FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

DEPARTAMENTO DE CURSOS INSTITUCIONALES

INTRODUCCION A REDES LAN DE MICROS

PARTE I

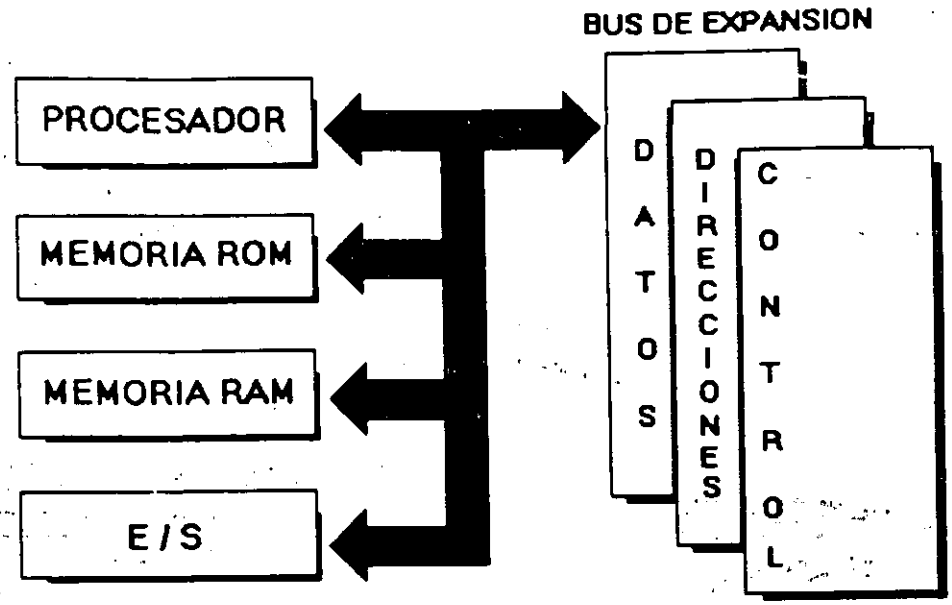
C O N A S U P O

21 - 26 Noviembre de 1994

Noviembre de 1994

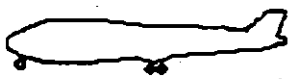
Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

Arquitectura General de la PC

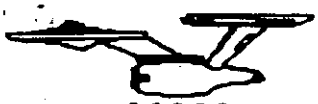


apuntes

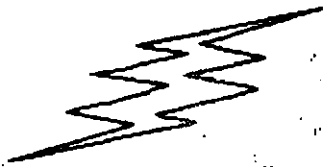
EL MICROPROCESADOR



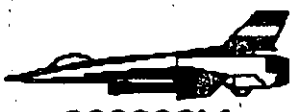
80286



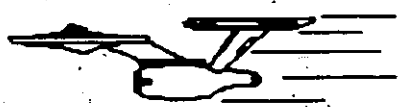
80386



80486



80386SX



80486SX

apuntes

Características de un Microprocesador

Un microprocesador es un circuito combinacional y secuencial que interactua con otros circuitos para formar en conjunto un sistema digital de cómputo.

Funciones Principales:

*Provee las señales de tiempo y control para todos los elementos del sistema.
*Busca instrucciones y datos desde la memoria.
*Transfiere datos desde y hacia Dispositivos de Entrada/Salida.
*Decodifica instrucciones.
*Realiza operaciones lógicas y aritméticas solicitadas através de instrucciones.
*Responde las señales de control de E/S, tales como RESET e INTERRUPT.

apuntes

NIVELES DE INTERRUPCION XT

N°	CAUSA
NMI	Error de Paridad
0	Contador
1	Teclado
2	Reservado
3	Comunicación / Puerto Serie (COM2), SDLC o BSC (Secundaria)
4	Comunicación / Puerto Paralelo (COM1), SDLC o BSC (Primaria)
5	Disco Duro
6	Puerto Paralelo

apuntes

NIVELES DE INTERRUPCION AT

N°	FUNCION
0	Timer del Sistema de salida 0
1	Salida del Teclado buffer lleno
2	Interrupción del controlador 2 (niveles 8-15)
3	Puerto Serial 2
4	Puerto Serial 1
5	Puerto Paralelo 2
6	Controlador de Discos
7	Puerto Paralelo 1
8	Reloj de Tiempo Real
9	Redireccionado vía Software a INT 0AH
10	Reservado
11	Reservado
12	Reservado
13	80287
14	Disco Duro
15	Reservado

apuntes

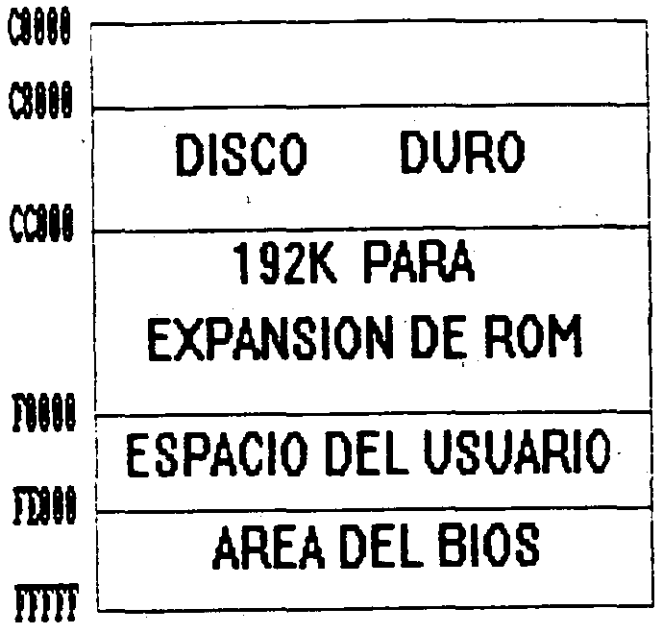
Memoria ROM (Read Only Memory)

Funciones Principales:

*Inicialización del Sistema.
*Diagnóstico de Encendido y Revisión del Sistema.
*Determinación de la Configuración del Sistema.
*Manejo de Dispositivos de E/S.- ***BIOS***
*Cargado del Sistema Operativo.
*Patrones de bits para los 1ros. 128 caracteres ASCII.

apuntes

Mapa de memoria XT (ROM)



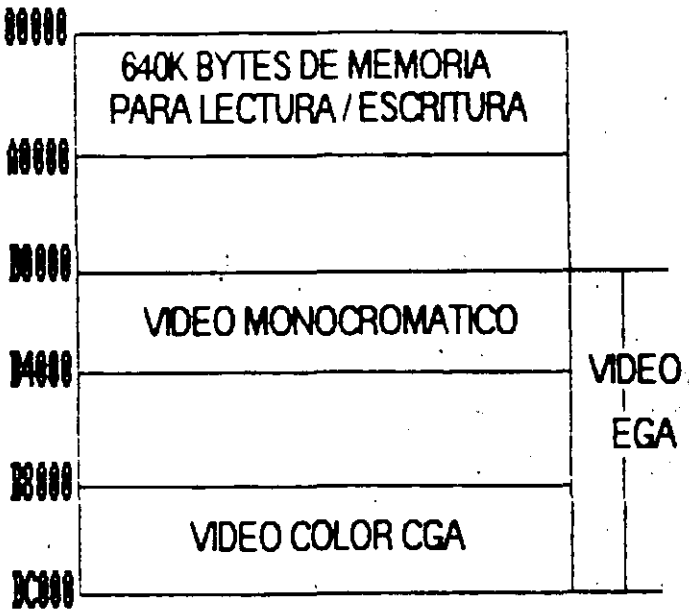
Memoria RAM (Random Access Memory)

Características Principales:

*Lectura / Escritura.
*Acceso Aleatorio.
*Espacio Disponible al Usuario y sus aplicaciones.
*Tamaño Limitado por el número de bits de direcciones del Microprocesador.
*Se direcciona através de un mapa de memoria predefinido.
*Tiempo de acceso de 150 a 80 nanosegundos.

apuntes

Mapa de memoria XT (RAM)



apuntes

Arquitectura de una computadora

D.1 I/O Address Map

Hex Range	Devices	Usage
000-01F	DMA Controller 1	System
020-03F	Interrupt controller 1	System
040-05F	Timer	System
060-06F	8042 (keyboard)	System
070-07F	Real time clock, NMI mask	System
080-09F	DMA page register	System
0A0-0BF	Interrupt controller 2	System
0C0-0DF	DMA controller 2	System
0F0	Clear math Coprocessor busy	System
0F1	Reset math coprocessor	System
0F8-0FF	Math coprocessor	System
1F0-1F8	Fixed disk	I/O
200-207	Game I/O	I/O
278-27F	Parallel printer port 2	I/O
2F8-2FF	Serial port 2	I/O
300-31F	Prototype card	I/O
360-36F	Reserved	I/O
378-37F	Parallel printer port 1	I/O
380-38F	SDLC, bisynchronous 2	I/O
3A0-3AF	Bisynchronous 1	I/O
3B0-3BF	Monochrome display and printer adapter	I/O
3C0-3CF	Reserved	I/O
3D0-3DF	Color/graphics monitor adapter	I/O
3F0-3F7	Diskette controller	I/O
3F8-3FF	Serial port 1	I/O

apuntes

Bus de Expansión

Funciones Principales:

*Conecta los componentes funcionales al Microprocesador.
*Está formado por: Bus de Datos
Bus de Direcciones
Bus de Control
*Además da las señales de:
Tiempo
IRQs
DMA

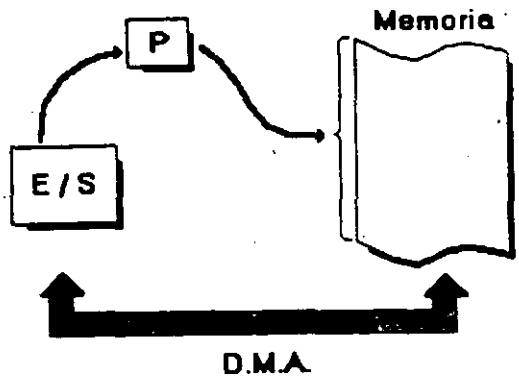
apuntes

Dispositivos Inteligentes

DMA (Direct Memory Access)

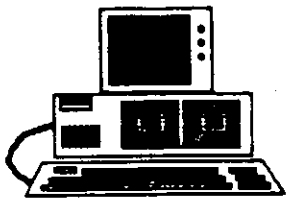
Ventajas:

*Velocidad en el Dispositivo.
*No "distrae" al Microprocesador.
*Transferencia de información rápida.



apuntes

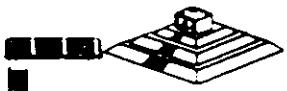
Especificaciones IBM Personal Computer



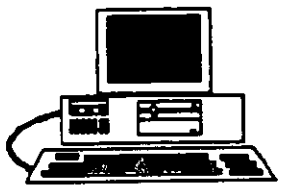
- Fuente de Poder de 63.5 Watts
- Microprocesador 8088 de 4.77 Mhz
- 5 Slots de Expansión (Con socket de 62 pins.)
- Memoria RAM base de 16K - 64K
- Bocina
- Unidad de Disco Flexible de 320K o 360K de 5¼
- Teclado de 83 teclas.

apuntes

Arquitectura de las Microcomputadoras



Especificaciones IBM Personal Computer XT



* Fuente de Poder de 130 Watts
* Microprocesador 8088 de 4.77 Mhz.
* 8 Slots de expansión (Con socket de 62 pins.)
* Memoria RAM base de 256K
* Disco Duro (En algunos modelos)
* Adaptador de Comunicaciones Asíncronas (En algunos modelos)
* Teclado de 83 teclas

apuntes

Microprocesador Intel 8086

*Velocidad de Reloj en MHz. 4.77 - 12
*Tamaño del Bus de Datos 16 / 16
*Tamaño del Bus
de Direcciones 20 ---> Memoria = 1MB
*Modos de Operación: Real

640 KBytes
Usuario

384 KBytes
Sistema

apuntes

Microprocesador Intel 8088

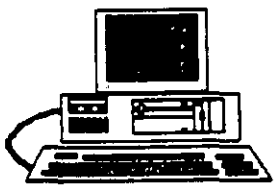
*Velocidad de Reloj en MHz. 4.77 - 12
*Tamaño del Bus de Datos 16 / 8
*Tamaño del Bus
de Direcciones 20 ---> Memoria = 1MB
*Modos de Operación: Real

640 KBytes
Usuario

384 KBytes
Sistema

apuntes

Especificaciones IBM Personal Computer AT



* Fuente de poder de 192 Watts switchable para 115 o 230 Vac
* Microprocesador 80286 de 6 Mhz.
* 8 Solts de expansión
  6 con 1 socket de 36 pins y 1 de 62 pins
  2 con 1 socket de 36 pins únicamente
* Memoria RAM base de 256K
* Memoria RAM de tipo Semiconductor Complementario de Oxidos Metálicos (CMOS) para mantener la configuración del setup del sistema.
* Bateria para mantenener activa la memoria CMOS cuando el equipo este apagado.
* Bocina
* Disco Duro
* Unidad de Disco Flexible de 5¼" de 1.2MB
* Seguro que inhibe cualquier entrada por el teclado
* Teclado de 84 teclas.

apuntes

Microprocesador Intel 80286

*Velocidad de Reloj en MHz. 6 - 20
*Tamaño del Bus de Datos 16 / 16
*Tamaño del Bus
de Direcciones 24 ---> Memoria = 16MB
*Modos de Operación: Real
Protegido

- 15 MBytes Usuario
- 1 MByte Sistema

apuntes

Microprocesador 80286

Modos de Operación 80286

Modo REAL

Se comporta como un: 

