recomendado seleccionar la opción +TTS, qunque esto obligará a adoptar algunas decisiones extra posteriormente. La opción TTS (Servicios de seguimiento de transacciones) permitirá

marcar los archivos de datos con el atributo TTS. En caso de fallo podrán realizarse recuperaciones automáticas y otros servicios en los archivos marcados de esta manera. Novell señala en su manual "SFT/Advanced Netware 286 Installation", que esta opción no afecta a la ejecución de las operaciones no transaccionales. Además, si se instala está disponible siempre que sea necesario. Lo normal, por tanto, será activar TTS.

Selección de los controladores de red, de disco y de otros componentes hardware. La próxima tarea consiste en definir los controladores que Netware necesitará para comunicarse con las NIC instaladas en el servidor, y con cualquier otro hardware instalado o conectado al mismo.

Si se selecciona "Select LAN Drivers", aparecerán dos menús y un recuadro de mensajes con instrucciones, como se muestra en la figura A.11. Es necesario insertar varios diskettes de los copiados al principio para llegar a este menú. NETGEN los irá pidiendo para cargar en la RAM los archivos de los controladores más comunes.

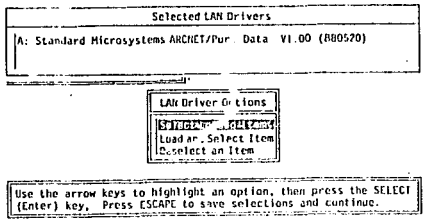


Fig. A.11 Submenús de selección de controladores de LAN

En la parte superior de la pantalla está el submenu "Select LAN Drivers" (Selección de controladores de LAN), inicialmente en blanco. En la parte central de la pantalla está el submenu "LAN Driver Options". Y en la parte inferior de la pantalla están las instrucciones para el uso del menú de las opciones de controladores de LAN. Deben leerse cuidadosamente estas instrucciones. Si se pulsa la tecla [Esc] no se volverá al menú de opciones disponibles. Este es uno de los momentos en que [Esc] sirve para grabar una selección en los diskettes y hacer que se continúe el proceso de selección de recursos.

Al seleccionar "Select Loaded Item" aparecerá una lista de NIC de los controladores que están ya cargados en la RAM (quizá sea necesario insertar el disco SUPPORT para que aparesca esta lista). Simplemente hay que desplazar el cursor a través de la lista, hasta que se vea el nombre de la NIC instalada en el servidor. Con este campo resaltado pulse [Enter]. En la parte superior de la pantalla se añadira ese nombre en el menú "Selected LAN Drivers". En la figura A.9 se seleccionó el controlador ARCNET/Pure Data V1.00 (880520) de Standard Microsystems.

Si el servidor tiene más de una NIC, se debe seleccionar un controlador para cada una. Si hay dos del mismo tipo, hay que seleccionar el controlador correspondiente dos veces, puesto que cada selección está asociada con una NIC particular.

Si se selecciona un controlador incorrecto, debe seleccionarse en el recuadro de opciones de controladores de LAN la opción "Deselect an Item" (Esta opción sólo aparecerá después de haber

seleccionado algún controlador). El controlador incorrecto deberá anularse antes de pulsar [Esc].

Si no aparece en la lista el controlador deseado, puede que no este cargado en la RAM pero si en alguno de los diskettes. Para añadir ese controlador a la RAM, hay que seleccionar "Load and Select Item" y seguir las instrucciones sobre como añadir un conjunto de controladores alternativo. Las instrucciones son claras pero deben leerse con cuidado. Si se intenta seleccionar un controlador que es incompatible con otro ya seleccionado anteriormente, el último no se añadirá a la lista de controladores disponibles. Esto indicaría un conflicto de hardware, que tendrá que resolverse modificando la IRQ o dirección de la NIC, o utilizando otro diferente. Estos cambios deben indicarse a NETGEN mediante las rutinas de configuración detallada "Custom Configuration".

Cuando se haya completado la selección de los controladores de la LAN, debe presionarse [Esc] para grabar la configuración en los diskettes de NETGEN. Se volverá al menu de opciones disponibles.

La opción "Select Disk Drivers" sirve para seleccionar los controladores de discos fijos internos del servidor. El proceso es similar al de los controladores de LAN, excepto en que se debe definir un tipo de *canal de disco duro* apropiado. Los tipos de canal están numerados de 0 a 4. Para facilitar la identificación del número de canal que se corresponda con cada tipo de disco duro instalado interna o externamente en el servidor, Novell incluye un diagrama dentro de sus manuales. En la documentación que se

adjunta al servidor debe decirse que tipo de disco fijo está instalado. Si tiene instalada una tarjeta controladora y uno o más discos duros externos, habrá que consultar la documentación que viene con esos dispositivos.
Al seleccionar "Select Disk Drivers" deberá escribirse, cuando se solicite, el número de canal apropiado al disco duro y pulsar [Enter]. En una ventana aparecerá un listado de los tipos de discos fijos que pueden funcionar con cada canal y que sean compatibles con el resto del hardware.

Cuando se haya completado el proceso de selección del controlador de disco fijo, debe pulsarse [Esc] para grabar las selecciones realizadas.
La opción "Select Other Drivers" permite seleccionar los controladores de software o hardware que puedan haberse adquirido independientemente del servidor. Estos controladores deben imnstalarse antes de que ese hardware o software se comunique con su servidor. Si se han realizado los procesos de selección anteriores, se podrá utilizar esta opción sin grandes dificultades.
Seleccionar un controlador configurable significa que puede definirse la interrupción IRQ u otra parámetro del hardware o software manejado por el controlador; en este caso, aparecerá en el menú "Available Options" la opción "Configure Drivers/Resources" (Controladores/Recursos configurables). Esta opción no aparece en las instalaciones por omisión más sencillas.
Cuando se termine de seleccionar todos los controladores y el

resto de las opciones instaladas, debe seleccionarse la opción "Save Selecctions and Continue". Debe continuarse con el proceso de configuración, y ya no se podrá volver a la pantalla de opciones disponibles. Sin embargo, si más tarde se necesitara cambiar o añadir un controlador a los seleccionados, podría hacerse mediante las rutinas de mantenimiento de NETGEN o volver a arrancar la computadora y ejecutar NETGEN para una nueva configuración del sistema.

Los siguientes pasos para terminar de configurar son muy sencillos simplemente siguiendo las instrucciones y aceptando los valores que Novell tiene por omisión.

Revision, grabacion y aceptacion de la configuracion del servidor.

Al continuar con la siguiente fase de configuración por omisión se pedirá confirmación de las opciones ya instaladas. Esta información se visualiza en la pantalla "Selected Configurations" (Configuraciones Seleccionadas).

Esta pantalla proporciona la oportunidad de aceptar o rechazar la configuración seleccionada. La pantalla da también la oportunidad de anotar la información de configuración en los formularios que contienen los manuales de Netware. Esta información es muy valiosa y debe tenerse a la mano.

Como se ha dicho anteriormente para grabar la información se debe pulsar [Esc] y luego contestar "Yes" para aceptar y pulsar [Enter]

Enlace (linking) de NETGEN y generacion del Sistema Operativo.

NETGEN realiza ahora algunas tareas de generación y enlace. La figura A.12 ilustra lo que ocurre. Se crean dos archivos.

NET$OS.EX1 y NET$OS.EX2. Estas dos partes del sistema operativo se cambiarán durante la fase en la que NETGEN instala el sistema operativo en el servidor.

En este momento se personalizan varias utilidades especiales para la configuración del sistema operativo creado anteriormente. Estas utilidades son:

- COMPSURF
- DISKED
- INSTOVL
- VREPAIR

Se pedirá la inserción de varios diskettes de Netware en las unidades correspondientes para grabar los archivos enlazados y adaptados a nuestro servidor. Al terminar este proceso se vuelve a la pantalla de opciones de generación de Netware.

Los siguientes pasos deben relaizarse forzozamente en el servidor.

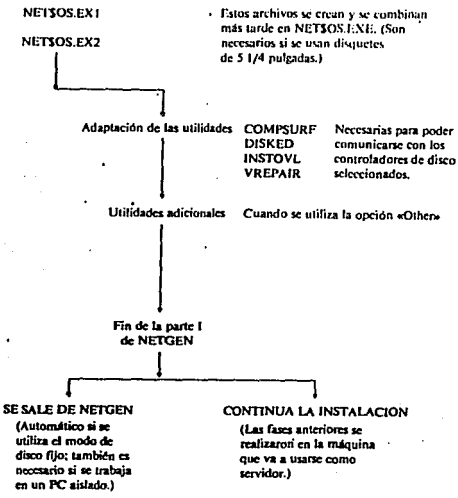


fig. A.12 Actividades de configuracion y enlace de la fase I

Instalacion de Netware mediante NETGEN

Para completar la fase de instalación de NETGEN debe trabajarse en el servidor. Hay que arrancar esta máquina bajo el DOS y después continuar la instalación por omisión iniciada originalmente en este mismo equipo. o bien entrar de nuevo en la pantalla de opciones de generación de red (fig. A.8) si la primera etapa se realizó en un equipo distinto.

En este paso se supone que ya se instaló y configuró todo el hardware. Ahora en el menú resalte la opción "Netware Instalation"

y presione [Enter].

Si se elige el nivel por omisión al instalar Netware, irán sucediéndose cíclicamente las distintas pantallas en las que habrá de introducir información o realizar alguna selección.

Al seleccionar el nivel de instalación por omisión, NETGEN creará una tabla de particiones por omisión en el disco fijo, esta tabla define la capacidad de almacenamieno total del disco como un volumen (SYS:). También se instala automáticamente el "Hot Fix" y otras utilerías de Novell.

Después de este paso, aparecerá una pantalla con los nombres de los volúmenes creados. Usted puede cambiar el nombre si así lo desea, pero recuerdo que el volumen SYS: debe existir puesto que ahí residirá el sistema operativo. NETGEN tarda un rato en realizar la tabla de particiones. Si se está instalando SFT Netware 286 con duplicación de disco, aparecerá un menú en el que se pide se creen unas tablas de duplicación ("Establish Mirror Pair") y tarda un poco más.

El siguiente paso es dar nombre al servidor. El nombre debe de ser único, fácil de recordar y no demasiado largo. Si hay más de un servidor los puntos anteriores son particularmente importantes. El nombre puede tener entre 2 y 45 caracteres, sólo es necesario escribir el nombre y presionar [Enter].

Definicion de las impresoras de red. El próximo paso es indicar a Netware la existencia de cualquier impresora de red que este conectada al servidor. Se debe especificar a que puerto del servidor está conectada. Si la impresora está conectada a un

puerto serie (COM) puede que necesite redefinir algún parámetro de las comunicaciones serie. También se puede instalar el sistema operativo sin incluir la impresora y añadirla más tarde mediante los procedimientos de mantenimiento del sistema.

Al terminar las tareas anteriores se vuelve al submenú "Installation Options", aquí debe seleccionarse la opción "Continue Installation". Se pregunta por pantalla si se desea instalar el software de la red en el servidor, respondiendo "Yes" se pasa a la fase final de la instalación.

NETGEN toma de nuevo el control y después de enviar a la pantalla un mensaje avisando que se tardará algún tiempo y no hay que impacientarse ("Please Be Patient"), comienza sus operaciones finales de instalación.

Si se está usando el método de instalación estándar en discos flexibles habrá que insertar numerosos diskettes de Netware en las unidades de disco. NETGEN avisará si se introduce un diskette erroneo y permite sustituirlo por el correcto.

Durante este tiempo NETGEN hace lo siguiente:

* Instala un programa cargador en la pista 0 del disco fijo sobre el que se define el volumen SYS:.
* Crea la estructura de directorios exigida por Netware (SYSTEM, PUBLIC, LOGIN, MAIL).
* Copia los archivos de programas Netware en la estructura de directorio (simultáneamente crea cualquier estructura de subdirectorios que se precise, el grupo EVERYONE y los usuarios SUPERVISOR y GUEST).

Con la instalación del servidor se ha recorrido la mitad del camino para utilizar Netware. Es importante también poder arrancar y conectar la estación al servidor para establecer una sesión con él. Para este propósito hay dos aspectos de interés:

* Cómo ejecutar la utilidad SHGEN en la creación de archivos shell necesarios para usar la LAN y comunicarse con Netware en el servidor.
* Cómo crear un archivo SHELL.CFG. Definir este archivo es importante si hay instaladas versiones distintas del DOS en las estaciones.

SHGEN

SHGEN es la abreviatura de SHell GENeration (generación del shell). Como NETGEN, SHGEN puede ejecutarse a diferentes niveles (por omisión, intermedio y detallado) y a través de diferentes métodos. Supondremos un nivel de configuración por omisión mediante el método de disco flexible en una PC aislada.

Se debe crear un diskette de arranque maestro para cada tipo de NIC y, posiblemenete para cada tipo de estación conectada a la red. Estos diskettes serán las copias de seguridad de los diskettes que se usen en las estaciones. Para crear un diskette de arranque maestro, primero debe formatearse bajo DOS e incluir los archivos del sistema. Esto es

FORMAT A:/S

Ya tenemos el diskette listo para su posterior utilización.

Para generar el shell necesitamos los siguientes diskettes:

* SHGEN_1
* SHGEN_2
* LAN_DRV_001
* LAN_DRV_002

Se inserta el diskette SHGEN_1 en la unidad A:, y si se dispone de unidad B:, se inserta en ella el diskette SHGEN_2. El sistema avisará en caso de no encontrar el disco que necesita.
Al escribir SHGEN y pulsar [Enter], aparecerá en pantalla un menú como el que se muestra en la figura A.13

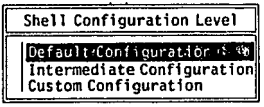


Fig. A.13 SHGEN: menu de niveles de congifiguracion de shell

Como dije anteriormente vamos a utilizar el nivel de configuración por omisión. si quisieramos cambiar la IRQ de alguna NIC tendríamos que usar el nivel intermedio. El nivel detallado se utiliza si una NIC no está contenida en los diskettes LAN_DRV_001 o LAN_DRV_002. Después de escoger el nivel aparece el menú "SHGEN Run Options" de la figura A.14. Aquí elegimos la opción "Floppy disks".

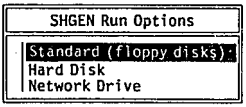


Fig. A.14 SHGEN: menu de opciones de ejecucion

Al seleccionar la configuración por omisión aparece en la pantalla una lista de controladores de LAN disponibles. La lista incluye todos aquellos controladores cargados en la RAM cuando se cargo SHGEN. Puede seleccionarse el controlador correspondiente a la NIC de red, desplazando la barra selectora a lo largo de la lista. Si no aparece en la lista alguno de los controladores buscados, se debe salir de SHGEN pulsando [Esc] y luego ejecutar el nivel detallado.

Al pulsar [Enter] con el nombre de la NIC resaltado, aparecerá el controlador en el menú "Selected Configurations" en la parte superior de la pantalla, junto con la indicación de si se desea continuar la instalción con el controlador seleccionado ("Continue Shell Generation Using Selected Configuration?).

Al responder "Yes", SHGEN llama a la rutina que enlaza IPX.COM con el controlador seleccionado. Si se trabaja con una sola unidad de disco o se tiene un disco incorrecto en B: aparecerá un mensaje indicando que se coloque el disco correcto en la unidad. Así por ejemplo:

```
Insert Disk LAN_DRV_001 in any drive
Strike any key when ready...
(Inserte el disco LAN_DRV_001 en una unidad.
Pulse cualquier tecla para continuar...)
```

A lo largo de este proceso, SHGEN puede seguir solicitando otros diskettes. Una vez que se han cargado todos los archivos necesarios, aparecerá en pantalla el siguiente mensaje:

```
Configuring SHGEN-1 :IPX.
(Configurando SHGEN-1 :IPX)
```

Al terminar la configuración se indica que se pulse [Esc] para continuar. Al hacerlo, aparece el indicador de órdenes del DOS. El archivo IPX.COM depositado por el sistema en el diskette SHGEN_1 ya está configurado y listo para trabajar en la estación con la NIC seleccionada.

Antes de intentar generar otros archivos shell, debe copiarse en su diskette de arranque maestro el archivo IPX.COM acabado de configurar, junto con los siguientes:

* NET2.COM
* NET3.COM
* NETBIOS.EXE
* INT2F.COM

Los dos últimos sólo se necesitan para ejecutar el emulador NetBios de Netware. Algunos paquetes de aplicación necesitan tenerlo instalado antes de ejecutarse. Una vez que se han copiado estos archivos, debe hacerse lo siguiente:

* Escribir el nombre de la NIC seleccionada en la etiqueta de su diskette de arranque maestro (por ejemplo ARCnet).
* Proteger contra escritura el diskette de arranque maestro.

Puede verse la configuración del diskette de arranque maestro mediante el uso de la orden TYPE del DOS. PAra hacerlo debe insertarse el diskette en la unidad A: y escribir en el indicador

TYPE CONFIG.DAT

Al pulsar [Enter], se verá la configuración en pantalla.

Ahora sólo hay que probar el diskette de arranque en la estación y si se desea crear un archivo AUTOEXEC.BAT para trabajar conectado

en red. Una vez realizados los pasos anteriores se esta lista para trabajar en la estación de trabajo.

Arranque del servidor.

Se debe comenzar por arrancar el servidor con el DOS. Para un servidor no dedicado, debe ejecutarse a continuación la orden NET$OS. El archivo NET$OS.EXE está contenido en el diskette OSEXE-2. Puede colocarse este diskette en la unidad A: del servidor y ejecutar NET$OS desde el indicador del DOS: O puede también copiarse NET$OS.EXE en un diskette de arranque DOS, donde este un archivo AUTOEXEC.BAT con una orden NET$OS.EXE.

También podria usar NET$OS.EXE desde una estación conectada al servidor. Lo más frecuente será arrancar su servidor simplemente desde el disco fijo al encenderlo.

Para un servidor no dedicado, se necesita un diskette de arranque, y junto con NET$OS.EXE colocar en él el archivo NETx.COM apropiado. Los archivos NETx.COM configurados con SHGEN están en el diskette SHGEN-1 . Si se ejecutó SHGEN usando el método de disco duro estará en el subdirectorio SHGEN-2 debajo del directorio de NETWARE.

El último paso, después de la instalción de los archivos del sistema operativo, es la instalación del software de aplicación. Dependiendo de la versión de Netware, puede venir con algún paquete extra de base de datos además del programa infobase de ayuda para el manejo del sistema operativo.

APENDICE B

SUPERVISOR DE LA RED.

Una vez instalado el sistema operativo y antes de empezar a trabajar en red, debe designarse una persona o grupo de personar como administrador o supervisor de la red. Esta persona será la responsable del buen funcionamiento de la red, debe evitar conflictos, asignar derechos, establecer niveles de seguridad, etc. En este punto trataré las tareas que debe realizar el supervidor y el modo en que Netware le facilita esta tarea.