Modo PROTEGIDO

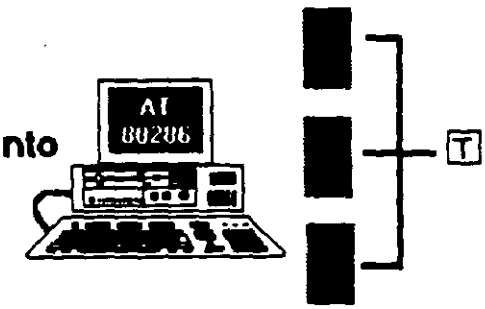
* 16 MB Memoria RAM
* Multitareas
* Multiprocesamiento
* Memoria Virtual

apuntes

Modo Protegido de Operación 80686

Multitareas

Multiprocesamiento



apuntes

Microprocesador Intel 80386/sx

*Velocidad de Reloj en MHz. 16 - 20
*Tamaño del Bus de Datos 32 / 16
*Tamaño del Bus
de Direcciones 32 ---> Memoria = 4GB
*Modos de Operación: Real
Protegido
Virtual

Limitante Tecnológica
(128 MBytes)Usuario

1 MByte
Sistema

apuntes

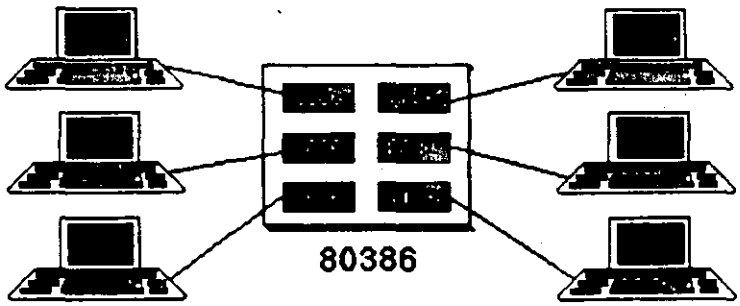
Microprocesador Intel 80386

*Velocidad de Reloj en MHz. 16 - 33
*Tamaño del Bus de Datos 32 / 32
*Tamaño del Bus de Direcciones 32 ---> Memoria = 4GB
*Modos de Operación: Real — 1 MByte
Protegido — Limitante Tecnológica (128 MBytes)Usuario
Virtual — Sistema

apuntes

Modos de Operación 80386

Modo Virtual 8086

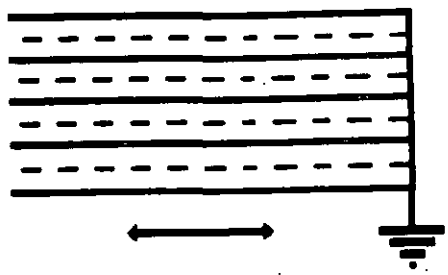


apuntes

Arquitectura 80386

Micro Channel IBM:

- "Nuevo Estándar....?"
- Canal Compartido.
- Alta Confiabilidad.
- Orientado a Multitareas y Multiprocesos.
- Utiliza e Implementa el POS.
- <u>No Compatible.</u>



apuntes

Arquitectura 80386

Smartslot AST Research:

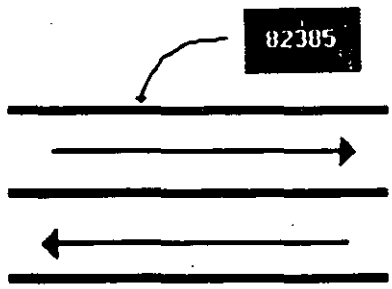
- *Enfoque Arquitectónico Intermedio.
- *Bus Arbitrado.
- *Procesador Múltiple.
- *Buena Velocidad.
- *No 100% Compatible.
- *Necesita Adeptos.

apuntes

Arquitectura 80386

Flex Compaq:

*Alta Velocidad.
*Compatibilidad.
*Canal Dual con
Procesador Adicional 82385.
* No Comparte Canal
Ni Memoria.



apuntes

E I S A

Miembros del consorcio *EISA*:

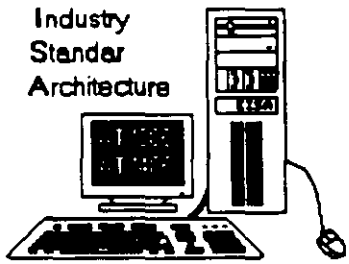
- *AST Research
- *Compaq
- *Hewllett Packard
- *NEC
- *Zenith Data Systems
- *Epson
- *Olivetti
- *Tandy
- *Wyse Technology

apuntes

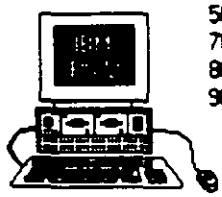
Tecnología de las Microcomputadoras

Industry
Standar
Architecture

Extended
Industry
Standar
Architecture



Micro
Channel
Adapter



Modelos:
50
50Z
50/386
70
80
90

apuntes

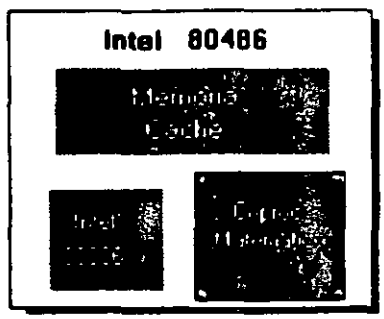
Caracteristicas Principales de las diversas Arquitecturas

CARACTERISTICA	MCA	EISA	ISA
Amplitud máxima de Datos	32 bits	32 bits	16 bits
Permite el uso de Periféricos Inteligentes y bus master de 32 bits	SI	SI	NO
Promedio máximo de Datos: DMA CPU	 20MB/seg 14MB/seg	 33MB/seg 16MB/seg	 2MB/seg 8MB/seg
Soporte para memoria direccionable	16MB	4GB	16MB
Compatibilidad	Ninguna	ISA	Ninguna

apuntes

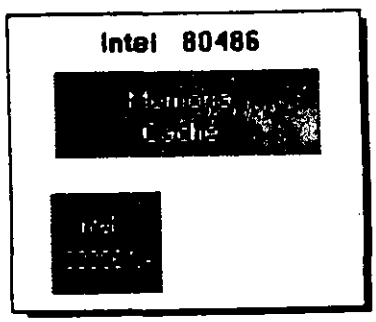
Microprocesador Intel 80486

*Características Similares al 80386
* Incluye Coprocesador Matemático
* Incluye Memoria Caché



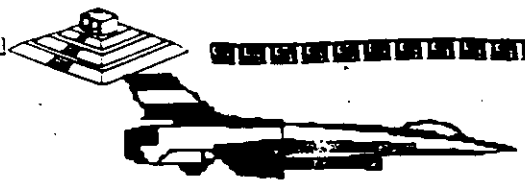
Microprocesador Intel 80486/sx

*Características Similares al 80386/sx
*Incluye Memoria Caché

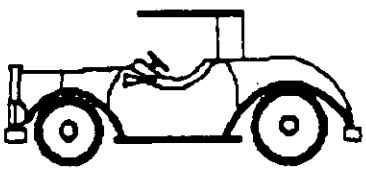


apuntes

LA MEMORIA



PROCESADOR



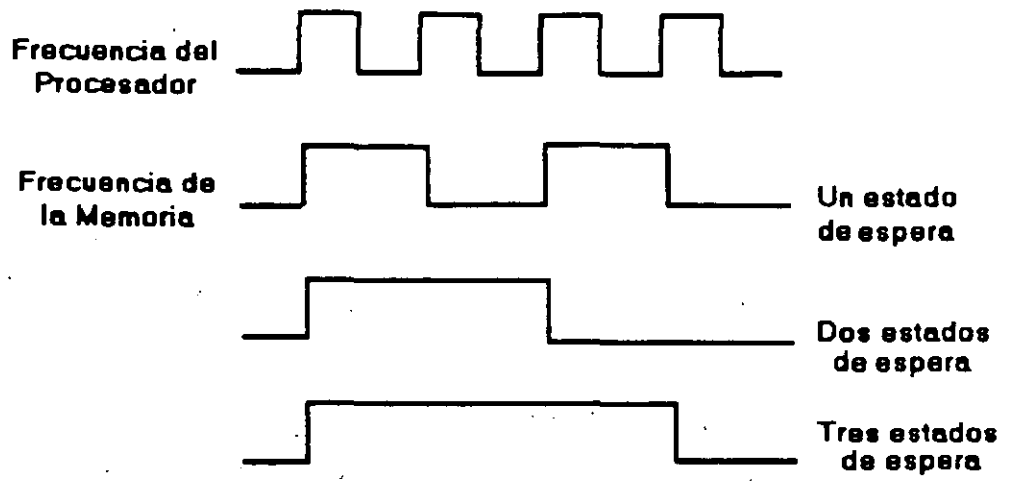
MEMORIA

ESTRATEGIAS

- Simple DRAMS
- Simple SRAMS
- Interleaved RAM
- Page Mode
- Caching

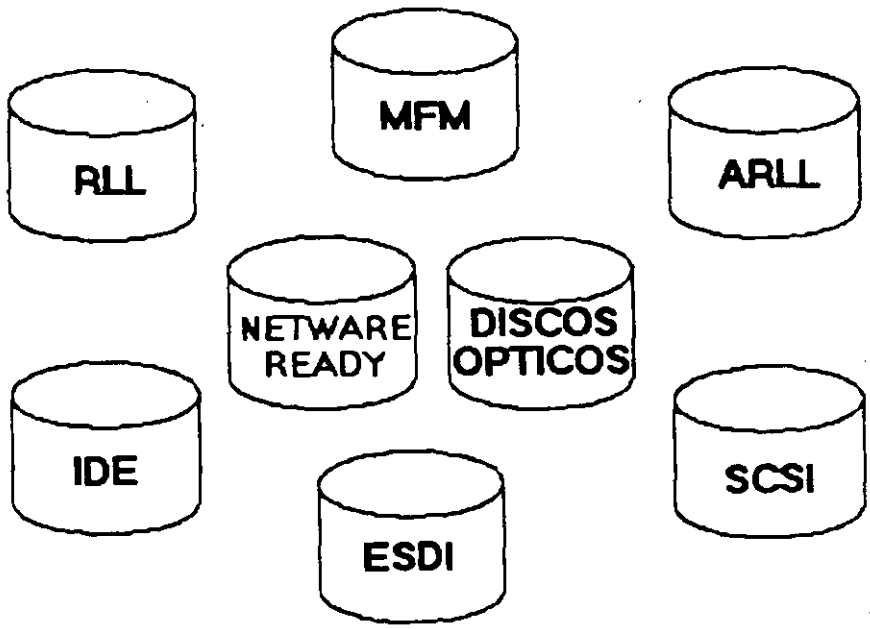
apuntes

Estados de Espera "Wait States"



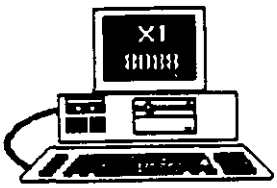
apuntes

TIPOS DE CONTROLADORES

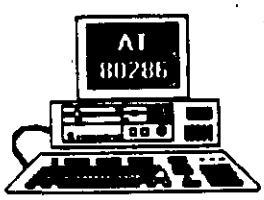


apuntes

Características de las Computadoras



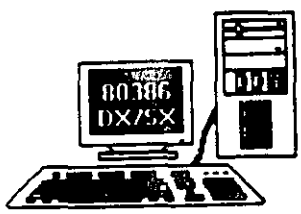
- Liberación México:1982
- Direccionamiento:1MB
- Memoria Usuario:640KB
- Almacenamiento:
  32MB (MS-DOS 2.xx)
  70MB (MS-DOS 3.xx)
  Tan grande como el disco duro (MS-DOS 4.xx y 5.xx)
- Velocidad:de 4.77 a 12 Mhz.
- Modo de operación:Real



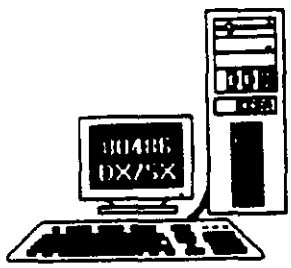
- Liberación México:1986
- Direccionamiento:16MB
- Memoria Usuario:15MB
- Almacenamiento:2GB
- Velocidad:de 8 a 20 Mhz.
- Modos de operación:Real y Protegido

apuntes

Características de las Computadoras



- Liberación México:1989
- Direccionamiento:4GB
- Memoria Usuario: Limitante Tecnológica (64MI
- Almacenamiento: en TB
- Velocidad: de 16 a 33 Mhz.



- Liberación México:1990
- Características: Similares al 80386
- Incluye Memoria Caché y Coprocesador Matemático
- Tecnología:RISC
- Velocidad: de 25 a 55 Mhz.

apuntes

INTRODUCCION A LAS REDES LOCALES DE MICROCOMPUTADORAS

PRESENTACION

Saber que la tecnología moderna tiene en la computación la más valiosa de las herramientas, ya no es noticioso, es tan común como el hecho de que todo el Orbe ha sido virtualmente invadido de microcomputadoras y más de las llamadas compatibles. Estos recursos bien aprovechados, indudablemente optimizan la productividad en todos los campos de las ciencias y del quehacer cotidiano del hombre.

La misma computación en su dinámica evolución, ha encontrado con las micros, una coyuntura más que ofrece mejores perspectivas al usuario. ¡**LAS REDES**!

La imperiosa necesidad de abatir costos en el manejo, transmisión e intercambio de información, ha encontrado en las **REDES** la respuesta positiva, ya que con ellas se comparten los recursos costosos, se actualiza y organiza la información tanto en empresas y organismos particulares, como en organismos oficiales, estatales, paraestatales; se logran enlaces remotos micro a **RED**, **RED** a mini, **RED** a macro, etc. Por ello es necesario que el usuario tenga un buen factor de realidad, de como aprovechar este recurso en la actualidad.

Congruente a esta panorámica, el curso estará apoyado en la tecnología actual a nivel internacional, dado a conocer Software de reciente liberación en Estados Unidos y Hardware nacional circulando ambos, en el mercado. Ya que en opinión de los observadores, a partir de 1988 las **REDES** empezaron a tener un gran auge en nuestro país , y para no ir a la zaga, es necesario estar actualizados.