El usuario supervisor. El SUPERVISOR es un poderoso usuario capaz de hacer casi cualquier cosa en la red, incluyendo las siguientes:

* Crear nuevos usuarios y definir sus caracteristicas de seguridad.
* Crear grupos, sus caracteristicas de seguridad y hacer a los usuarios miembros de un grupo.
* Borrar usuarios de la lista de miembros de un grupo o también dar de baja a un usuario.
* Crear colas de impresión y determinar a que usuarios les está permitido actuar como *operadores de cola*.
* Designar usuarios como *operadores de consola*.
* Crear usuarios equivalentes al SUPERVISOR, los cuales tienen todos los derechos del supervisor.

El usuario SUPERVISOR no puede borrarse de la lista de usuarios de un servidor. Pero debido al poder del SUPERVISOR, deberá establecer una contraseña confidencial que debe ser introducida por cualquiera que quiera entrar como SUPERVISOR.

La forma de designar derechos, dar de alta usuarios, asignar grupos, etc. se verá más adelante, por ahora nos enfocaremos a la planeación previa al funcionamiento de la red.

Lo primero que debe hacerse como administrador de la red es escribir en una hoja en blanco los grupos de trabajo que desea tener. Así como Netware crea automáticamente al usuario SUPERVISOR, también existe el grupo EVERYONE. Una lista de grupos podría ser como sigue:

EVERYONE
EJECUTIVO
CONTABILIDAD
OPERACIONES
COBROS
PAGOS
INVENTARIO
PROYECTOS
LOTUS_MGR
INGENIERIA

Un buen plan debe considerar las futuras ampliaciones a la red. Evite hacer sólo un plan "para empezar", aunque se tarde un poco más ahora, se ahorrará mucho tiempo en el futuro.

El siguiente paso es hacer una lista de usuarios, incluya aquellos que por el momento no usarán la red pero que tengan alguna relación con ésta. Dependiendo del grupo al que pertenezca el usuario y a los derechos asignados al grupo y a éste se determina lo que puede hacer en la red. Deberá tener una lista como la que ilustra la figura B.1

	EVERYONE	BACKUP_MGR	WP50_MGR	CLIENTE_DB	EQUIPO_DB	WP50_USUARIO	EJECUTIVO
GUEST	X						
JOSE	X				X		X
VANESA	X		X				
VIKI	X	X			X		

Fig. B.1 Tabla de correspondencia entre usuarios y grupo

El siguiente paso a realizar por el supervisor o administrador de la red es la elaboración de un diagrama de árbol de directorios. Debe considerar todas las aplicaciones y en base a ellas elaborar un bosquejo para su estructura de directorios como el ejmemplo mostrado en la figura B.2 .

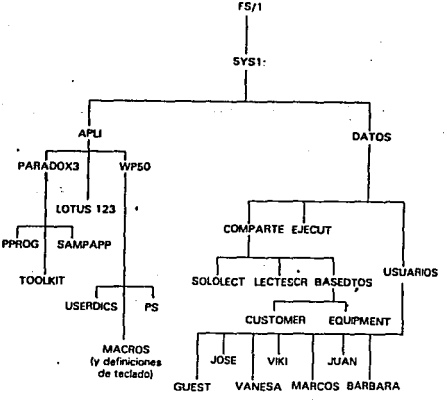


Fig. B.2 Estructura de subdirectorios en el servidor

Después de tener el bosquejo de subdirectorios debe realizar la planificación de derechos usando en formulario en blanco que viene dentro de los manuales de Netware. Es conveniente sacar varias copias ya que puede haber varias modificaciones posteriores. Escriba la estructura de directorios en la parte superior del modelo de planificación de derechos sobre directorios

para grupos. Hay dos sugerencias que debe seguir.

- Liste cada directorio y subdirectorio en la parte superior de la tabla de planificación. Esto le ayudará a asegurar que los derechos de usuarios sean definidos en el nivel correcto de su estructura de directorios.

- Cuando cambie el nivel de su estructura de directorios, deje un par de columnas en blanco. Posteriormente podría querer volver a elaborar la estructura de árbol de su directorio y dejando espacios siempre tendrá donde insertar un subdirectorio adicional.

La figura B.3 muestra un ejemplo de un modelo de planificación de derechos sobre directorios para grupos.

Fila	Columna 1		Columna 2	Columna 3	Columna 4	Columna 5	Columna 6	Columna 7	Columna 8
1	Derechos de directorio < >		<COMPRSW>	<COMPRSW>	<COMPRSW>	<COMPRSW>	<COMPRSW>	<COMPRSW>	<COMPRSW>
2	Derechos de usuario ( ) / Derechos efectivos [ ]		TAPERACE	APLI/	APLI/ LOTUS123	APLI/ WP50/	APLI/ WP50/ USERDICS	APLI/ WP50/ MACROS	APLI/ WP50/ PS
3	EVERYONE	(TA)	[__O_RS_]	[__O_RS_]	[ ]	[ ]	[C__O_RSW]	[ ]	[C__O_RSW]
4		[ER]	[__O_RS_]	[__O_RS_]	[__O_RS_]	[__O_RS_]	[C__O_RSW]	[__O_RS_]	[C__O_RSW]
5	BACKUP_MGR	(TA)	(C__O_RSW)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
6		[ER]	[C__O_RSW]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]
7	WP50_MGR	(TA)	[ ]	[ ]	[ ]	[CDMOPRSW]	[*]	[ ]	[ ]
8		[ER]	[ninguno]	[ninguno]	[ninguno]	[CDMOPRSW]	[CDMOPRSW]	[CDMOPRSW]	[CDMOPRSW]
9	EJECUTIVO	(TA)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
10		[ER]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]
11	CLIENTE_BD	(TA)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
12		[ER]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]
13	EQUIPO BD	(TA)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
14		[ER]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]	[ninguno]
15	USUARIO_WP50	(TA)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
16		[ER]	[ ]	[ ]	[ ]	[.]	[ ]	[ ]	[ ]

Fig. B.2 Tabla de planificacion de seguridad para grupos

La explicación de los derechos de usuario y de grupo, así como la forma de asignarlos se tratará en el siguiente punto.

El supervisor o administrador de la red no sólo debe realizar la

planeación previa al funcionamiento de la red, sino que ya estando en funcionamiento la red debe de realizar labores de mantenimiento y estar siempre al pendiente del buen funcionamiento y la seguridad de la misma. El administrador será un usuario más pero con derechos especiales sobre los demás. Novell asigna a este usuario precisamente como SUPERVISOR. Lo que puede hacer este usuario y como debe hacerlo será tema de los puntos siguientes.

NIVELES DE SEGURIDAD

Como mencione anteriormente. Netware tiene cuatro niveles de seguridad.

* Login y password
* Derechos de usuario
* Derechos de directorio
* Atributos de los archivos

Ahora veremos como funciona cada uno de ellos. Para iniciar una sesión en su estación de trabajo debe tener listo su diskette de arranque. Al indicativo de DOS teclear lo siguiente:

```
IPX
NET3
PROMPT $P$G
F:
LOGIN
```

También puede crear un archivo AUTOEXEC.BAT con las anteriores instrucciones y entrar al servidor automaticamente. Después de teclear LOGIN se le preguntará lo siguiente

```
F:\> LOGIN
Enter user's name:
(Entre nombre del usuario)
```

Escriba el nombre y pulse [Enter], en seguida el sistema le pedirá su contraseña o password. La contraseña puede ser previamente establecida por el supervisor o por usted mismo. Si no sabe su contraseña, se le negará el acceso a la red indicandole a que servidor está conectado. Se verá lo siguiente:

```
Enter your password:
Access to server denied
You are attached to server FS1
```

Otra posibilidad para negar el acceso es que el usuario no este dado de alta, en cuyo caso sólo el supervisor lo podrá corregir. Existen otras restricicones para acceso al sistema, mismas que el supervidor determina con anterioridad. Estas son:

Sesiones concurrentes. En teoría, un usuario podría establecer hasta 100 sesiones en un servidor particular, que es el número máximo de sesiones que Netware 286 y SFT Netware pueden controlar simultáneamamente. Si usted quiere puede limitar el número de sesiones concurrentes que puede llevar a cabo cualquier usuario. Esto no sólo impide que un usuario acapare el servidor, también lo obliga a desconectarse de la estación de trabajo antes de ir a otra parte del edificio a utilizar una segunda estación de trabajo. Si un usuario debe salirse, nadie podrá usar su cuenta en su ausencia.

En una pequeña oficina puede que esta limitación de sesiones concurrentes no sea necesaria. O puede querer que algunos de sus usuarios puedan establecer dos o tres conexiones concurrentes. Por ejemplo:

* Un usuario encargado de asistencia en la red encontrará conveniente poder iniciar con el nombre del usuario al que está ayudando.

Restricciones temporales. Consiste en limitar las horas de cada día, y los días de la semana durante los cuales está permitido a un usuario establecer una sesión. Por ejemplo, esto es muy útil si se quiere estar seguro de que los usuarios no entren mientras se realiza una copia de seguridad, o si quiere asegurarse de que no se utilice la red durante los fines de semana. Las restricciones temporales son específicas para cada usuario y pueden definirse en forma diferente para cada uno de ellos. Cada usuario puede establecer sus propias restricciones, pero sólo el supervisor puede restringir otros usuarios.

Bloqueo de intrusos. Otra caracteristica que puede utilizar es el bloqueo de intrusos. Esta caracteristica, si se utiliza, se aplica por igual a todos los usuarios en su servidor.

Si un intruso desea entrar en una cuenta de usuario, seria bastante fácil averiguarlo, leyendo en la pantalla del usuario el nombre utilizado para entrar. Sin embargo, las contraseñas no se visualizan en pantalla al teclearlas. Un intruso puede intentar entrar con su nombre pero le costará trabajo encontrar su password.