OBJETIVOS

Proporcionar a los participantes el concepto de una **RED** y lograr que tengan unas bases confiables al decidir aprovecharla como herramienta moderna de la computación.

Abrir al usuario la puerta que les mostrará diferentes oportunidades para implementar una **RED**, con base en el más reciente Hardware y Software que hay en la actualidad, así como las espectativas reales de ambos.

Lograr que esta información sea el apoyo firme y seguro que permita al interesado dar los primeros pasos en el ambiente de **REDES**, ya que de ningún modo se pretende que este sea un manual formal, pues tal no existe, en virtud de que cada **RED** varía en función de los requerimientos del caso y del índice de crecimiento. Por ello, el manual necesario se tiene que ir implementando con base a los manuales oficiales de los productos (Hardware, Software y Conectividad) que se estén utilizando, a fin de dar mantenimiento a cada **RED**.

A QUIEN VA DIRIGIDO

A funcionarios y ejecutivos, a técnicos y a personas que por sus necesidades profesionales, requieran introducirse en el campo de las **REDES LOCALES**, aprovechando la oportunidad que ofrece esta herramienta de actualidad. Es conveniente que los participantes posean un buen nivel en microcomputación.

Para aquellos profesionales del medio que ya estén introducidos en este campo, se espera que tanto el material como el curso, sirvan para aclarar dudas y confirmar conceptos, a efecto de que incursionen con menos problemas en los cursos de constante actualización en **REDES LOCALES**, que posteriormente ofrecemos.

TEMARIO

1.- INTRODUCCION
- 1.1 Definición
- 1.2 Conceptos Básicos
- 1.3 Terminología
- 1.4 Componentes de una RED LOCAL

2.- TOPOLOGIAS Y PROTOCOLOS
- 2.1 Topología de Estrella
- 2.2 Topología de Bus
- 2.3 Topología de Anillo
- 2.4 Protocolos según Topologías
- 2.5 Sesión de Taller

3.- SISTEMAS OPERATIVOS Y HARDWARE PARA REDES
- 3.1 NetWare de Novell
- 3.2 LAN-Manager, IBM PC/LAN
- 3.3 Otros
- 3.4 Ponderación entre Sistemas Operativos
- 3.5 El Server sus características y funciones
- 3.6 Tipos de Tarjetas para RED.

4.- SOFTWARE PARA RED
- 4.1 El Problema del Acceso Concurrente
- 4.2 Manejadores de Bases de Datos y Lenguajes de 4ª Generación
- 4.3 Software de Paquetería
- 4.4 Software de Aplicaciones Verticales
- 4.5 Tendencias Actuales y Futuras
- 4.6 Sesión de Taller

5.- EL SUPERVISOR DE UNA RED
- 5.1 Instalación del Hardware
- 5.2 Instalación del Software
- 5.3 Niveles de Seguridad y Acceso
- 5.4 Mantenimiento de la RED
- 5.5 Interface con el Usuario
- 5.6 Sesión de Taller

6.- FUNDAMENTOS DE CONECTIVIDAD
- 6.1 Conceptos de Conectividad
- 6.2 Enlaces Remotos
- 6.3 *Puentes ó Bridges* (Conexión entre REDES)
- 6.4 *Gateways*(Conexión a Equipos Grandes)
- 6.5 Sesión de Taller

7.- CONCLUSIONES
- 7.1 Necesidad de la RED. ¿Cuándo?
- 7.2 ¿Cómo escoger la RED adecuada?
- 7.3 Características del Mercado Nacional

INTRODUCCION

1.1.) DEFINICION

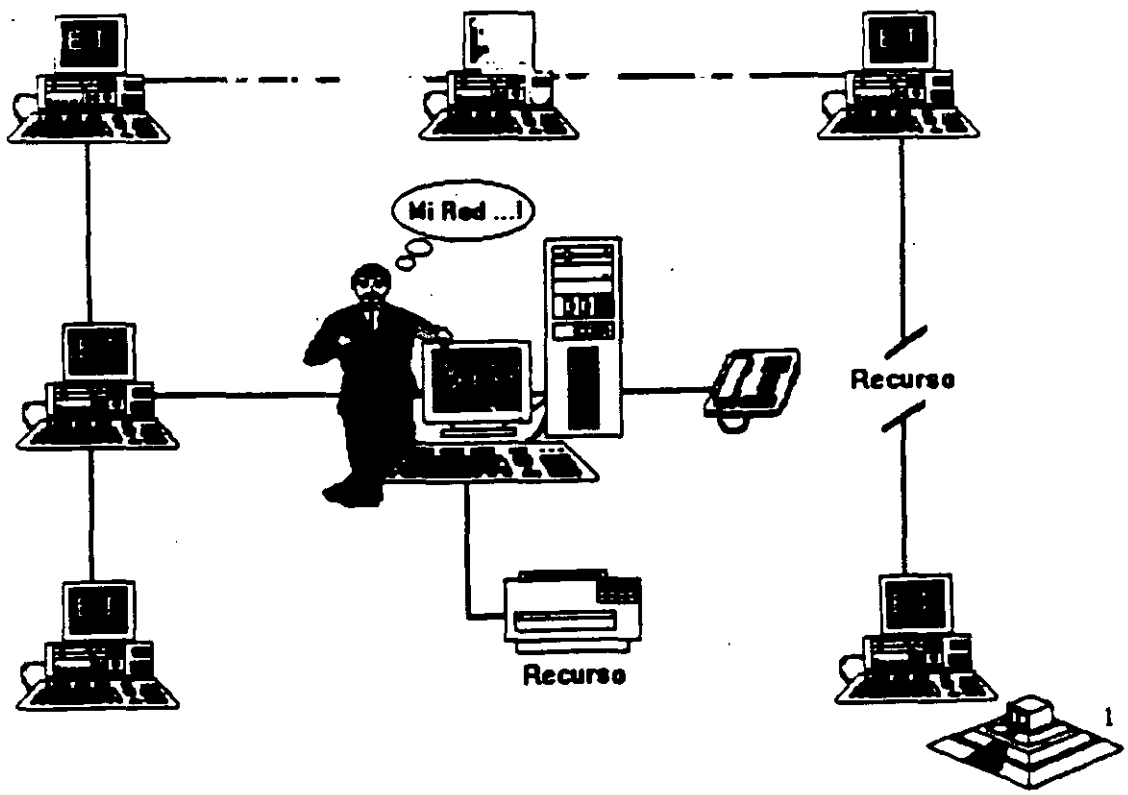
¿Qué es una RED ? : En el campo de la computación se puede decir que una **RED**, es un conjunto de computadoras enlazadas entre si y/o con otros equipos, cuya configuración permita que esto sea un medio para transmitir, recibir, compartir y manejar información.

1.2) CONCEPTOS BASICOS

¿Qué hace una RED ? : Una **RED** tiene como objetivo principal, compartir recursos materiales (equipos y sus periféricos) y recursos informáticos (archivos de datos y programas), actualizándolos, organizándolos y explorándolos.

¿Por qué una RED ? : Porque la **RED** es la respuesta correcta a la necesidad de compartir entre usuarios, los recursos más costosos del equipo y la información centralizada y/o dispersa de un organismo, obteniendo con esto, la tan necesaria organización y economía en la informática.

Sin mucha pretención, se puede aseverar que los tres puntos anteriores, vienen a ser el " A, B, C. " de las **REDES LOCALES**.




RECURSOS NORMALES DE UNA PC

Normalmente las microcomputadoras necesitan distintos recursos (periféricos), como son: impresores, graficadores, discos duros, unidades de respaldo en cinta magnética, programas de aplicación, paquetería, etc. que se tienen que adquirir a costos adicionales.

En una **RED**, estos recursos en una sola micro se van a compartir con las demás, mediante un canal de comunicación que por lo general, es un cable dedicado a las comunicaciones. Las micros se conectan a este canal por medio de una interface, que es una tarjeta electrónica que se coloca en una de las ranuras de expansión de cada micro.

La microcomputadora que cuenta con los recursos periféricos recibe el nombre de administrador de la **RED** o "server" que auxiliado por el sistema operativo de la **RED**, viene a ser virtualmente, el "cerebro" dedicado a administrar los recursos y las comunicaciones entre las demás micros, mismas que trabajando así, reciben el nombre de estaciones de trabajo.

1.3) COMPONENTES DE UNA RED LOCAL

Los componentes principales de una **RED** son:

I.- **El Server** que puede ser *DEDICADO* o *NO DEDICADO.*

- Cuando EL SERVER ES DEDICADO, exclusivamente administra los recursos de la **RED**.
- Cuando EL SERVER NO ES DEDICADO, además de administrar los recursos de la **RED**, funciona como Estación de Trabajo.

La PC que sea posible definir como SERVER, está en función de los requerimientos del caso, por lo que la tarjeta debe ser específica para esa **RED** y el sistema operativo, el adecuado.

II.- **Estaciones de Trabajo** que están representadas por cada una de las microcomputadoras conectadas en **RED**.

En la **RED**, tanto Servers como Estaciones de Trabajo, pueden ser PCs XT o PCs ATs equipos 386, 486, los modelos PS/2 de IBM e inclusive microcomputadoras no compatibles como es el caso de Macintosh.

En la actualidad se fabrica Hardware exprofeso para **REDES LOCALES** como es el caso de los Servidores y Estaciones de Trabajo de fábrica, con ventajas que posteriormente analizaremos. En el Mercado Nacional podemos encontrar fabricantes como *Micron, Acer, Digital Data,* etc., que ofrecen productos de estas características.

III.- **Tarjeta de Interface** que va instalada dentro de cada micro, y según su especificación, cada tarjeta determina, la forma de conexión **(Topología)** de cada **RED**. Existen tres tipos de tarjetas que denominan el mercado a nivel internacional:

ARCNET: Que tiene una relación costo-beneficio favorable, con un sistema de cableado sencillo y de amplio rango.

ETHERNET: La de mayor tradición, resulta ideal para conexiones Minicomputadoras-PCs. Por ejemplo: *Digital-Vax, HP-3000, NCR-TOWER*; etc.

TOKEN-RING: Muy costosa, pero con el respaldo técnico y promocional de IBM, esta tarjeta puede conectar toda la línea de equipos IBM, desde una PC hasta un *309X* ó *93XX* en una sóla **RED de este tipo.**

Sería importante recalcar que empresas mexicanas, como el caso de *Digital Data* y Micron, producen con tecnología propia tarjetas bajo estos tres estándares.

Para abundar en los datos de estas tarjetas ver el capítulo de Hardware y la sección de información anexa.

IV.- **Canal de Comunicación** que por lo general es un cable dedicado a las comunicaciones, mismo que puede ser:

a) De tipo telefónico.
b) De par roscado. (Twisted Pair).
c) C o a x i a l.
   Broadband - Lento, varios canales.
   Baseband - Rápido, un canal.
d) Fibra óptica - Más rápido y varios canales.

Este canal de comunicación determina la velocidad máxima de transferencia de información que va desde 2.5M bits/Seg ; hasta 100 Mbits/Seg., dependiendo del tipo de cable que se utiliza.

Actualmente se están desarrollando nuevas tecnologías para que el medio de comunicación sea inalámbrico.

A partir de 1990 *NCR* comercializa una **RED** de este tipo y en 1991 se empezaron a comercializar en Estados Unidos, **REDES LOCALES** con enlaces de Microondas, dedicados específicamente a la **RED.**

V.- **Repetidores**, que en algunos casos por la distancia entre unidades de la **RED**, son necesarios para reforzar la señal, sin importar la Topología; pueden ser tarjetas internas o cajas externas. Se dividen en activos y pasivos.

VI.- **Cajas de Conexión** que por lo general son siempre necesarias.

VII.- **Sistema de Cableado** cuya forma de conexión entre los equipos (TOPOLOGIA), está en función de la tarjeta que se haya seleccionado.

VIII.- **Sistema Operativo de RED** que entre otros, por su penetración en el Mercado Internacional , pueden ser:

- **NETWARE de Novell. En diferentes versiones.**
- **LAN MANAGER de Microsoft.**
- **Todos los NETBIOS compatibles.**
- **IBM PC NET también conocido como IBM PC/LAN.**
- **VINESS**
- **NETWORK - DOS.**
- **QNX de Quantum Software System Ltd.**
- **TAPESTRY.**

En Software, además del sistema operativo normal de los equipos (regularmente el MS-DOS), es necesario que se cuente con un sistema operativo para **RED** que lo auxilie o lo sustituya en el trabajo de compartir recursos.

Este sistema operativo permitirá explotar ampliamente los recursos del SERVER.

IX.- **Software de Aplicaciones** del cual se puede decir que también viene a ser componente de una **RED**. Por la existencia en versiones para RED, mencionaremos entre otros:

OPEN ACCESS III, FRAMEWORK III .- Paquetes integrados.
DBASE-IV ,DBASE III + , DB - XL ,
PARADOX, REVELATION,
DATAFLEX, ORACLE .- Manejadores de base de datos.
LOTUS 1-2-3, EXCEL .- Hojas de cálculo.
WORD, WORD PERFECT .- Procesadores de textos.
OFFICE WORKS, EL COORDINADOR .- Automatización oficinas, correo electrónico
WINDOWS 3.0 Y SUS APLICACIONES


COMPONENTES DE UNA RED
Microsoft
LAN
Manager
LAN
NOVELL
NetWare
LANtastic
LANtastic

1.4) TERMINOLOGIA

A efecto de estar familiarizados con los términos básicos que pueden resultar "no muy conocidos" para algunos de los participantes, se hacen los siguientes breves comerciales: En el medio, las **REDES LOCALES** también son llamadas **LANs (de Local Area Network)**, término que se menciona más por la asociación de ideas, que por el protocolo formal de una traducción del inglés.

De los vocablos **RED** y **LOCAL**, diremos que el primero se asocia a la conexión entre equipos de cómputo y el segundo, a la cercanía física entre éstos, que va de unos cuantos metros hasta unos cuantos kilómetros.-

Se sabe que a veces hasta 10 Km; distancia que ya más bien es un parámetro de enlace remoto.

Se habló al principio de las microcomputadoras compatibles, llamadas así por pretender ser "clonos" de las producidas hasta hace poco por la IBM. Los distintos fabricantes de las primeras, comercializaron sus equipos con la "etiqueta" de PCs/IBM, término que es muy familiar en el mundo de la computación.

También se mencionaron los términos **HARDWARE** y **SOFTWARE** cuyos significados son ya muy conocidos, no obstante, será saludable recordar que *Hardware* implica todo aquello que es electrónica física (como la propia C.P.U; con sus circuitos integrados, conductores, drives, discos, periféricos, cableado, etc.), y que *Software* implica todo aquello que sean programas (como sistemas operativos, programas de aplicación, paquetería etc.).

Otro término que se ha mencionado, y que es necesario conocer bien, es la palabra **TOPOLOGIA.**

Entre los matemáticos que estudiaron esta disciplina, está **A. Listing** quien le dió el nombre y la **definió como la parte de las Matemáticas que estudia la disposición de agrupaciones de elementos.**

Por lo tanto en el ambiente de **REDES**, y en congruencia con la definición anterior, en adelante, se entenderá simplemente que: **TOPOLOGIA**, es la forma en que están conectados el grupo de elementos que conforman una **RED.**

Para no abundar innecesariamente en la terminología, sobre la marcha se irán definiendo los conceptos que vayan requiriendo aclararse según el tema además, en el momento que no se entienda un término se podrá consultar el glosario anexo al final de estas notas.

TOPOLOGIAS Y PROTOCOLOS

Para Protocolo, simplemente se adoptará la definición que por extensión se da a este término, es decir, la aceptación de Regla, aplicada a las comunicaciones.

En **REDES LOCALES**, prácticamente existen tres tipos básicos de Topologías, a saber:

- **Estrella**
- **Bus**
- **Anillo**

Se puede sumar a estos tipos básicos la topología de **Arbol** que es una conexión compuesta . Para el estudio de la Topología se deben de considerar dos tipos:

- **Física**
- **Lógica**

La *Topología Física* es determinada por la disposición de los elementos conectados a la **RED**. La *Topología Lógica* la determina el Protocolo de Comunicación operando en la **RED**, no importando la disposición física de los elementos; en otros términos, se puede implementar un anillo lógico en un bus físico.

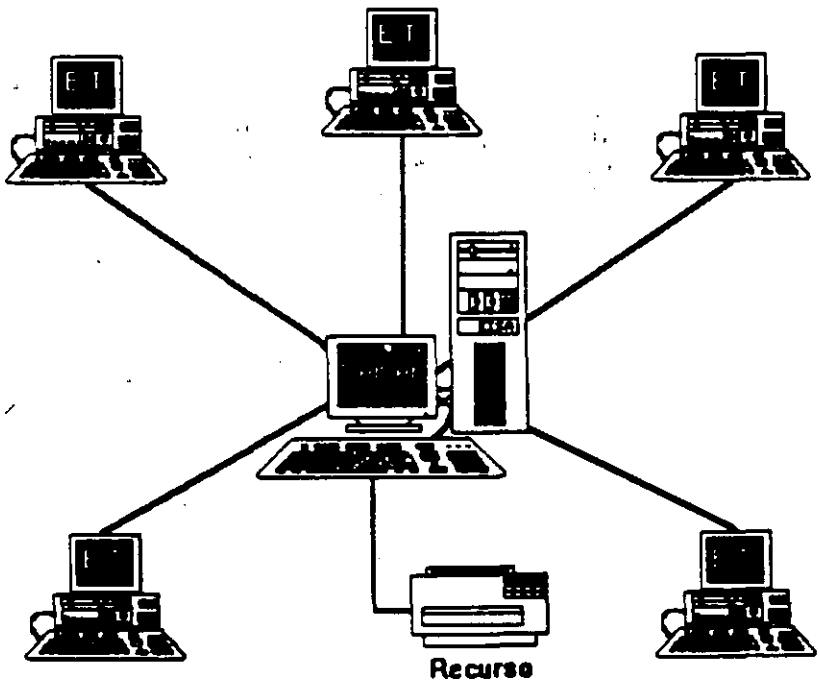
En el mercado actual existen una gran variedad de Topologías Físicas, para entender como funcionan todas estas, es importante conocer como funcionan lógica y físicamente los tipos básicos antes mencionados; sobre todo su Protocolo de Comunicación, para que se puedan entender y conocer las características de cualquier topología que el mercado pueda ofrecer.

2.1.- TOPOLOGIA DE ESTRELLA

En este tipo de conexión, el elemento central es el **SERVER CON SUS PERIFERICOS**. Se mantiene preguntando constantemente a cada estación de trabajo mediante comunicación exclusiva y por turno, si desea transmitir información; de ser afirmativo, la atiende y al terminar, prosigue con otra su interrogatoria permanente.

Para este caso de preguntas-respuesta-pregunta a la siguiente etc; a la regla de comunicación se le conoce como Protocolo **POLLING** (poleo), empleada en las "minis".

En el despertar de la **REDES**, esta topología fue la que se utilizó primero, pero resultaba una de las más caras.

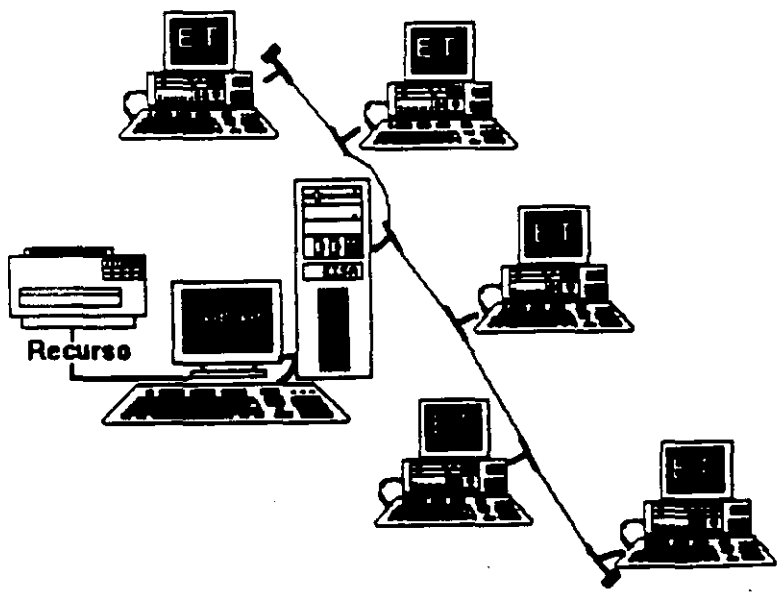


2.2.- TOPOLOGIA DE BUS

Esta conexión se considera que es la más sencilla de todas, donde las micros incluyendo al SERVER, están enlazadas por un solo cable (coaxial o par roscado), y la información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones.

Por ello el Protocolo apropiado es **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection).

Con este protocolo la **RED** transmite y espera a que se le confirme que la información fue recibida correctamente, de otra forma, detecta la posible colisión, espera un tiempo a que el canal esté desocupado y la información se transmite nuevamente.

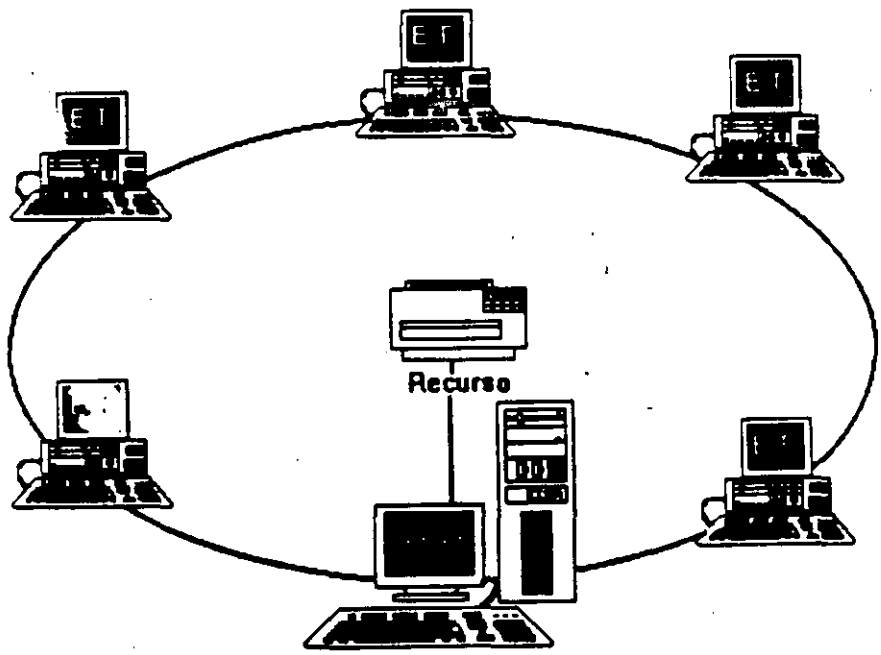


2.3.- TOPOLOGIA DE ANILLO

En esta conexión la información viaja ordenadamente en un solo sentido a través de un solo cable, describiendo un ángulo de 360° en cuyo anillo imaginario, están conectadas en serie las estaciones de trabajo y el SERVER.

Una señal llamada **TOKEN** (Receptáculo, a modo de estafeta), va circulando por la **RED** y pasando por cada estación, si la primera resultó ser la solicitante, previa identificación entrega la información, de lo contrario la deposita en "sobre cerrado", para que esta a su vez así la envíe a la siguiente, llevando consigna de entregarla hasta identificar a la solicitante.

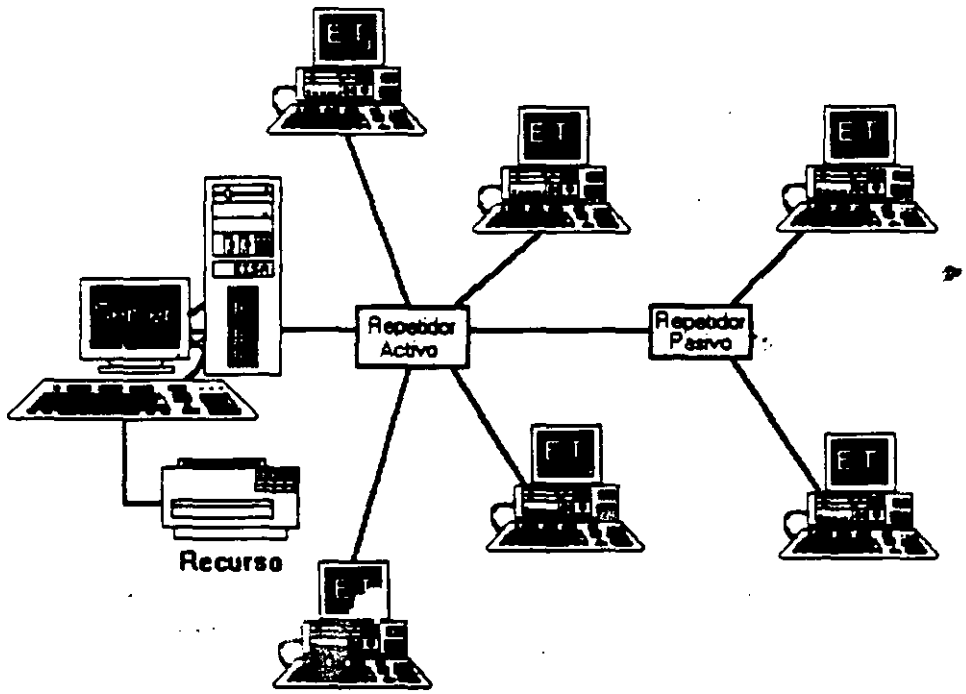
Cada estación de paso, cuando más, colecta información adicional enviándola a la siguiente y así se la pasa la señal cerrando ciclos "circulares"; por ello el protocolo apropiado para este caso se conoce como **TOKEN PASSING**.



2.4.- TOPOLOGIA DE ARBOL

Esta conexión como se dijo anteriormente, es combinada y es una opción más para implementar **REDES**, según las necesidades del usuario.

Normalmente trabaja con el Protocolo **TOKEN PASSING**, tarjeta **ARCNET** y repetidores tanto **PASIVOS** como **ACTIVOS**.



3.4 PONDERACION ENTRE SISTEMAS OPERATIVOS

En esta sección se analizarán los pros y contras de los sistemas operativos más comunes, **IBM-PC LAN** , **NetWare de Novell** y **LAN-Manager**, con el objetivo de que se tengan elementos de juicio para poder elegir la mejor opción.

Es necesario aclarar que en cuanto a **REDES** no se puede decir que un producto es mejor que otro, sino que esto depende de las necesidades particulares de cada caso, algunas veces la Opción puede ser *NetWare de Novell* y en otras *IBM* o *LAN-Manager* , o algún otro producto de los que ya se han mencionado insistimos todo depende de cada caso.

Al finalizar se darán algunas conclusiones al respecto y el tema será ampliando en el último capítulo en la sección de Como escoger una **RED**.

IBM-PC/LAN : Pros y Contras

Las principales ventajas son:

* Es un sistema sencillo de operar e instalar (aproximadamente 15 minutos).

* Todos los comandos de la **RED** pueden estar dados a través de menús (*MS-NET* no contiene esta característica), con la posibilidad de grabar un batch para ejecutar los comandos dados a través de los menús.

* Posee un sistema básico de mensajes en línea, de manera que puede enviar avisos a otros usuarios, declarando para ello el nombre de la estación.

* A diferencia de *MS-NET*, no se necesita que sean declarados en una lista todos los usuarios que puedan accesar la **RED**, ni su dirección asociada. De manera que cualquier usuario puede entrar en la **RED**.