El bloqueo de intrusos controla el número de veces que puede equivocarse en la contraseña. Una vez que se excede el número de intentos permitidos sin dar la contraseña correcta (por omisión son siete veces) la cuenta es bloqueada y los posteriores intentos de entrar son rechazados por un periodo de tiempo que usted puede variar (por omisión son 15 minutos).Es decir, nadie podrá entrar con su cuenta por el tiempo predeterminado aún cuando de la contraseña correcta.

Para establecer estas opciones de seguridad, se debe entrar al menu SYSCON. Para hacerlo teclee SYSCON y aparecerá la pantalla ilustrada en la figura B.4 . Desde esta pantalla se puede pedir ayuda pulsando la tecla [F1] dos veces. Pulsando [Esc] dos veces se regresa al menú anterior.

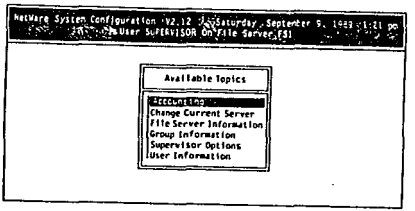


Fig. B.4 Pantalla de opciones disponibles en SYSCON

Para establecer restricciones temporales globales por omisión, sitúese sobre "Supervisor Options" y pulse [Enter]. Verá una lista con las opciones del supervisor, como se muestra en la figura B.5.

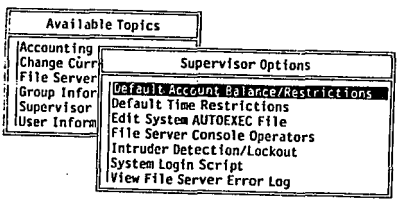


Fig. B.5 Opciones SYSCON para el SUPERVISOR

Seleccione "Default Time Restrictions" y pulse [Enter]. Aparece una pantalla con los días de la semana en la columna izquierda y en la parte superior, las horas y medias horas de cada día, marcadas con un asterisco (fig. B.6). Los asteriscos indican que la entrada está permitida por periodos de media hora. Usando las flechas se puede mover a lo largo de la tabla.

Para borrar un asterisco, pulse la [barra espaciadora]. Para reemplazar un asterisco pulse [Ins]. Estas restricciones globales son aplicables a los usuarios que se den de alta a partir de ese momento. Para restricciones a usuarios ya activos, debe seleccionarse "Other User Information".

Para establecer restricciones para la detección de intrusos, en el menú SYSCON seleccione "Supervisor Optionns" y dentro de este submenu seleccione "Intruder Detection/Lockout". Aparecerá la figura B.7. Para activar la detección de intrusos debe poner Yes. las demas opciones son el número de intentos y el tiempo de bloqueo. usted puede cambiar los valores que Netware asigna por default.

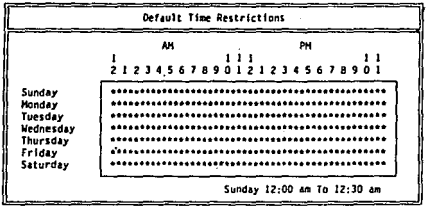


Fig. B.6 Plantilla para limitar los dias y horas de conexion

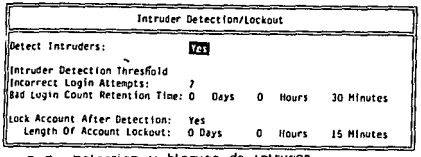


Fig. B.7 Deteccion y bloqueo de intrusos

Para dar de alta a un usuario también se utiliza el menú SYSCON. Si selecciona "User Information", se verá la lista de usuarios actualmente definidos en el servidor como en la figura B.8.

En un servidor Netware recientemente instalado, sólo aparecen dos usuarios: GUEST y SUPERVISOR. Para añadir un nuevo usuario a lista (debe ser el SUPERVISOR de la red, de lo contrario se negara el acceso) pulse la tecla [Ins]. Esta tecla se utiliza en todos los menús para añadir un elemento a la lista. Verá una ventana donde puede introducir un nombre de usuario. Introdusca el nombre y pulse [Enter]. El usuario se integrará a lista en orden alfabético. Pulse [Esc] para regresar al menú "Available Topics" de SYSCON.

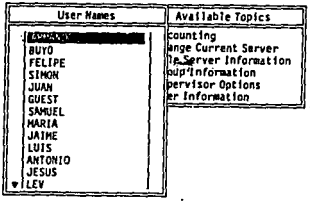


Fig. B.8 Lista de usuarios de SYSCON

El siguiente paso, después de dar de alta a un usuario es asignarle una contraseña. Para esto no ubicamos nuevamente en el menú "Available Options" en la opción "User Information". Al pulsar [Enter] se vera como en la figura B.9 . Dentro de este submenú ubiquese en "Change Password" teclee [Enter] y aparecerá una ventana donde teclear su contraseña. La contraseña la deberá

teclear dos veces a manera de confirmación.

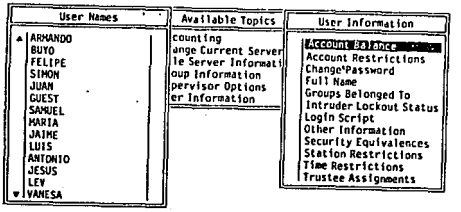


Fig. 8.9 Pantalla "User Information" de SYSCON

El siguiente nivel de seguridad de Netware son los derechos de usuarios. Para establecer estos derechos es necesario ser el SUPERVISOR o al menos tener los derechos equivalentes.

Los derechos que pueden tener los usuarios son los siguientes:

1. R (READ)	Lectura de archivos abiertos
2. W (WRITE)	Escribir en archivos abiertos
3. O (OPEN)	Abrir archivos existentes
4. C (CREATE)	Crear archivos y directorios
5. D (DELETE)	Borrar archivos y directorios
6. S (SEARCH)	Buscar archivos en el directorio
7. M (MODIFY)	Modificar nombre y atributos de un archivo y nombre del directorio.
8. P (PARENTAL)	Derecho de propiedad que permite acceso a otros usuarios y la creación de subdirectorios

Para otorgar derechos debe accesar la red como supervisor y entrar al menu SYSCON. En este menú seleccione "User Information", aparecerá la lista de usuarios. Seleccione el usuario al que desea otorgar o quitar derechos, pulse [Enter] y aparecerá el submenú

"User Information" , seleccione "Trustee Asignments" y aparecerá una pantalla como la de la figura B.10. Como podrá ver, en pantalla aparecen del lado izquierdo los directorios a los que se tiene acceso en el servidor y del lado derecho los derechos sobre esos directorios. Podemos otorgar acceso a más directorio pulsando [Ins] y tecleando la nueva ruta de acceso o directorio. Para otorgar derechos se debe ubicar en el directorio deseado, pulsar [Enter] y aparecerá una pantalla con los derechos. Para agregar uno más debe pulsar [Ins] y escoger el derecho, para quitar un derecho debe pulsar [Del].

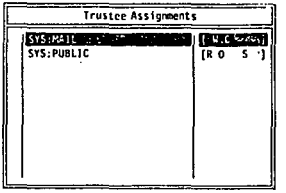


Fig. B.10 Menu de Trustee Asignments

Otra caracteristica de Netware es poder agrupar a los usuarios. De esta manera resulta más fácil tener algunos cuantos grupos en ves de varios usuarios. Podemos asignar derechos al grupo, los cuales serán los mismos para todos los usuarios. La planeación previa nos permite llevar a cabo esta tarea de manera eficiente. Para integrar un grupo debe escogerse la opción "Group Information" dentro del menú "Available Topics" de SYSCON al pulsar [Enter], aparecerá una lista con los grupos existentes en el servidor. Si

la red está recién instalada sólo aparecerá el grupo EVERYONE. Para dar de alta nuevos grupos debe pulsar la tecla [Ins] y teclear el nombre del grupo. Ya ha creado un grupo pero por el momento no tiene ningún miembro. Ubíquese en el nombre del grupo deseado y presione [Enter] y verá la pantalla como la figura B.11

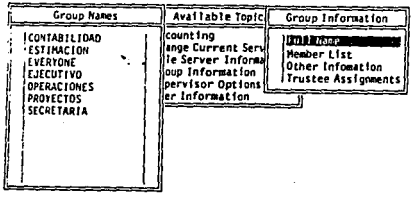


Fig. B.11 Pantalla "Group Information" de SYSCON

Dentro del submenú "Group Information" seleccione "Member List" al pulsar [Enter] aparecerán los nombres de los usuarios pertenecientes a ese grupo. Para dar de alta nuevos miembros se sigue el mismo procedimiento que en otros menús de pulsar [Ins] y en nombre del usuario. De igual manera para dar de baja a alguien se pulsa [Del]. La pantalla se verá como la figura B.12

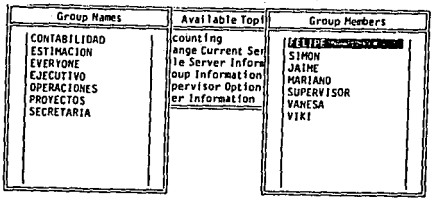


Fig. 8.12 Lista de miembros del grupo EJECUTIVO

El siguiente nivel de seguridad son los derechos de directorio. Estos derechos son los mismos que los derechos de usuario pero se asignan a un determinado directorio o subdirectorio del servidor. La combinacion de los derechoos nos da como resultado los derechos efectivos del usuario.

Atributos de los archivos. Este es el último nivel de seguridad de Netware. Por ejemplo, si un usuario tiene derechos efectivos para borrar archivos en un área o directorio especifico, pero los atributos del archivo no lo permiten, no podrá borrarlo.