* La declaración de recursos a compartir es muy simple.

* Utiliza el estandar *NET-BIOS*, por lo que casi todo el Software para **RED** funcionará sin problemas bajo este sistema operativo.

Principales desventajas:

* La seguridad de la **RED** es muy pobre, un usuario que se ponga a trabajar en el server puede formatear el disco duro sin ningún problema.

* No se tienen registros de usuarios autorizados, no se tiene un control de las entradas y salidas ni de la contabilidad de la RED.

* El acceso inicial a la **RED** es muy lento. Por su forma de manejo, cuando un usuario entra, se tiene que verificar NODO por NODO. que su nombre no exista en otra estación. Esto toma varios segundos (de 30 a 45) dependiendo.

* A pesar de las mejoras en la versión 1.2, el rendimiento de la **RED** decae fuertemente después de cuatro usuarios, de forma que **REDES** de seis o siete usuarios son el límite adecuado con carga normal de trabajo.

* Bajo cargas muy fuertes y dependiendo del Hardware puede ser que con sólo 4 NODOS, en rendimiento ya sea muy deficiente y por lo contrario con cargas ligeras tener más de 8 usuarios trabajando sin ningún problema.

* Por lo que respecta a la conectividad, sobre todo con equipos grandes y el establecimiento de puentes (debido al protocolo que se utiliza) es un producto muy escaso de recursos, ciertos productos como los *Gateways* no funcionan.

Novell Advanced NetWare : Pros y Contras

Principales Ventajas.

* Rendimiento (Performance) muy superior a los demás. Para **REDES** de más de 8 usuarios: 20 a 50 o más, creemos que la única alternativa viable es la de *NetWare de Novell* .

* Existen versiones especiales para servers tanto AT/286 como AT/386, la ventaja es que trabajan en el modo protegido del procesador.

* El sistema de seguridad es completo y eficiente, se fijan seguridades de acuerdo a los usuarios, grupos de usuarios y los directorios.

* El Supervisor de la **RED** es el único que puede determinar estos niveles de acceso y seguridad.

* El Supervisor de la **RED** puede definir entradas personalizadas para cada usuario.

* Se pueden definir menús para accesar a la **RED** ó utilizar comandos de ésta.

• Facilidades de Enlaces y Comunicaciones: Poder para hacer *Puenteos, Gateways, Enlaces Remotos* de un Nodo a la **RED**, enlace de una **RED** remota a otra etc.

• Es posible instalar el emulador de *NETBIOS*, si así lo requiere el Software de **RED**.

Principales Desventajas:

• Se requiere una mayor preparación técnica por parte de los usuarios, sobre todo del Supervisor de la **RED**.

• Instalación tardada: Una adecuada instalación de *NetWare* requiere de casi 24 Hrs (muchas de las cuales el server sólo está verificando pistas del disco duro, por lo que no es necesario cuidarlo), y cuando se trata de instalar puentes locales o remotos, hay que invertir tiempo en leer cuidadosamente los manuales.

• En el sistema de mensajes, los usuarios dejan mucho que desear ya que lo supera el de IBM.

• Costo elevado: NetWare es un producto costoso que se justifica si la **RED** es más grande, o sí se requieren altas seguridades para el acceso de usuarios a la información.

Pero este problema empieza a tener solución con la aparición de las nuevas versiones *ELS*, la cual su precio es muy competitivo, incluso con el propio *IBM-PC/LAN*.

En el caso de *LAN-Manager*, la principal desventaja es el alto consumo de recursos , tanto memoria como discos duros

Conclusiones

Reiteramos que tanto el Software como el Hardware a escoger para la instalación de una **RED**, depende en primera instancia de las necesidades particulares de cada caso, pero en términos generales se podrían hacer las siguientes recomendaciones:

Si la **RED** es de más de 8 nodos, o se desea crecer a un corto o mediano plazo, o sí es necesaria una seguridad muy alta en la **RED** , la mejor alternativa por el momento es *NetWare de Novell*, buscando la versión que sea la más adecuada. Si la **RED** es de 2 a 6 nodos y no se requiere de mucha seguridad en cuanto al manejo de la información y no se necesita hacer ningún tipo de aplicación "esotérica" como hacer enlaces a otras **REDES**, o cosas similares, entonces **IBM-PC/LAN** puede ser la mejor alternativa, pero hay que considerar las nuevas versiones **Lite de NetWare** , o versiones como **LAN-Tastic** que también esta penetrando fuertemente en el mercado nacional.

Si se cuenta con un Hardware poderoso (AT's 286, 386, 486, más allá de los 4MB de memoria, monitores VGA y Disco Duro rápido), **LAN-Manager** puede ser considerado como una buena opción , orientado a aplicaciones muy fuertes; teniendo conectividad hacia equipos IBM y ambientes UNIX.

No se deben soslayar otras alternativas que existen en el mercado nacional, pero que no tienen el poder de penetración de **Microsoft, IBM** o de **Novell**, lo mejor es estar bien informado y orientado. Estamos ciertos que estás notas coadyuvarán a tal fin.

3.5 HARDWARE PARA REDES LOCALES

En esta parte veremos los elementos principales en Hardware para una **RED LOCAL**:

- Sistema de Cableado.
- Tarjetas de **RED**.
- Servers.

En la parte de sistemas de cableado, hablaremos particularmente de Fibra Óptica, y en el caso de las tarjetas de **RED**, sólo analizaremos los tres estándares en el mercado; Arcnet, Ethernet y Token Ring. Lo relativo a los servers, lo describiremos en la sección de tendencias.

Sistemas de Cableado

Existen básicamente tres tipos de cableado:

- Par torcido o par roscado, (twisted pair)
- Coaxial.
- Fibra Optica.

En general, el orden en que están expuestos respeta sus características ascendentes en cuanto a:

- Velocidad de transmisión que permiten distancias máximas.
- Precio.
- Dificultad en Instalación.

En los últimos años, con la popularidad de Arcnet y Ethernet, el cable coaxial ha sido el más usuado. Sin embargo en los últimos meses, han aparecido modificaciones en Arcnet y Ethernet que utilizan twisted pair, por lo que algunos expertos le auguran un futuro muy promisorio al twisted pair.

Si bien el Twisted Pair normal es más barato que el coaxial, hay que tener en cuenta que cuando éste es habilitado, su precio es muy superior al coaxial.

La mayor ventaja que podría tener el Twisted Pair, es aprovechar en cierto tipo de **REDES LOCALES**, el cable que ya se encuentra tendido a través de las oficinas.

Pero en México, sinceramente, el aprovechar esa característica se ve realmente difícil. Por otra parte, la ventaja de la Fibra Optica en cuanto a mayores velocidades, en general no se utiliza hoy en día, por los dispositivos con los que se cuenta.

Por ejemplo, si instalamos fibra óptica para una **RED Arcnet**, la velocidad a la que transmitiremos seguirá siendo 2.5 Mbits/seg; y no 100 ó 200 Mbits/seg; que son velocidades a las que se pueden transmitir en la fibra óptica.

También en este renglón, cabe hacer notar, que el equipo necesario para la instalación de la fibra óptica cuesta alrededor de $20,000 dólares, por lo que lo hace de momento incosteable dadas las características económicas prevalecientes en el país.

De particular interés es el sistema de cableado de Token Ring, que utiliza varios tipos de cable: Twisted Pair de diferentes tipos: además, de existir versiones para utilizar fibra óptica.

Ethernet

Ethernet surge como el primer esfuerzo real hacia las **REDES LOCALES** de computadoras. Nace en la década de los 70's, del laboratorio de investigación de Xerox Corp. en Palo Alto California, mejor conocido como Xerox-PARC y su principal diseñador es Mentcalfe, actual presidente de 3Com. Corp.

El nombre de Ethernet proviene de que, basados en las experiencias con Aloha Net (**RED** de propósitos académicos, instalada en Hawai que usaba como medio de propagación el aire, a través de ondas RF), el diseño de Ethernet se sustentaba en un bus general, que unía a todos los elementos, por analogía con el "Eter" de los antiguos griegos, que era la substancia que unía todas las cosas (el sol con la tierra y los demás planetas así como los cuerpos entre sí) por lo que se le denominó ETHERNET.

Resumen de Características Técnicas

Ethernet trabaja con el protocolo CSMA/CD (Carrier Sense Multiple Acces/Collision Detection), a velocidades de 10 Mbits/seg, con lo cual hace que en general posea características de rendimiento muy particulares:

- La velocidad de transmisión (10 Mbits/seg) es excelente.

- Sin embargo, en cuanto crece la **RED**, dicha velocidad se nivela con la desventaja que representa el método CSMA, al tener que manejar más colisiones en el canal.

Lo anterior hace que para REDES de pocos nodos, Ethernet tenga un rendimiento estupendo. El cableado y las longitudes máximas de Ethernet, no están estandarizadas como se podría pensar.

El cableado típico de Ethernet, utiliza un cable coaxial especial, con doble blindaje, que entre otras cosas es sumamente costoso, además de que dicho cable sólo sirve para instalar dispositivos en Ethernet, (es decir el cable es Ethernet). Bajo Thin-Ethernet o Cheapernet, las distancias por segmento son menores (entre 200 y 300 mts; dependiendo de la tarjeta de RED que se use) y el enlace no es a base de transceivers sino formando una cadena (daisy chain); para formarla, se colocan conectores "T" en el cable coaxial, que en este caso es un cable significativamente más económico, con blindaje estandar de cable coaxial, y con una impedancia de 50 ohms.

¿Por qué es importante ETHERNET?

Existen pocas razones para que Ethernet pueda ser considerada en un proyecto de RED LOCAL, pero algunas de estas son de mucho peso, e incluso en ciertas ocasiones definen como única alternativa a Ethernet.

1) ETHERNET es un Estandar

Tanto por ser una con varios años de desarrollo, como por formar parte de los 3 estándares de Hardware fijados hasta ahora por el *IEEE*, Ethernet asegura un camino de permanencia en el mercado. (ver sección de conectividad para mayores detalles).

2) Garantiza Conectividad hacia otros Ambientes

En este punto, Ethernet es hoy en día, el estandar en tarjetas de RED LOCAL que permite las conexiones más amplias entre equipos de diferente naturaleza.

De hecho la mayoría de las minicomputadoras (*Digital/VAX, NCR-Tower, Tandem, ALTOS, UNISYS/5000* y *7000*, etc); tienen la capacidad de enlazarse vía Ethernet, y normalmente es el único Hardware de RED que soportan. Algunas características de estos enlaces se verán con más detalle en la sección de conectividad, particularmente al hablar del protocolo *TCP/IP*.

3) Excelente Rendimiento con Pocos Nodos

Cuando se desea lograr una alta velocidad entre los nodos de la RED, y estos no son muchos (posiblemente entre 10 y 20), podemos confiar en que con Ethernet tendremos velocidades efectivas en el canal, muy altas.

En las oficinas de Novell Inc. en Utah EUA, se decidió que la RED que se usaría para enlazar veintitantos servers, sería Ethernet; logrando con esto, tener una RED en la que los nodos (en este caso solamente servers, que a su vez atienden sus propias **REDES LOCALES**) "platicarían" pocas veces, pero de mucha información cada vez. La decisión fué que Ethernet era la mejor solución.

4) Tradición

Desde el punto de vista puramente técnico no tiene ningún valor de observación, pero nuestra experiencia en el campo nos indica que en algunos casos, los usuarios en ocasiones, prefieren soluciones más conocidas y probadas, o por lo menos más oídas y vistas en folletos y libros.

Principales Fabricantes

En el mercado americano, existen 4 fabricantes importantes que utilizan Ethernet como su plataforma de conectividad:

- 3 Com Corp.
- Ungermann-Bass (también conocido como U-B).
- Microm-Interlan.
- Excelan.

De entre los productos de estos 4 fabricantes , existen una gran variedad de tarjetas Ethernet, unas inteligentes y otros no, unas con el bus general de PC (8 bits), otras con el bus aumentado de la AT (16 bits), y con tarjetas equivalentes para enlazarse a minis o super-minis, así como el Software necesario para hacerlo.

Básicamente las tarjetas inteligentes, tienen un procesador más poderoso (por ejemplo 80186) que brinda un manejo de paquetes y buffers más ágil, esto combinado con un server que posea una tarjeta con un bus AT, logrará un rendimiento más adecuado.

En últimas fechas, Novell mismo liberó una tarjeta Ethernet económica, al igual que Western Digital. Y aquí en México, durante el mes de noviembre, Computadoras Micron liberá su tarjeta Ethernet.

Una noticia importante que ha empezado a comentarse en las revistas, y que se ve reflejada en algunos folletos publicitarios, son los recientes anuncios de IBM de soportar Ethernet en algunos equipos suyos.

Para mencionar 2 ambientes diferentes:

En un desarrollo conjunto con U-B, anunció la liberación de una tarjeta Ethernet para los equipos PS/2. Por otra parte en la información técnica de sus nuevos minis-mainframes 9370s, explica el soporte que se dará a Ethernet (802.3) y al estandar 802.2.

Lo anterior hace que Ethernet se sitúe como un estandar sólido, sobre todo en cuanto a conectividad con minicomputadoras. Y como un futuro competidor de la misma Token-Ring, aún en el área de equipos IBM mayores.

Arcnet

Una de las REDES más populares en Estados Unidos y en el mundo, es ARCNET: Attached Resource Computer Network, desarrollada por Datapoint Corp; inicialmente la RED y el protocolo eran del fabricante, pero el protocolo del nivel de Data Link, las especificaciones de interface y aún los circuitos integrados, fueron hechos públicos a partir de 1982.

Funcionalmente, ARCNET es una RED de tipo Token-Passing bus, similar a lo especificado en el documento IEEE 802.4, pero en su topología forma realmente un árbol utilizando un sistema de cableado a base de repetidores activos y pasivos.