Los atributos de los archivos son:

Transacciones	(transaction) (Usado por el sistema "Transaction Tracking System")
Indexado	(Indexed) Incluido en una tabla privilegiada
Oculto	(Hidden) No permite ser borrado, ni ejecutado ni copiado
Sistema	(System) Funciones del sistema
Modificado	(Modified since last backup)

Los atributos que se aplican directamente a la seguridad son:

* Leer/Escribir (Read/Write)

* Solo lectura (Read Only)
* Normal (Normal)
* Compartido (Shareable)
* No Compartido (Non-Shareable)

y sus combinaciones

SRW (Compartido, lectura y escritura)
SRO (Compartido solo lectura)
NRW (No compartido lectura y escritura)
NRO (No compartido solo lectura)

Lo más común es que los archivos de los programas tengan como atributos SRO, para que puedan ser utilizados por todos los usuarios y no exista el peligro de que sean borrados. Para cambiar los atributos es necesario tener el derecho efectivo de Modificación (M) en el directorio donde se encuentre el archivo.

ACCESO AL SISTEMA

Como mencioné anteriormente, para poder accesar al servidor de la red debe de contar con un diskette de arranque mismo que se configuró en el proceso de instalación. Este diskette cuenta con los siguientes archivos: IPX.COM, NETx.COM aparte de los archivos de arranque del DOS. Para iniciar la sesión en red puede teclar las siguientes instrucciones o incorporarlas al archivo AUTOEXEC.BAT.

```
IPX
NET3
F:
LOGIN
```

Una vez conectado al servidor de la red, hay dos maneras de interactuar con Netware. Una es desde el indicador de órdenes similar al de DOS y la otra es a través de menús.

Cabe mencionar que las instrucciones de Netware son muy similares a las de DOS e inclusive las instrucciones de DOS son compatibles con Netware.

En la figura B.13 se muestra un ejemplo de menús de Netware. Este menú se ejecuta desde el indicador de DOS usando la orden MENU. Por ahora, estas son las funciones que nos interesan. Con la excepción del número 9, Logout, que nos saca del servidor, cada opción tiene un menú especifico asociado como el menú de SYSCON que vimos en el punto anterior. Cada uno de estos menús pueden ejecutarse indicidualmente por su nombre desde el indicador de DOS. Los siguientes son los posibles nombres de menús Netware, que pueden utilizarse desde el indicador de DOS o desde el menú MAIN:

```
1 Session
2 Filer
3 Volinfo
4 Syscon
```

5 Fconsole
6 Pconsole
7 Printcon
8 Printdef

El menú que muestra la figura 8.13 viene incluido en Netware, pero es un menú que podría hacerlo usted mismo. La posibilidad de que los usuarios puedan crear menús personalizados, incluso si son inexpertos, es una característica a destacar de Netware.

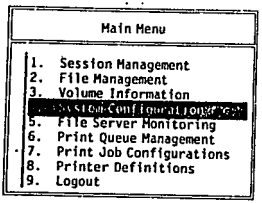


Fig. 8.13 Pantalla de MAIN.MNU de Netware

Los menús de Novell personalizados se crean sobre un archivo de texto ASCII, con una serie de requerimientos de diseño. El archivo de texto que define a MAIN es el siguiente:

```
%Main Menu,0,0,3
1. Session Management
        Session
2. File Management
        Filer
3. Volume Information
        Volinfo
4. System Configuration
        SysCon
5. File Server Monitoring
        FConsole
6. Print Queue Management
        PConsole
7. Print Job Configurations
        PrintCon
8. Print Definitions
        PrintDef
9. Logout
        Logout
```

Como podrá notar, para tener acceso al servidor, nos tenemos que cambiar al drive F: Esto es porque generalmente los drives de A: a E: son considerados drives locales propios de la estación de trabajo. Sin embargo, no sólo podemos utilizar el drive F:, de hecho Netware nos permite usar las letras de unidades de la "A" a la "Z" para tener acceso a directorios específicos. Dentro de la red usted puede organizar sus archivos en varios subdirectorios como se hace en DOS, pero también podemos organizarlos en drives lógicos. Se puede acceder a estas vías de acceso escribiendo simplemente la letra asociada en el indicador.

Si se olvida qué letras están asociadas con las vías de acceso o asignaciones, escribiendo MAP y pulsando [Enter] se obtiene esa información. Por ejemplo,

```
Drive A: maps to a local disk
Drive B: maps to a local disk
Drive F: = FS1/SYS:LOGIN
Drive H: = FS1/SYS1:DATOS/USUARIOS/FRANCISCO
Drive I: = FS1/SYS1:
Drive J: = FS1/SYS1:OSAS/DATOS
Drive K: = FS1/SYS1:DATOS/USUARIOS
Drive L: = FS1/SYS1:DATOS
Drive M: = FS1/SYS:
Drive P: = FS1/SYS1:DATOS/PRODATOS
Drive R: = FS1/SYS1:DATOS/COMPARTE/SOLOLECT
Drive S: = FS1/SYS1:DATOS/COMPARTE/LECTESCR

    ============

SEARCH1:  = Z:. [FS1/SYS:PUBLIC]
SEARCH2:  = Y:. [FS1/SYS:PUBLIC/ACER/IBM_PC/V3.3]
SEARCH3:  = X:. [FS1/SYS:APLI/LOTUS]
SEARCH4:  = W:. [FS1/SYS:APLI/WORD]
SEARCH5:  = V:. [FS1/SYS:APLI/PROJECTS]
SEARCH6:  = U:. [FS1/SYS:PUBLIC/MENSAJES]
SEARCH7:  = T:. [FS1/SYS:MNT_TAPE]
SEARCH8:  = Q:. [FS1/SYS:SYSTEM]
```

Para apuntar a la localización FS1/SYS1:DATOS/USUARIOS en el servidor de archivos, habría que pulsar K: y [Enter]

La instrucción SEARCH es una trayectoria de búsqueda y Netware permite crear hasta 16 unidades. SEARCH funciona de manera similar al PATH de DOS. Es decir, si esta definida una unidadad de busqueda un archivo puede ser llamado desde cualquier parte siempre y cuando este incluido en la trayectoria.

Otra instrucción que tratare en este punto el el LOGIN SCRIPT que es el equivalente al AUTOEXEC.BAT de DOS. La diferencia radica en que el LOGIN SCRIPT funciona al accesar al servidor y no al arrancar la estación. Se puede crear un LOGIN SCRIPT personal que funcione al accesar la red con nuestro usuario, o podria hacerce un LOGIN SCRIPT general si el SUPERVISOR lo desea.

Para crear un LOGIN SCRIPT tenemos que llegar al menú "User Information" del menú SYSCON. Dentro de este submenú seleccione "Login Script", al pulsar [Enter] aparecera una pantalla editor de textos donde podrá teclar su LOGIN SCRIPT.

Las instrucciones más comunes que puede usar para editar su LOGIN SCRIPT son las siguientes:

```
MAP DISPLAY ON          Habilita despliegue de drives
MAP DISPLAY OFF         Deshabilita despliegue de drives
WRITE "mensaje" Identificador       Para escribir en pantalla
WRITE "mensaje %Identificador mensaje"
```

Identificadores:

HOUR	Da la hora de 1 a 12
HOUR24	Da la hora de 0 a 23
MINUTE	Da los minutos de 00 a 59
SECOND	Da los segundos de 00 a 59
AM_PM	Indica si es am o pm
MONTH	Da el número de mes de 0 a 12
MONTH_NAME	Nombre del mes
DAY	Dia del mes de 0 a 31
NDAY_OF_WEEK	Número del dia de la semana (Domingo = 1)
YEAR	Año 19XX
SHORT_YEAR	Año XX (Ej. 91)
DAY_OF_WEEK	Dia de la semana
LOGIN_NAME	Nombre del usuario
FULL_NAME	Nombre completo del usuario

STATION Número de estación

GREETING_TIME Saludos: Good morning, afternoon, evening

También es posible usar operadores lógicos y estructuras IF...THEN para crear una especie de pequeños programas. La figura 8.14 es un buen ejemplo de un LOGIN SCRIPT.

```
NetWare System Configuration  V2.12          Thursday  May 23, 1991  10:11 am
                    User FRANCISCO On File Server ICM

                        Login Script For User FRANCISCO

WRITE "GOOD %GREETING_TIME % LOGIN_NAME"
MAP DISPLAY OFF
MAP INS S1:=SYS:\PUBLIC
MAP INS S2:=SYS:\TRABAJO\MATUTINO\DB
MAP *1:=SYS:\TRABAJO\MATUTINO\DB\PACO
MAP DISPLAY ON
MAP
WRITE ""
WRITE "              HORA:%HOUR:%MINUTE:%SECOND  %AM_PM"
IF HOUR24 > "01" AND HOUR24 < "14" THEN BEGIN
        WRITE ""
        WRITE "          BUENOS DIAS      "; LOGIN_NAME
        FIRE 5 TIMES
END
WRITE ""
WRITE "      HOY ES %DAY_OF_WEEK    %DAY /%MONTH_NAME /%SHORT_YEAR"
#SK
```

Fig. 8.14 Ejemplo de LOGIN SCRIPT para usuario Francisco

La primera línea del LOGIN SCRIPT indica que debe escribir un saludo de "GOOD (MORNING, AFTERNOON, EVENING) dependiendo de la hora seguido del nombre del usuario. Enseguida se deshabilita la orden de map y se crean dos trayectorias de búsqueda con la orden MAP INS S1 y MAP INS S2, después apuntamos al directorio \TRABAJO\MATUTINO\DB\PACO con la orden MAP *1. Volvemos a activar el mapeo de drives y pedimos un despliegue de estos. (Más adelante explicare en forma más detallada el uso de MAP).