Nivel Físico

ARCNET interconecta los repetidores con las tarjetas (*NICs*) usando cable coaxial RG62 (93 ohms), con transmisiones "baseband" a 2.5 Mbps.

La longitud máxima entre nodos es de 6 km, y entre repetidores activos, o entre repetidor activo y PC es de 600 mts.

Regularmente los repetidores activos poseen 8 puertos, y los pasivos sólo 4. Mientras el activo amplifica la señal a sus niveles óptimos, el pasivo sólo divide la señal (técnicamente hace un acoplamiento de impedancias, a través de un sencillo circuito de 4 resistencias).

Protocolo de Nivel 2

Arcnet emplea 5 formatos de mensaje, los primeros cuatro formatos son usados para mensajes de control, mientras el quinto es para llevar datos entre las estaciones.

Todos los campos de dirección consisten de 8 bits, lo cual restringe el número de estaciones a 255 (la dirección o se reserva para mensajes generales: broadcast a todas las estaciones), la dirección destino (*DID*) está duplicada con cada mensaje para protección de errores.

Cuando una tarjeta recibe el Token (mensaje tipo 1) con la dirección apropiada, elige entre dos caminos dependiendo si tiene o no transmisión que hacer. Si tiene datos para transmitir, la misma tarjeta envía una requisición de buffer-libre (mensaje tipo 2) a la tarjeta destino, preguntando con esto si está lista para recibir. La tarjeta destino responde con un *ACK* (tipo 3) si tiene espacio de buffers disponible, o con un NAK (tipo 4) si no lo tiene.

Después que la tarjeta ha transmitido sus datos, o cuando determina que no tiene datos por enviar, pasa el Token a la estación con la dirección mayor siguiente. Después de enviar el mensaje tipo 1, los mensajes 2 ó 5 indican que el Token es aceptado, y si no hay repuesta en el lapso de 74 microsegundos implica que la estación deseada está fuera de líneas y el Token debe ser pasado a la estación cuya dirección es la siguiente.

Servers

Para la selección de un Servidor adecuado, siempre hay que tener en cuenta los siguientes parámetros, mismos que se comentarán a lo largo de la exposición:

- Marca y modelo.
- Marca del BIOS (por aquello de la compatibilidad).
- Procesador y Frecuencia de Operación.
- Velocidad de memoria y estados de espera.
- Tamaño de la memoria principal.
- Escalabilidad
- Compatibilidad con el S.O. de **RED** que se usará (fundamental).
- Capacidad del disco duro.
- Cuantos discos duros acepta.
- Tiempo de acceso promedio del disco duro.
- Marca del disco duro (ojo con marcas raras).
- Velocidad de transferencia entre disco duro y memoria

EL SOFTWARE PARA LA RED

EL SOFTWARE PARA LA RED

En este capítulo se analizará el problema a resolver dentro del desarrollo de Software en un ambiente de **REDES**, la actualización simultánea por más de un usuario del mismo archivo o grupo de archivos, se comentarán algunas soluciones al respecto y las necesidades dentro de su implementación.

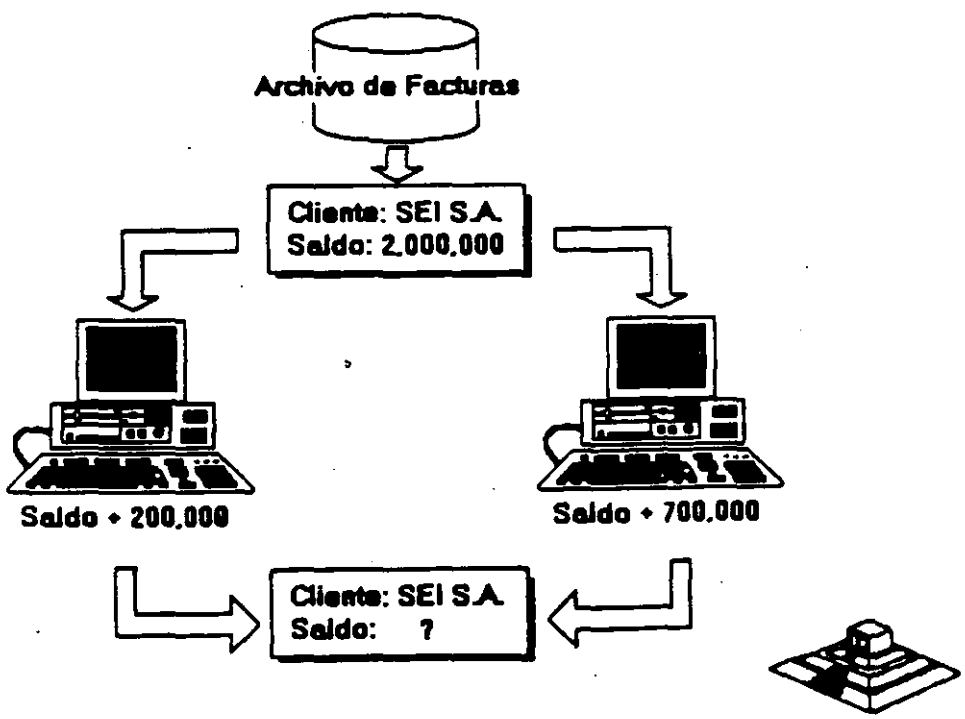
Se revisarán algunos paquetes comerciales que ofrecen versiones para su uso en **RED**. En este punto se incluirá la traducción del Software en **REDES**. Al final se comentará qué se espera en el mercado de Software en los próximos años.

4.1 EL PROBLEMA DEL ACCESO CONCURRENTE

En una **RED LOCAL**, donde pueden existir 3, 10, 50 ó más usuarios, es muy probable que dos o más de estos usuarios quieran o tengan que usar un mismo programa a la vez, posiblemente con los mismos archivos. Lo anterior trae como consecuencia un problema para mantener la "consistencia" de la información.

Supóngase el caso de la figura 4.1, en el que se tienen 2 capturistas trabajando el sistema de facturas, ambas se encuentran utilizando los mismos archivos, clientes, inventario, etc. Por casualidad una de ellas empieza a capturar una factura de una determinada compañía, a nivel de Ejemplo: SEI, S.A. Mientras su compañera está capturando otra factura de la misma Industria.

ACCESO CONCURRENTE



Para este caso el programa de facturas realiza las siguientes tareas:

1.- Leer los datos del cliente (incluyendo saldo).

2.- Permitir la captura de la factura.

3.- Calcular el TOTAL de la factura.

4.- Calcular el NUEVO SALDO del cliente.

(NUEVO SALDO = TOTAL DE FACTURAS + SALDO)

5.- Grabar NUEVO SALDO y otros datos.

Observe que entre leer datos (paso 1) y grabar datos (paso 5) suceden algunas tareas tales como el capturar la factura.

Si los procesos de los dos capturistas se realizan simultáneamente se llega a un estado INVALIDO o INSOLENTE del archivo.

Ya sea que el proceso se "vaya" por un capturista o por el otro, el saldo nuevo será incorrecto, se grabará un saldo de $2,700,000 ó $2,300,000 en lugar de $3,000,000 que sería lo correcto.

Hasta aquí debe quedar claro que, a diferencia de una aplicación clásica para una computadora personal en la cual, SOLO UNA PERSONA actualiza los archivos, cuando se tiene una **RED LOCAL** se presenta un potencial a resolver, asegurar de alguna forma, que en el momento de actualizar SIMULTANEAMENTE la información, NO se llegue a un estado inválido, si no se tiene esa precausión, no servirá de mucho todo el Software de aplicación que se vaya a manejar, simplemente porque no son confiables los datos de los archivos.

Existen algunos casos, en los cuales los usuarios de determinados programas, NO usarán simplemente los archivos, o más concurrente, NO los actualizarán al mismo tiempo. En general este tipo de Software puede funcionar sin más trámite en una **RED LOCAL.**

Sin embargo, es necesario verificar que dichos programas no generen archivos temporales que puedan ser duplicados por otros usuarios al utilizarlos simultáneamente y sino se infringen derechos de autor al utilizarlos en la **RED LOCAL.**

El problema descrito anteriormente de actualizar simltáneamente la información, se le denomina Acceso Concurrente, es necesario comentar que muchas personas denominan SOFTWARE MULTIUSUARIO a aquel que, de un ambiente de **RED LOCAL** o de Equipo Multi-terminales-permite el acceso y actualización concurrente a la infomación, en las presentes no se utilizará dicho término.

Mecanismos de Señalización (Semaforización)

Existe una base teórica muy amplia (ver bibliografía del capítulo 1), pero no es objetivo de las notas el analizar todas las posibles soluciones conocidas. Se ha demostrado que el actualizar un mismo registro por más de un usuario (sin ningún control) conlleva a estados inválidos.

Ahora bien, la solución más fácil es IMPEDIR de alguna forma que más de una persona (o programa) pueda USAR o GRABAR en ese registro. Se puede ilustrar el proceso a realizar con una escena de la vida cotidiana, se verán los pasos que lleva a cabo una persona para realizar una llamada telefónica en la calle.

a) Alejandro ve la cabina telefónica, y se acerca a ella, y comprueba si está ocupada o no.

b) Si está acupada, lo cual es muy fácil de comprobar a simple vista, entonces espera hasta que se desocupe, y podrá entonces pasar al inciso (c). En el tiempo que espera, Alejandro continuamente comprueba si la cabina se desocupa o no, de hecho si es grande su urgencia, sólo estará atento a que se desocupe, y a esto se le denominará estado: "ESPERA POR OCUPADO".

c) Cuando la cabina se desocupa, o si nunca estuvo ocupada, Alejandro pasa a ocuparla, y cierra la puerta indicando a los posibles usuarios del teléfono, que la cabina ha sido ocupada. Se llamará a este paso "BLOQUEO DEL RECURSO", por que Alejandro está fijando una restricción para utilizar el recurso llamado telefónica.

De hecho si una persona deseara usar la cabina mientras Alejandro se encuentra en ella, No lo podrá hacer por que hay un impedimento físico que le indica que está ocupada.

d) Cuando Alejandro termina de hacer su llamada, sale de la Cabina dejando la puerta abierta, con lo cual queda claro que la cabina está libre para ser usada por otra persona, a este hecho se llama "DESBLOQUEO DEL RECURSO".

Aunque parezca raro el ejemplo; es muy ilustrativo de lo que se desea dar a entender:

a) Existe un recurso (la cabina) que sólo puede ser usado por una persona a la vez.
b) Debe existir un método por el cual, cuando alguién utilice el recurso, los demás usuarios potenciales se enteren de que está siendo ocupado, y esperen para poderlo utilizar.
c) Dicho mecanismo de BLOQUEAR el recurso deberá deshabilitarse cuando se deje de utilizar el recurso.

Para explicar la solución del problema, se cambiarán sólo algunos términos de lo que sucede en el ejemplo, para que se extrapolen con lo que sucede en una **RED**:

1.- El recurso será el registro a grabar.

2.- La forma de BLOQUEAR el registro dependerá del lenguaje con que se trabaje, pero normalmente los sistemas operativos de **RED** (ver capítulo 3) poseen funciones específicas para dichos bloqueos, técnicamente llamados Candados (LOCKS). En vez de que Alejandro cierre la puerta de la cabina, en una **RED** el programa deberá bloquear o poner un candado al registro que vaya a graber.

3.- Cuando el programa ha terminado de grabar el registro, deberá desbloquear el registro correspondiente (operación de quitar el candado o en inglés UNLOCK).

Hasta el momento se ha partido del supuesto de que el usuario puede esperar un tiempo indefinido, hasta que se desocupe el recurso, lo cual en la práctica no siempre es factible ni recomendable. En el ámbito de una **RED LOCAL**, es importante considerar este factor, posiblemente un programa no deba esperar indefinidamente hasta que el registro que se desea leer, se desocupe; sino más bien intentar un cierto número de veces durante un período definido de tiempo.

Si al cabo de ese tiempo (normalmente algunos segundos) el registro sigue ocupado, determinar una condición de "tiempo fuera" (timeout) y realizar otras tareas. Cuando se trabajan varios archivos a la vez, es posible tener problemas, aún si se utilizan candados. Analícese el siguiente ejemplo en donde dos programas están actualizando simúltaneamente los mismos archivos:

Programa A :	***Programa B :***
Actualiza Inventario	
Salidas:	*Consulta:*
Lock (Registro X Archivo Inv)	*Lock (Registro Y Archivo Movim)*
Existencia = Existencia-Z	*Leer Salida Z*
Unlock(Registro X Archivo Movim)	*Unlock (Registro X Archiv Inv)*
Lock(Registro Y Archivo Movim)	*Lock(Registro X Archivo Inv)*
Agregar Registro para	*Leer Existencia*
el Artículo I Salida Z	*Unlock(Registro X Archivo Inv)*
Unlock(Registro Y Archivo Movim)	*Desplegar Existencia,*
	y total Salidas

El problema que se presenta es que mientras un programa está actualizando una serie de registros de diversos archivos, puede existir otro programa (en el ejemplo el programa consulta) que está leyendo registros que el primero ya ha desbloqueado.

En otras palabras, el programa de actualizar inventario está "liberando ", antes de lo necesario, ciertos registros lo cual hace que caiga en estados inválidos, aunque aparentemente está actuando de forma correcta.

Método de Bloqueo en Dos Fases (Two Phase Locking)

Bajo este método los programas deben de poner candados a todos los registros necesarios, actualizarlos y después quitar dichos candados en el orden inverso a como fueron puestos.

Siguiendo el método, los programas del ejemplo anterior quedarían:

Programa A:	***Programa B:***
Salidas del Inventario	*Consultas al Inventario:*
Lock (Registro X Archivo Inv)	*Lock (Registro Y Arch Movim)*
Lock(Registro Y archivo Movim)	*Lock (Registro X Archivo Inv)*
Existencia = Existencia -Z	*Leer Salida Z*
Agregar Registro para	*Leer Existencia*
El artículo I Salida Z	*Desplegar Existencia*
Unlock (Registro Y Archivo Movim)	*Unlock (Registro X Archivo Inv)*
Un lock (Registro X Archivo Inv)	*Unlock (Registro Y Movim).*

Esta forma de trabajar resuelve el problema de estados inválidos, y en general es muy segura, pero puede existir el problema de caer en un " abrazo mortal" (deadlock). De los mismos programas de los ejemplos, observe que pasaría con la siguiente secuencia de pasos:

Programa A:	***Programa B:***
Lock(Registro X Archivo Inv)	
	Lock(Registro Y Archivo Movim)
Lock(Registro Y Archivo Movim)	
	Lock(Registro X Archivo Inv)
- - -en espera- - -	*- - - en espera - - -*

El programa A, está en espera de poder usar el registro "Y" del archivo de movimientos, el cual ha sido bloqueado por el programa B, y el programa B está en una situación similar; se encuentra usando el registro "Y", y está esperando poder usar el registro X del archivo inventario el cual está ocupado por el programa A.

En otras palabras, los programas están esperando mutuamente, en este caso cabría la siguiente pregunta: ¿ Hasta cuándo?

Si en el ambiente de programación no existe una salida por tiempo (TIMEOUT) , o no se utilizó, los programas quedarán en ese estado hasta que se les interrumpa externamente (por ejemplo con control-c) o hasta que se apague y vuelva a encender el equipo. Más adelante se analizarán algunos gestores de bases de datos que pueden controlar abrazos mortales.

Método de Sellos de Tiempo (Time Stamp)

Para no confundir al lector, se simplificarán algunos pasos de este método.

Supóngase que dos personas están en un mismo programa y coinciden en utilizar el registro 5, obviamente sólo podrá entrar a utilizarlo el primero que lo tome, porque el otro tendrá que esperar a que el registro no tenga candado. Ahora supóngase que la persona que tiene con candado el registro 5, mientras está capturando los datos y antes de grabarlos en el mencionado registro, decide levantarse e ir a tomar un café con unas galletas y platicar un rato con la secretaria (situación nada rara). ¿Qué pasa mientras con la otra persona?

Si el programa tiene definido un *"timeout"* entonces al cabo de algunos segundos de tratar de leer el registro 5, el programa marcará un error interno, que se deberá manejar a través de un aviso al usuario tal como: *"Registro ocupado. Desea manejar otro cliente"* o algo similar, si el programa no tiene capacidad anterior, los resultados pueden ser trágicos. De cualquier forma, con la definición de tiempos máximos de espera (timeouts) o sin ellos, lo ideal es tratar de OPTIMIZAR el tiempo en el que un registro está con candado. La técnica de series de tiempo trata de optimizar entonces dicho tiempo "Locking" de la siguiente manera: A cada registro del archivo, se le agregará un campo en donde se registre la hora de la última actualización. Con este campo adicional, se realizarán los siguientes pasos:

```
LEER el Registro i  (en un tiempo T1)
CAPTURAR datos, hacer cálculos, etc.
LOCK (Registro i)
  LEER el Registro i
    Verificar SI el sello de tiempo st (i) < T1
    ENTONCES: grabar el Registro
  DE LO CONTRARIO se actualizó desde que se leyó el registro.
TOMAR las medidas necesarias.
```

En el campo de las computadoras tipo PC, la mayoría de los nuevos lenguajes comerciales poseen instrucciones de LOCK Y UNLOCK, que se pueden aplicar dependiendo de como se implementaron a nivel de todo el archivo de un solo registro o incluso de un cierto número de bytes que el programador especifique.

Si el lenguaje no posee las funciones de bloqueo y desbloqueo bajo ningún nombre (es posible que tengan una denominación de un LOCK Y UNLOCK) , entonces lo recomendable es escribir el código para ellas, de la forma más modular posible; es decir si se trabaja en Pascal.

Hacerlos como procedimientos de un archivo que se puede incluir en la compilación (normalmente bajo la opción $I de algunos compiladores Pascal), si se desea programar en lenguaje C, de forma similar se deberá definir una función externa que se incluya de preferencia en una biblioteca.

Otra recomendación más sencilla es comprar utilerías de manejo de archivos indexados que poseen las capacidades de manejo de **RED** y que se puedan "interfasear" con el lenguaje de preferencia.

Es posible también desarrollar las funciones primitivas (LOCK Y UNLOCK) en lenguaje ensamblador, y ligarlas al programa haciendo un llamado directo a ellas.

4.2 BASES DE DATOS Y LENGUAJES DE CUARTA GENERACION PARA REDES PCs

Antecedentes y Terminología

En los últimos años se ha venido dando en le mercado de Software, una marcada tendencia a la utilización de ambientes más poderosos, que reduzcan por una parte el tiempo de desarrollo y mantenimiento al Software y que permitan mayores flexibilidades en la explotación de la información.

Los términos Bases de Datos y Lenguajes de Cuarta Generación se usan hoy en día tan frecuentemente, que muchas veces en vez de clarificar entorpecen el entendimiento de los conceptos.

Lo que si queda claro es que ambos términos son "vendedores", la gente los pide aunque no siempre se identifique exactamente lo que son. Para uniformizar criterios se definen los siguientes conceptos:

UN MANEJADOR O GESTOR DE DATOS.- Es un conjunto de programas, enfocados a conseguir como principal objetivo:

Fungir como intermediario entre los datos (archivos) y los usuarios o programas.

Algunas de las propiedades más útiles de los manejadores de Bases de Datos son:

+ **Independencia** (o casi) entre los datos y los programas. Si cambian los datos, no hay que corregir los programas.

+ **Visión Global de la aplicación:** Como normalmente se plantea en un manejador, es diseñando todos los archivos y datos que estarán involucrados en la aplicación.

Esto permite reducir al máximo la repetición de los datos (Tan frecuente en las aplicaciones clásicas sin bases de datos).

+ **Lenguaje de interface hacia el usuario.** Comunmente llamado Query o Lenguaje de Consulta. Este mismo lenguaje con algunas modificaciones posiblemente, u otro diferente, es el que algunos manejadores permiten utilizar desde lenguajes de alto nivel, (Lenguajes "embebido" o interfaces de aplicación para programas: API).

Observe la distinción hecha entre Manejadores de Bases de Datos y Bases de Datos en sí: los primeros son lo programas que controlan, y actualizan a las segundas.

Por mala costumbre, la mayoría de las personas usan en forma contraria o indistinta ambos términos.

Como un avance más hacia la productividad, se encuentran las Herramientas o Lenguajes de Cuarta Generación.

Debido a que no existe tanta formalización en los desarrollos de este tipo de herramientas, no hay ninguna definición más o menos estandarizada.

Pero con el objeto de poder definir, lo que es y lo que no es una herramienta de cuarta generación, se puede decir que es un ambiente (conjunto de programas y utilerías) enfocado a aumentar la productividad de un programador en un orden de magnitud y a facilitar posiblemente a un usuario no técnico, para que pueda él mismo desarrollar aplicaciones con cierto grado de complejidad, que en un ambiente normal de desarrollo simplemente no podría realizarlas.

Normalmente los lenguajes de cuarta generación están apoyados en un manejador de Base de Datos, y observando la definición del párrafo anterior, se podría pensar con cierto fundamento que muchos manejadores de Bases de Datos son también lenguajes de Cuarta Generación.

Como se comentó antes, en general la declaración de si es una herramienta de cuarta generación o no, depende de todas las facilidades que den a los programadores o a los usuarios finales, para desarrollar aplicaciones.

Características Deseables en un Manejador de Base de Datos y/o Lenguaje de 4° Generación

+ **Interface al usuario:**

  - Sencilla.
  - Posibilidad de Menús.
  - Lenguaje de consulta poderoso pero sencillo.
  - Ayudas en línea.
  - Acceso a varios archivos a la vez.
  - Reportador elemental.
  - Generador de aplicaciones.
  - Lectura de archivos de otros programas o manejadores.

+ **Interface al programador:**

  - Lenguaje nativo poderoso o Interfaces a lenguajes de alto nivel.
  - Manejo de acceso concurrente (indispendable en aplicaciones de **RED**).
  - Concepto de transacción y "roll-back".
  - Manejo de ventanas.
  - Manejo de ayudas contextuales.
  - Facilidad de compilar las aplicaciones.
  - Posibilidad de restricción de los accesos.
  - Validación de datos.
  - Generación de un Diccionario de Datos.
  - Generación de Pantallas.
  - Manejo eficiente de los archivos.
  - Posibilidad de establecer relaciones múltiples entre los archivos.

En las siguientes secciones, se revisarán algunos de los principales conceptos asociados a los manejadores de bases de datos y a su implementación en **REDES LOCALES**.

El Diccionario de Datos

Se denomina diccionario de datos a las tablas que mantienen toda la relación de los campos y sus atributos asociados, es decir el nombre del campo su longitud, tipo de dato etc.

En manejadores pequeños y en algunos no tan chicos, no se tiene un diccionario de datos como tal, en el mismo *dBase-III Plus* no se contempla esta facilidad.

En general es muy ventajoso un diccionario de datos porque permite definir las características de los datos UNA SOLA VEZ, no importa que dichos datos sean usados en varios archivos. De esta manera si el campo CLAVE DE CLIENTE, se usara en varios archivos, sus características son almacenadas una sola vez.

Además permite un mejor control sobre los nombres de campos, ventaja muy útil cuando existen varios programadores desarrollando módulos distintos del mismo sistema.

Interfaces con Lenguajes de Alto Nivel y SQL

En un manejador de bases de datos existen 3 posibilidades básicas en cuanto a programación:

- Que no tenga poder de programarse bajo ninguna forma, y a lo sumo se pueda almacenar las consultas que se deseen. Normalmente este tipo de manejadores caen como manejadores de archivos, más que de bases de datos.

- Que se programen en un lenguaje propio. Por ejemplo DBASE, R: base o Dataflex.

- Que tengan una interface hacia lenguajes de alto nivel como Pascal, C ó Cobol.

En esta última categoría se pueden encontrar paquetes que básicamente sólo funcionan desde lenguajes de alto nivel (*dB-Vista* o *B-Trieve*) y paquetes que tienen todo un lenguaje de consulta para usuarios no-técnicos, pero que poseen la capacidad de mezclarse con lenguajes de alto nivel.

De una u otra forma, en estos casos los programas de *Cobol* o de *C* o del lenguaje que se trate, contienen instrucciones adicionales para llamar al manejador de Base de Datos, y manipular los datos.

Regularmente se utilizan compiladores comunes y corrientes (por ejemplo el *Compilador C* de *Lattice*, o el *Cobol* de *Microsoft*) y las intrucciones especiales de llamada a la Base de Datos se anteponen con algún símbolo convencional, por ejemplo '%%'.

En sistemas de Bases de Datos, se distinguen diferentes tipos de lenguajes para manejar información:

* Lenguaje de Definición de Datos (DDL) con el cual se crean las tablas y el diccionario de datos.

* Lenguaje de Consulta (Query Language) con el cual, se hacen consultas no planeadas a la información.

  En ocasiones el lenguaje de consulta (Query) puede ser simplemente un subconjunto del lenguaje de manipulación de datos.

* SQL (del inglés Structured Query Language) es más que un simple lenguaje de consulta, es también un lenguaje de definición y un lenguaje de manipulación de los datos.

Las principales vantajas de ***SQL*** son:

+ Posee todas las operaciones para manejar las Bases de Datos con el enfoque relacional (operaciones de select, project y join).

+ Tiene recursividad en los *Querys*.

+ Tiene interfaces a lenguajes de alto nivel (*embedded SQL*),

+ Tiene instrucciones de seguridad en restricciones de accesos.

Pero la característica más importante de todas, es que SQL ES UN ESTANDAR.

Por una parte, *IBM* - su creador - lo ha impulsado en sus manejadores de bases de datos de equipos mayores (*DB2* y *SQL/DS*) y ahora anuncia soportarlo bajo el nuevo sistema operativo *OS/2* para equipos *PS/2*.

Y desde 1986, es un estandar aprobado por ANSI.

Lo anterior ha hecho que *Lotus, Microsoft, Ashton-Tate* y *Microcrim* entre otros, hayan anunciado un soporte futuro al estandar *SQL* y que productos actuales como *ORACLE* en minicomputadoras y *SQL-Base* en REDES de micros, estén tomando un auge importante en el mercado de Bases de Datos.

El impacto comercial que traería una estandarización hacia *SQL* vendría en relación directa a la economía que representaría al poder correr los mismos programas, con las mismas llamadas a *SQL*, lo mismo en una *PC* o *PS/2*, en una RED, de estos equipos, en una microcomputadora o que en un Mainframe. De esta forma, en vez que los programadores estuvieran rehaciendo a cada momento los sistemas para cambiarlos de ambiente, se preocuparían de tener un adecuado mantenimiento y mejora a los mismos, tarea para la que normalmente "no hay tiempo".

Transacciones, Bitácoras y "Roll Back"

Conforme se van sofisticando las aplicaciones en Bases de Datos, va siendo necesario el contar con herramientas que simplifiquen diversas tareas. Una de esas tareas es la recuperación de la información en caso de fallas, así como el asegurar la consistencia en dicha información. La consistencia se refiere a que la información refleja siempre el estado del mundo real y que no puedan suceder casos, que por fallas en algún proceso (por Hardware o Software), un grupo de actualizaciones a diversos archivos se quede "a medias".

Para poder asegurar una consistencia en la información, se creó el concepto de una transacción. Una transacción es un bloque atómico de actualizaciones a diversos archivos. Al decir atómico, queremos decir INVENCIBLE, en otras palabras una transacción sólo se puede estar en dos estados: no hecha, o hecha totalmente.

Si algo llega a suceder en el período entre el inicio y el final de una transacción debe ser eliminada.