Las siguientes ordenes nos proporcionan la hora exacta con horas, minutos y segundos). Después hay un pequeño bucle IF...THEN para

determinar la hora del día. Si es entre las 01 y 14 horas despliega un mensaje de "BUENOS DIAS" y produce un "beep" 5 veces con la orden FIRE 5 TIMES. La siguiente instrucción es para que nos proporcione el día de la semana, mes y año.
Por último con la instrucción #SK se ejecuta el archivo SK.

IDENTIFICACION Y COMUNICACION ENTRE USUARIOS

Una característica importante de las redes es la de poder comunicarse con los diferentes usuarios quienes tienen una identificación única definida por su nombre de usuario y número de estación. El número de estación lo asigna Netware de acuerdo al momento en que se conecte al servidor.

Las principales órdenes para la indentificación y comunicación entre usuarios son las siguientes. Estos comandos se teclean desde el indicativo de DOS.

WHOAMI. Despliega el nombre del usuario, el servidor, número de estación, la versión del Sistema Operativo Netware, la fecha y hora de entrada a la red.

Sintaxis:

WHOAMI [Servidor][/opción]

Opciones:

/Groups	Indica a que grupos pertenece
/Security	Muestra las equivalencias de seguridad
/Rights	Muestra los derechos efectivos en cada directorio.
/All	Muestra la información de las tres opciones anteriores.

Ejemplo:

WHOAMI STAFF /G/R

Indica quien soy en el servidor STAFF, incluyendo los grupos a los que pertenezco y los derechos efectivos en los directorios del servidor.

USERLIST. Despliega la lista de usuarios que están activos en cualquier servidor conectado a la red, el número de estación y la fecha y hora de entrada a la red.

Sintaxis:

USERLIST [Servidor/][[Usuario][/opción]

Opcion:

/All	Muestra la dirección de la red y del nodo en el que se encuentra trabajando el usuario.

Ejemplos:

USERLIST STAFF/Alex

Muestra la estación, fecha y hora de entrada a la red del usuario Alex en el servidor STAFF.

USERLIST /A

Muestra el número y dirección de la estación de trabajo, dirección de la red, hora y fecha de entrada a la red de los usuarios activos del servidor por omisión.

SEND. Esta orden permite enviar mensajes directamente a uno o varios usuarios o a la consola (servidor). El mensaje no debe de exceder de 45 caracteres. Para enviar mensajes a usuarios que se encuentren en otro servidor, es necesario haberse conectado o "Atachado" antes a ese servidor.

Sintaxis:

SEND "mensaje" [TO] opciones

Opciones:

[USER][Servidor/]usuario1 usuario2 ...
Manda el mensaje a los usuarios indicados que se encuentren en un servidor determinado.

[GROUP][Servidor/]grupo1 grupo2 ...
Manda el mensaje a los grupos indicados

[USER][Servidor/]usuario1...[GROUP][Servidor/]grupo1...
Manda el mensaje a los usuarios y grupos indicados

[Servidor/]estación1 estación2 ...
Manda el mensaje a las estaciones con ese número.

[Servidor/]CONSOLE
Manda el mensaje a la consola.

Ejemplo:

SEND "Hola que tal" Alex

Manda el mensaje Hola que tal al usuario Alex.

SEND "Hola que tal" TO 1 2 3

Manda el mensaje a las estaciones de trabajo número 1, 2 y 3

SEND "Hola que tal" STAFF/Alex STAFF2/CONTABILIDAD

Manda el mensaje al usuario Alex que se encuentra en el servidor STAFF y al grupo CONTABILIDAD que se encuentra en el servidor STAFF2.

CASTOFF. Esta orden evita que los usuarios reciban mensajes de otra estación de trabajo, si el mensaje es enviado desde la Consola el CASTOFF no tiene efecto.

Sintaxis:

CASTOFF

Ejemplo:

CASTOFF

La estación no podrá recibir mensajes de otras estaciones de trabajo.

CASTON. Deshabilita el candado colocado por el CASTOFF, permite a la estación de trabajo recibir mensajes de otros usuarios.

Sintaxis:

CASTON

Ejemplo:

CASTON

Reestablece la terminal para recibir mensajes.

MANEJO DE DIRECTORIOS Y ARCHIVOS

Al hablar de los niveles de seguridad y acceso al sistema de Netware ya hemos tratado el manejo de directorios y archivos. En este punto ampliare más la información.

Netware organiza la información almacenada en el servidor como sigue:

* Nombre del servidor. Distingue unos servidores de otros en una red con varios servidores.

* Nombre de volumen. Distingue cada disco fijo o parte de él, conectado al servidor.

* Directorio. Indica el primer nivel, por debajo del volumen, en la organización del disco fijo.

* Subdirectorio. Una o más divisiones lógicas por debajo del nivel de directorio.

Por lo tanto una estructura de directorio puede ser como la siguiente:

F:\> FS1/SYS:USUARIOS/DATOS/FRANCISCO

Netware tiene un volumen llamdo SYS que es indispensable en el servidor. Debajo de ese volúmen también crea automáticamente, en el momento de la instalación, una estructura de cuatro directorios obligatorios. La figura B.15 ilustra la estructura de directorios exigida por Netware, y resume los derechos efectivos que los usuarios tienen en cada uno de ellos.

Los cuatro directorios exigidos que aparecen en la raiz del volumen SYS son LOGIN, MAIL, PUBLIC y SYSTEM. La estructura de subdirectorios bajo MAIL se crea cuando se añaden usuarios al servidor.

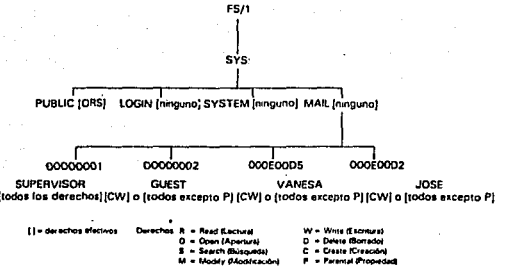


Fig. B.15 Estructura de directorios exigida por Netware y derechos efectivos de usuario.

LOGIN. El directorio LOGIN existe, para permitir a los usuarios entrar en el servidor. Como se muestra en la figura B.15, los usuarios no reciben derechos efectivos en el directorio LOGIN, aunque es posible conectarse a un servidor a través de los servicios del directorio LOGIN. LOGIN existe para asistir a los usuarios en el acceso a la red. Aparte de esta función, los usuarios no tienen derechos en el directorio LOGIN. Sin tener el derecho de búsqueda, no pueden ni hacer un listado de los archivos contenidos en LOGIN.

SYSTEM. Este directorio contiene los archivos necesarios para las operaciones en el servidor y para la administración de la red como SUPERVISOR. Contiene las órdenes de consola de Netware.

Como en LOGIN, los usuarios no tienen derechos efectivos en SYSTEM, por tanto, no tienen acceso a los archivos en SYSTEM. Como SUPERVISOR se puede acceder a los archivos de este directorio con todos los derechos, incluyendo el de borrar archivos. Para evitar borrar accidentalmente los archivos de SYSTEM puede darles el

atributo de sólo lectura.

PUBLIC. El directorio PUBLIC contiene las órdenes de Netware y los archivos ejecutables utilizados por los usuarios. Las órdenes que se ejecutan en el indicador de Netware están en PUBLIC. Netware concede a los usuarios sólo los derechos mínimos necesarios para usar los archivos de PUBLIC: Busqueda, Apertura y Lectura. Sólo el SUPERVISOR o un usuario equivalente puede modificarlos o borrarlos.

MAIL y sus subdirectorios para los usuarios. Es el último de los directorios exigidos por Netware y por debajo de el, los subdirectorios específicos de usuario. Los subdirectorios de MAIL se nombran con el código alfanumérico con el que el servidor identifica a cada usuario. Estos subdirectorios tiene la función de servir como "buzón" en aplicaciones de Correo Electrónico.

Ordenes de administracion de archivos y directorios de Netware.

Las órdenes de administración de archivos y directorios de Netware proporcionan una mayor funcionalidad que la de DOS. Mencionare las más importantes.

LISTDIR y NDIR. Las órdenes LISTDIR y NDIR de Netware son equivalentes a la orden DIR del DOS. La diferencia está en que las órdenes de Netware listas los archivos y subdirectorios separadamente.

NDIR es mucho más potente que la orden DIR del DOS. Están permitidos los comodines del DOS (* y ?). Sin embargo, usando el parámetro SUB, se puede buscar un archivo en todos los directorios y subdirectorios de un volumen de disco duro. Hacer esto en el DOS significa ir cambiando de directorio y usar cada vez la orden DIR.

Una vez situados en la raiz del volúmen SYS: del servidor, debe escribir la orden:

NDIR *.EXE SUB

Al pulsar [Enter] verá una lista de todos los archivos ejecutables debajo de su volumen SYS:, directorio por directorio.

NCOPY. NCOPY trabaja como la orden COPY del DOS, excepto que NCOPY visualiza, para cada archivo, el directorio en el que es leido el archivo, el directorio en el que es copiado y los nombres que recibe en cada directorio. En la mayoria de los casos, la orden COPY tendrá el mismo efecto que la orden NCOPY. La única diferencia es que se puede usar NCOPY para copiar un archivo desde un directorio a otro.

Para borrar archivos Netware utiliza las mismas órdenes del DOS que son **DEL** y **ERASE**. La diferencia en este caso es que Netware posee un comando que nos permite recuperar los archivos que hayamos borrado previamente. Este comando es **SALVAGE**. Para usar esta orden sólo es necesario teclear SALVAGE y el nombre del archivo a recuperar. Este comando será inútil si paso algo de lo siguiente:

* Se sale del servidor y luego vuelve a entrar.
* Borra otro archivo. (SALVAGE sólo recupera el último archivo)
* Utiliza la orden PURGE de Netware que borra permanentemente todos los archivos.

El menu FILER

FILER es el menú de Netware que nos ayuda a manejar todo lo relacionado con directorios y archivos.

Se accede a FILER tecleando FILER y [Enter], aparecerá el menu

"Available Topics" mostrado en la figura B.16. En la cabecera del menú aparece el directorio en el que nos encontramos al ejecutar FILER.

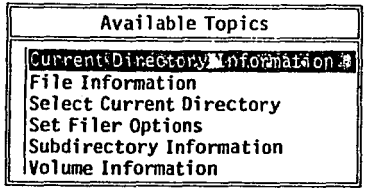


Fig. B.16 Menu "Available Topics" de FILER

Para crear un subdirectorio nos ubicamos en la opción "Select Current Directory" y damos [Enter]. Recuerde que para poder crear un subdirectorio debemos tener los derechos de propiedad en el directorio inmediato superior. Con esta opción aparece una ventana que nos pide el "Current Directory Path" o vía de acceso al directorio. Podemos teclear nuestra ruta de acceso o utilizar la tecla [Ins] y seleccionarla.

Una vez ubicados en el directorio correcto puede crear sus subdirectorios. Mueva el cursos a la opción "Subdirectory Information" y pulamos [Enter]. Verá una lista con los directorios de la red como el mostrado en la figura B.17

Fig. B.17 Menú "Network Directories" de FILER

Para crear un nuevo directorio solo teclee [Ins] y aparecerá una ventana donde debe poner el nombre del nuevo directorio.

Si lo que desea es conocer información respecto al directorio en el cual está trabajando debe escoger la opción "Current Directory Information" y aparecerá el menú de la figura B.18.

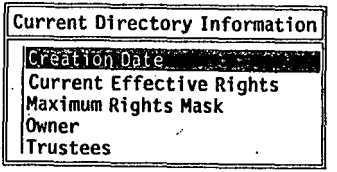


Fig. B.18 Menú "Current Directory Information" de FILER

Si destaca la opción "Creation Date" verá la fecha en que creó ese directorio. Resalte "Current Effective Rights" y pulse [Enter] para averiguar los derechos que tiene sobre ese directorio.

Las demás opciones del menú FILER son muy similares y se refieren a información de los archivos (files) o el volúmen (volume). Es

muy sencillo manejar los menús y siempre se puede recurrir a la opción de presionar [F1] para una pantalla de ayuda. Lo que he presentado en este punto son los aspectos más relevantes del manejo de directorios y archivos.

IMPRESION DE ARCHIVOS

La compartición de impresoras es fundamental cuando se decide instalar una red. En este punto veremos como trabaja Netware para administrar el trabajo de impresión. Netware no permite compartir impresoras conectadas localmente a una estación, pero sí permite conectar hasta cinco impresoras a cualquier servidor e inclusive tener un servidor de impresión dedicado exclusivamente al controlar el flujo de impresiones.

El trabajo de impresión en una red se maneja como se ilustra en la figura B.19. Lo más probable es que el trabajo se envíe desde una aplicación que se ejecuta en una estación. En lugar de enviar el trabajo directamente a la impresora local, el shell de Netware lo *redirige* por los cables de la red hacia una *cola de impresion* del servidor. Las colas de impresión del servidor reúnen trabajos y los mantienen en la RAM del servidor o los envían al disco duro para almacenarlos en caso de que el servidor se desconecte antes de dar el servicio. Cada trabajo espera su turno para recibir servicio en la impresora específica a la que está asignada la cola de impresión. El servidor normalmente envía los trabajos a la impresora según el orden de llegada.

Si hay más de una cola asignada a la misma impresora, como se ve en la figura con PRINTO_C y BAJA_PRIORIDAD, todos los trabajos de la cola de mayor prioridad obtendrán servicio antes que cualquiera de la otra cola.

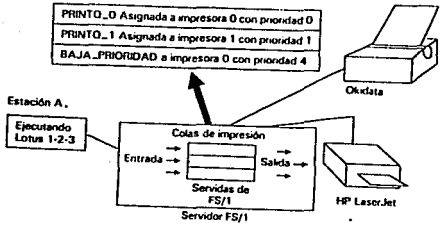


Fig. B.19 Diagrama del camino que sigue un trabajo que se imprime en una impresora de la red.

Para ser reconocidas por el sistema operativo, las impresoras conectadas a un servidor deben instalarse los procesos de intalación o mantenimiento de Netware. En el momento de la instalación, cada impresora tiene asignado un número del 0 al 4. Es recomendable saber el número de cada impresora ya que serán necesarios para asignarles una cola.

Según el numero de impresora Netware por omisión asigna una cola de impresion. Es decir la impresora 0 tendrá una cola PRINTQ_0 y la impresora 4 tendrá una cola PRINTQ_4.

El menú de ayuda para manejar la impresion de archivos se denomina PCONSOLE y se invoca tecleando PCONSOLE y pulsando [Enter]. Aparecerá el menú de la figura B.20

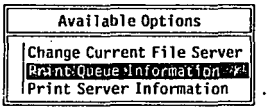


Fig. B.20 Opciones disponibles en el menu PCONSOLE

La primera opción "Change Current File Server" se utiliza cuando se está trabajando en una red multiservidor y se desea conectar con un servidor diferente al actual. Al accesar PCONSOLE, el cursor siempre se coloca sobre "Print Queue Information". Pulsando [Enter] se verá una lista con las colas de impresión del servidor. La figura 8.21 muestra sólo dos nombres de cola de impresión: las colas por omisión establecidas por el sistema operativo durante la instalación. Como sucede con todos los menús de Netware, se puede crear una nueva cola de impresión pulsando [Enter] y proporcionando el nombre de la cola de impresión en la ventana que aparece.

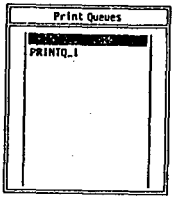
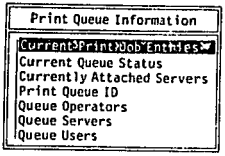


Fig. 8.21 Listado de colas de impresion en PCONSOLE

Para que estas colas lleguen a ser operativas, se debe definir quién puede usarlas (por omisión sólo los del grupo EVERYONE), asignar la cola a una impresora en particular, configurar y designar los operadores de cola (a menos que el SUPERVISOR la administre). Cada cola de impresión puede tener su usuario o grupo de usuario a quienes servir y únicamente los que pertenezcan a su lista de usuarios podrán mandar trabajos a la cola.

Si nos ubicamos en cualquier cola y presionamos [Enter], aparecerá el menu de la figura B.22 "Print Queue Information". En dicho menú, si se selecciona "Queue Users" aparecerá la pantalla ilustrada en la figura B.23 en la que aparece el grupo EVERYONE como único usuario de la cola de la lista. Es decir, todos los miembros del grupo EVERYONE, y solamente ellos, pueden hacer uso de la cola.

Para añadir un usuario a la cola se pulsa [Ins] y se teclea el nuevo grupo o nombre de usuario. Por otro lado si lo que se quiere es borrar a alguien se debe ubicar con el cursor en el usuario o grupo y se pulsa [Del] seguido de [Enter] para confirmar.



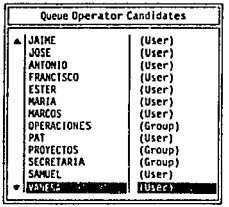


Fig. B.22 Menu de información sobre una cola de impresión

Fig. B.23 Lista de usuarios de una cola de impresión.

Operadores de una cola de impresión.

Cada cola de impresión puede tener uno o más operadores de cola asignados. Un operador de cola de impresión puede hacer los siguiente:

* Marcar la cola para permitir o impedir que la cola sea servida por el servidor.

* Marcar la cola para permitir o impedir que los usuarios dejen sus trabajos en ella.

* Suprimir cualquier trabajo de impresión en la cola.
* Retener un trabajo.
* Retrasar la impresión de un trabajo a una hora y un día específico.
* Cambiar los parámetros de un trabajo de impresión, como, por ejemplo, el número de formato asociado a él.
* Cambiar el orden de impresión de las tareas de la cola.

El SUPERVISOR posee todos los atributos para realizar las acciones anteriores, sin embargo, quiza sea conveniente designar a alguien más como operador de cola de impresión.

Para designar a alguien, debe seleccionar "Queue Operators" de la pantalla "Print Queue Information". Al presionar (Ins) aparecerá la lista de usuarios de la cual usted puede seleccionar. (Figura B.24)

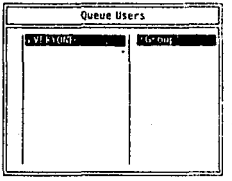


Fig. B.24 Lista de candidatos a operadores de cola

Para que el operador pueda saber el estado actual de la cola y decidir si suprime trabajos o impide que los usuarios mandan más trabajo a la cola, debe seleccionar la opcion "Current Queue Status" y aparecerá una pantalla como la ilustrada en la figura B.25. La sección "Operator Flags" es la que le da un control al operador. Como se ve en la figura pueden establecerse marcas para que los usuarios puedan enviar tareas a la cola, uno o más

servidores pueden servir a la cola, y nuevos servidores pueden conectarse a la cola.

Si una de las dos primeras marcas "Users can place entries in queue" o "Servers can service entries in queue" está puesta a "No", la cola no servirá para nada. Durante la instalación estas tres marcas se ponen en "Yes" por omisión.

Current Queue Status	
Number of entries in queue:	2
Number of servers attached:	1
Operator Flags	
Users can place entries in queue:	Yes
Servers can service entries in queue:	Yes
New servers can attach to queue:	Yes

Fig. B.25 Recuadro del estado actual de una cola

Para ver que trabajos hay en una cola de impresion, se debe seleccionar "Current Print Job Entries". Aparecerá una pantalla como la que se muestra en la figura B.26. Como se ve hay una lista, en este caso con sólo dos trabajos de impresion.

La primera columna indica el número de trabajo, la segunda es el nombre del usuario que mandó a impresión. "LPT1 Catch" es el nombre del trabajo que se da por omisión cuando el usuario no da un nombre especifico. Cuando el statutus está en "Active" quiere decir que el trabajo se está imprimiendo.

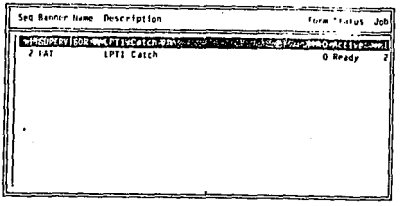


Fig. 8.26 Lista de trabajos de una cola de impresion

Ordenes de impresion de la consola del servidor.

Ciertas tareas deben seleccionarse mediante órdenes de consola, por ejemplo:

* Parar o reaunudar la impresión de un trabajo.
* Retroceder páginas en un trabajo de impresion cuando el papel se estropea y queremos volver a imprimir parte de un documento.
* Montar un formato especifico. Esta es una manera especial de reiniciar la impresión despues de que el servidor nos haya proporcionadola oportunidad de cambiar el papel de la impresora.

Estos comandos se hacen desde el teclado del servidor y por lo tanto debe tener cuidado de quien tiene acceso a el.

Si desea puede adquirir algunos paquetes de software especiales que permiten el control de consola desde una estación de trabajo.

Las principales órdenes de consola son las siguientes:

Para ver una lista de las impresoras intaladas en el servidor, puede escribirse PRINTERS desde el teclado del servidor y pulsar [Enter]. Se verá una lista como la que sigue:

```
FS1 is configured for 3 printers.
Printer 0: Running On-Line Form 0 mounted Servicing 1 Queues
Printer 1: Running On-Line Form 0 mounted Servicing 1 Queues
Printer 3: Running On-Line Form 0 mounted Servicing 0 Queues
```

Si escribe Q y pulsa [Enter], se verá una lista de todas las colas de impresión creadas en el servidor

```
FS1 Print Queue:
PrintQ_0            0 queue jobs     serviced by 1 printers
PRINTQ_1            0 queue jobs     serviced by 1 printers
```

Para ver una lista de trabajos en una cola de impresión particular debe escribirse Q nombre_cola JOBS y pulsar [Enter]. Si hay trabajos en la cola se verá una lista como la que sigue:

```
Jobs currently in Print Queue PRINTQ_0:
  Priority      User        File        Job        Copies      Form
         1      SAM         LST:         1           1          0
```

Se puede activar o detener una impresora desde el servidor. Para detener una impresora, debe utilizarse en modo consola la orden siguiente:

P xx STOP

Hay que sustituir xx por el número de la impresora de red a la que se envió el trabajo. Para que siga imprimiendo se escribe P xx START y se pulsa [Enter].

Si el usuario SUPERVISOR creó una cola desde PCONSOLE, ahora puede asignarla a una o más impresoras conectadas e instaladas en el servidor. Para ello, estando en modo consola, hay que escribir en el servidor:

P nn ADD nueva_cola AT PRIORITY 04

donde nn se sustituye por el número de impresora a la que se desea asignar la cola, y nueva_cola se sustituye por el nombre de la cola creada previamente. La prioridad depende de si ya tenemos otras impresoras instaladas.

Hasta ahora he tratado lo referente a la administración de los trabajos de impresión, sin embargo todavia no vemos como ordenamos esos trabajos. En forma general, cualquier aplicación, LOTUS, DBASE, etc., que tengamos en la red tiene sus propios comandos de impresión sin embargo estos comandos no funcionarán en la red sin que antes le digamos a ésta direccione nuestra salida. La orden de Netware para realizar esta tarea es CAPTURE.

CAPTURE indica que salida de impresión a un puerto de la terminal se mandará hasta una impresora conectada al servidor. Esta orden permite imprimir un archivo en el servidor desde un paquete. Para su adecuado funcionamiento se debe ejecutar antes de cualquier aplicación e inclusiva puede incluirla en su LOGIN SCRIPT.

Su sintaxis es CAPTURE [/opciones]

Las opciones de CAPTURE son las siguientes:

Server.	Enviar hacia un determinado servidor
Queue	Enviar a una cola especifica
Printer = n	Un número entre 0 y 4 correspondiente a la impresora
NAMe	El nombre que aparecerá en la bandera de impresión en lugar del nombre del usuario. No debe exceder de 12 caracteres.
Banner	Impresión de la hoja de identificación o bandera sustituyendo el nombre del archivo por el texto. La bandera es una hoja de identificación que informa quien mandó a imprimir el archivo, nombre del archivo, subdirectorio donde está el archivo, número de estación, la hora y la fecha de impresión.
No Banner	No imprime la bandera de identificación.
Forms	Formato de las hojas, pueden ser el número de la forma o el nombre de la forma.
Copies = n	Un número entre 0-255. Por omisión = 1
Tabs = n	Colocar un tabulador 0-18. Por omisión = 8

No Tabs	Sin tabulador. Recomendable en gráficas.
Form Feed	Manda un salto de hoja a la impresora
No Form Feed	Elimina el salto de hoja
TImeout = n	Número entre 1-1000, indica cuantos segundos tardará en mandarse a impresión.
Autoendcap	Envia el archivo a impresión al salir de la aplicación.
No Autoendcap	Evita la impresion de un archivo al salir de una aplicacióno al entrar. Imprime los archivos hasta que el usuario ejecute la instrucción ENDCAP.
CReate=archivo	Crear un archivo ASCII, para posteriormente imprimirse con la orden NPRINT.
Keep	Permite que el servidor ponga a salvo la información de impresión en caso de jornadas largas de trabajo contra posibles fallas de la estación.
Job =job	Un Job es un conjunto de caracteristicas de impresión predefinidas con el menú PRINTCON y quecontiene la gran mayoria de las órdenes anteriores.
SHow	Permite ver el estado de los puertos de impresión. (No debe usarse con ninguna otra opción).
Local = n	Para impresión local donde n indica el número de puerto.(LPT1,LPT2 o LPT3).

Para ejecutar las opciones es suficiente escribir las letras mayúsculas.

Ejemplos:

```
CAPTURE /P=1/BAN=CONTABILIDAD/C=2/F=0
```

Indica la salida a la impresora 1, la hoja de identificación mostrará el letrero CONTABILIDAD, con dos copias y forma cero.

```
CAPTURE P=1 TI=5 NB NFF
```

Manda el trabajo de impresión a la impresora 1, tiene un tiempo de espera de 5 segundos no lleva hoja de identificación y no da salto de hoja.

Aunque por omisión Netware identifica los trabajos de impresión con el nombre del usuario, es conveniente, especialmente en redes grandes, el colocar un banner o identificación al trabajo y dar una salto de hoja. De esta manera será mucho más facil localizar su trabajo a la hora de pasar a recogerlo.

BIBLIOGRAFIA

REDES LOCALES DE COMPUTADORAS
Protocolos de alto nivel y
Evaluación de Prestaciones
Jose Antao Moura - Jacques Philippe Sauve
William Ferreira Giozza- Jose Fabio Marinho
Ed. Mc.Graw Hill
1990

REDES DE ORDENADORES
Segunda edición
Andrew S. Tanenbaum
Ed. Prentice Hall
1991

LAN TROUBLESHOOTING HANDBOOK
Mark A. Miller
Ed. M & T Books
1989

APUNTES SEMINARIO DE PRODUCTOS
Novellco de México S.A. de C.V.
1990

APUNTES SEMINARIO DE REDES LOCALES
Novellco de México S.A. de C.V.
1991

APUNTES INSTALACION Y MANEJO DE REDES
CON NETWARE DE NOVELL
Facultad de Ingeniería
División de Educación Continua
1990

NOVELL NETWARE
Ordenes e Instalación
Douglas Weber
Ed. Mc.Graw Hill
1991

SISTEMA OPERATIVO NETWARE 286
Nivel Usuario
Novellco de México S.A. de C.V.
1991

Apuntes Curso "Programación en redes"
ICM de México.

RED. LA REVISTA DE REDES DE COMPUTADORAS
Año 1, número 4
Año 1, número 5
Año 2, número 8
Año 2, número 9
Año 2, número 10
Año 2, número 11
Año 2, número 12
Año 2, número 15
Año 2, número 16
Año 3, número 17

REVISTA LAN TECHNOLOGY
The Technical Source for Network Integrators
February 1989
July 1989
September 1989
September 1990
June 1991

LAN, THE LOCAL AREA NETWORK MAGAZINE
November 1987
February 1991
April 1991
June 1991

PC COMPUTING
Revista
September 1990

PERSONAL COMPUTING
Revista
Año 3, número 31

PC/TIPS
Año 3, número 34
Año 3, número 35
Año 4, número 37
Año 4, número 41
Año 4, número 46
Año 4, número 47

PC MAGAZINE
Volume 9, number 1
Volume 9, number 21

PC MAGAZINE
En español
Volumen 1. número 1
Volumen 1. número 2
Volumen 1. número 5
Volumen 1. número 6
Volumen 1. número 7
Volumen 2. número 1
Volumen 2. número 2
Volumen 2. número 3
Volumen 2. número 7
Volumen 2. número 9
Volumen 2. número 11

SISTEMAS DE COMUNICACION
B.P. Lathi
Ed. Interamericana
1986