Para poder eliminar transacciones no-terminadas, y asegurar la consistencia en la información, el método más práctico es llevar una bitácora donde se grabe el estado anterior y el movimiento que afecta al registro y al campo específico, de esta forma, si algo sucede dentro de una transacción, se recorrerá la bitácora y se volverán a colocar los archivos en su estado inicial, a la operación anterior se le denomina "roll-back", y a la bitácora es común que se le llame "log".

La mayoría de las bases de datos que han evolucionado bien de ambientes micros-monousuarios, o de microcomputadoras multiusuario, hacia **REDES LOCALES**, llevan en su construcción un problema inherente que en ocasiones puede ser grave. Para ilustrarlo mejor, se mostrará un ejemplo:

Desde una estación de trabajo, un usuario desea conocer cuántos de los empleados de la compañía ganan más de un millón de pesos al mes.

Se parte del hecho que el archivo total de empleados es de 2,000 registros "viajarán", en la **RED**, y sólo hasta llegar a la estación de trabajo se seleccionarán para ser desplegados sólo 15 (los que cumplen la condición).

Si operaciones similares a la anterior las empiezan a realizar 10, 15 ó 20 usuarios, la degradación de la **RED** puede ser muy notoria.

La solución teóricamente es muy sencilla: en vez de que el resultado del query se "calcule" en la estación de trabajo, se puede hacer que se ejecute en el mismo server, y cuando así se logre, el server se convertirá en un **Server de Base de Datos.**

El concepto de **Server de Base de Datos** es muy importante que se tome en cuenta, ya que las orientaciones futuras de los manejadores de bases de datos, estarán enfocadas a funcionar bajo este concepto, lográndose con estos grandes avances en el rendimiento de las **REDES.**

En la actualidad ya existen un par de productos que manejan el server de base de datos pero son sumamente caros y no están disponibles en el mercado.

A continuación, se describirán brevemente las principales características de varios paquetes Manejadores de Bases de Datos.

MANEJADORES DE BASES DE DATOS

DATAFLEX

+ Una de sus principales ventajas, es el trabajar en varios ambientes. Entre otros, *Unix* y *VMS* de *VAX*

+ Su lenguaje es poderoso, pero el paquete no es fácil de usar por usuarios principiantes. Es un sistema orientado a realizar aplicaciones por programadores.

+ Incluye algunas herramientas como *AUTOEDF* y *FILDEF* para crear archivos.

+ Posee un diccionario de datos aceptable.

+ Uno de sus puntos fuertes es el manejo de concurrencia, la cual usa una técnica similar a la de sellos de tiempo a través de dos instrucciones *REREAD* y *NOCHANGE*.

+ No hay protección por password.

DATASTORE: LAN

+ Varias herramientas/utilerías para menús, creación de bases de datos, pintar formas, escribir reportes y hacer queries.

+ En vez de lenguaje propio, tiene un conjunto de utilerías *LAN:DATACORE*, que pueden ser invocadas desde *Fortran*, *Pascal* o *Basic*.

+ Locking implícito-automático.

+ Seguridades excelentes por varios niveles, incluyendo campo, o incluyendo grupos de resgistros.

+ Tiene una forma de encriptamiento para los archivos.

INFORMIX-SQL

+ Basado en el concepto de database-server, pero a su manera, con un server tipo *Unix*.

+ Posee *SQL*, y *API* hacia *C*.

+ Seguridades vía comandos de *SQL: Grant y Revoke*.

+ Creación de menús, *Report-Write* y creación de formas.

+ Se tiene también *INFOMIX-4GL* con una interface más sencilla para facilitar la programación.

+ Genera programas en *C*.

R:BASE SYSTEM V

+ Una mejor significativa de *R:Base 5,000*.

+ Muchos manuales.

+ Excelente generador de aplicaciones (el mejor).
  - Aplication Express.
  - Definition Express.
  - Forms Express.
  - Reports Express.

+ Puede ser usado por usuarios principiantes prácticamente sin problemas.

+ El Record Locking, no hay problema. Totalmente implícito y todos pueden accesar el mismo registro, si no cambió un campo y el otro también, al último le aparece un mensaje de que se ha cambiado el campo lo quiere de todos modos grabar?

+ Pero ciertas operaciones pueden bloquear todo el archivo y cuidado.

+ Seguridad en el acceso, sólo a nivel de tablas.

REVELATION

+ Registros de longitud variable (registros y campos).

+ Lenguaje poderoso para aplicaciones y reportes. *R/BASIC* es el lenguaje de las aplicaciones, similar a basic o pascal.

+ También esta *R/Design*, un lenguaje de 4ta generación y *R/List*, un lenguaje generador de queries y reportes.

+ Todos los Records Locking totalmente explícitos, checando que no esté bloqueado.

+ Seguridad sólo por grupos de aplicación.

SQL-BASE

+ Una implementación excelente de *SQL*. Utiliza el concepto de *Data Base Server*.

+ Interface *API* hacia *C* y *Cobol* (más en el futuro).

+ Seguridades a través de *GRANT* y *REVOKE*.

+ Record Locking optimizado y automático. Para grandes volúmenes de información.

+ Posee un producto de conectividad hacia *DB2* y *SQL/DS* de *IBM* llamado *SQL-NET*. Mediante *SQL-NET*, es transparente para los usuarios y las aplicaciones, si sus archivos se encuentran en el mainframe o en el server.

4.5 TENDENCIAS ACTUALES Y FUTURAS EN SOFTWARE PARA RED

Las tendencias que se mencionarán, se deducen en general del comportamiento del mercado, los productos que están teniendo más éxito, las necesidades de los mismos usuarios y lo que los mismos redactores de libros y revistas marcan.

Sin embargo, se vierten aquí opiniones particulares sobre las tendencias del Software por lo que se respeta cualquier, punto de vista de personas adentradas en el medio de las **REDES** que difiera de las opiniones que se expondrán.

En resumen, las tendencias más importantes en el área de Software para **REDES LOCALES** son:

En sistemas operativos:

- **NetWare de Novell** ha fijado la pauta para medir el rendimiento de otros sistemas operativos por venir.

- Las capacidades de comunicaciones y enlaces, así como la tolerancia a fallas son cada vez más importantes.

- Se harán más populares los sistemas que interactúen directamente con el *S.O.* a través de *APIs*. Se requerirá de más documentación por parte del proveedor del *S.O.* para realizar adecuadamente estas interfaces.

En Software de aplicación:

- Sin lugar a dudas, que en Bases de Datos, *SQL* y el concepto de Servidores de Bases de Datos tendrán un lugar primordial.

- La conectividad de Software es un tema que surge fuertemente apenas en 1987. Tanto en Bases de Datos como en Hojas de Cálculo y otras aplicaciones, las cuales se tendrán en las capacidades en los próximos años.

- Las herramientas de Software para monitorear el "performance" de la **RED**, toman también interés.

- En México, se vió nacer Software para **REDES** tanto administrativo como de mercados verticales notoriamente a partir de 1988.

- Muchos desarrolladores cambiarán sus ambientes a *SQL* y lenguaje *C*, pero este cambio será paulatino. Se necesitará de programadores con mejor nivel profesional.

- Programas varios para **RED**, con interfaces tipo *Windows*, y asociadas realmente al *Windows de OS/2*.

SUPERVISOR DE UNA RED

SUPERVISOR DE UNA RED

Introducción

Una de las principales ventajas de trabajar con una **RED** Local, es lograr que el usuario final, tenga la facilidad de compartir los recursos de la **RED**, sin tener la necesidad de realizar operaciones complicadas al estar trabajando en ella. Sin embargo, para que esto pueda ser posible, se requiere llevar a cabo una serie de tareas, que deberán ser realizadas por una persona responsable del óptimo funcionamiento de la **RED**. **A esta persona se le conoce como EL SUPERVISOR DE LA RED.**

Tareas del Supervisor

Para mantener la **RED** en óptima operación, es necesario que el Supervisor realice determinadas tareas, unas iniciales y otras cotidianas o esporádicas. Las primeras de ellas, cuando la **RED** es adquirida, y las segundas cuando la **RED** ya ha sido puesta en operación. El Supervisor puede realizar un sin fin de actividades dentro de las principales tareas que debe realizar están las siguientes:

Tareas Iniciales:

Instalación del Hardware:

* Montar tarjetas, cableado y repetidores, probar el Hardware.

Intalaciones del Software:

* Formatear o preparar el o los Servers.

* Definir las impresoras para el Spooler.

* Alta a los usuarios de la **RED**, sus Passwords, Derechos, Restricciones, etc.

* Configurar el Software (si es necesario) para que corra bajo la **RED**.

* Preparar para cada usuario y/o grupo de usuarios, los procedimientos de entrada a la **RED**, de forma de facilitar sus operaciones.

Tareas Cotidianas y Esporádicas:

* Avisos generales a los usuarios (desde consola).
* Revisión del Hardware en caso de falla.
* Re-enrutamiento de impresora (s) para el "Spooler".
* Modificación de parámetros en el server (buffers, archivos abiertos, etc) para mejorar el "Perfomance" de la **RED**.
* Monitoreo de las tareas de los usuarios.
* Asignación y designación de recursos compartidos.
* Revisión de los procedimentos de entrada a la **RED**, y de asignación de derechos y protecciones.
* Instalación de nuevos paquetes.

Las tareas anteriores de no ser realizadas por el SUPERVISOR DE LA **RED**, tendrán que ser ejecutadas necesariamente por el usuario final, o por el distribuidor. En ambos casos los resultados no serán totalmente satisfactorios, ya que el usuario final no está debidamente capacitado para administrar la **RED**, y el distribuidor no conoce con la profundidad suficiente las necesidades de la empresa a la cual le está proporcionando la **RED**.

En forma general, podemos agrupar las tareas del Supervisor de la **RED** en:

- Instalación del Hardware.
- Instalación del Software.
- Establecer Niveles de Seguridad y Acceso.
- Realizar Interfaces Amigables al Usuario.
- Mantenimiento de la **RED**.

Instalación

Como la instalación de una microcomputadora, la instalación de una **RED** comprende tanto Hardware (tarjetas de **RED**, cableado, etc.) como Software (básicamente el sistema operativo de la **RED**).

Instalación del Hardware

En general esta es más tarea del distribuidor que del propio Supervisor; sin embargo en forma ideal ambas partes deberán de realizar las siguientes tareas:

+ Instalación física de las tarjetas de **RED** dentro de cada PC o AT. El principal detalle a observar, es el *DIRECCIONAR* correctamente los switches de cada tarjeta, teniendo la precaución de que no se repita para más de una de ellas.

+ Previamente se debió de determinar la topología exacta de la **RED**. Definiendo cuantos repetidores activos y pasivos serán necesarios, si este es el caso, tomando en cuenta distancias a cubrir, equipos físicamente cercanos y posible crecimiento a futuro. (Tareas en la que normalmente el distribuidor ASESORA al usuario.

+ El cableado físico de la **RED**, debe ser por lo menos verificado por el Supervisor, tratando de que los cables pasen a través de ductos (sin que vayan a tener interferencia por cables de voltaje cercanos) y que no haya posibilidad de desconexión porque se encuentren en el paso de personas.

Interfaces Amigables con el Usuario

Una de las principales tareas que tendrá siempre el Supervisor de la **RED**, será proporcionar de alguna forma al usuario, la facilidad de accesar a la **RED**, sin que éste deba utilizar comandos especiales. Para esto el Supervisor deberá realizar una serie de **Interfaces "Amigables"** para que el usuario accese sin problemas a la **RED**.

Dependiendo del sistema operativo de la **RED** en que se esté trabajando se pueden tener algunas ventajas, pero en general siempre se podrán utilizar archivos BATCH (.bat), que simplifican muchas tareas. A continuación, describiremos algunos "tips" para la realización de archivos BATCH.

Archivo Batch

Es conveniente realizar un archivo AUTOEXEC.BAT, como se muestra a continuación.

```
ECHO OFF
CLS
ECHO ---------------------------------------------------------------
ECHO                    • • •  SEI, S.A. DE C.V.  • • •
ECHO ---------------------------------------------------------------
ECHO
ECHO
ECHO                          MENU DE OPCIONES
ECHO
ECHO                  ENTRAR A OPEN ACCES ..... O
ECHO                  ENTRAR A LA RED..... R
ECHO                  SISTEMA OPERATIVO..... S
ECHO                  FIN DE LA SESION..... F
ECHO
ECHO
PROMPT            Cuál es su opción ?
ECHO  ON
.
.
.
```

Este archivo deberá estar en el directorio raíz de uno de los nodos, suponiendo que OPEN ACCESS y SISTEMA OPERATIVO son aplicaciones exclusivas del nodo, y que todas las demás aplicaciones serán manejadas a través de la **RED**.

Además del archivo AUTOEXEC.BAT será necesario generar los archivos BATCH para cada opción.

Suponiendo que estamos el IBM-PC LAN (IBM PC-NET) como ambiente de nuestra **RED**, entonces el archivo BATCH para entrar a la **RED** podría contener la siguiente información:

ECHO OFF
CLS
NET START RDN NODOS2
NET USE D: SERVIDOR GENERAL
NET USE E: SERVIDOR WS
NET USE LPT2: SERVI-II IMPRE
AUTORED
ECHO ON

Donde AUTORED, se refiere a otro archivo BATCH cuyo nombre es: AUTORED.BAT.

Consideraciones Importantes para *NetWare de Novell*

Además de lo anterior, NetWare de Novell se tienen dos ventajas adicionales:

1.- Posibilidad de generar un *"Login Scrpit"*; esto es, personalizar la entrada por usuario, por grupo o definir una entrada general, en donde se indique al usuario un mensaje de bienvenida, y donde el Supervisor define que es lo que desea que ejecute el usuario, cuando entre a la **RED**.

2.- Generación automática de *MENUS*, a atravéś del programa.

Mantenimiento de la RED

El mantenimiento de una **RED LOCAL**, es necesario una vez que la **RED** entra en operación.

Para dar el mantenimiento, el Supervisor de la **RED** deberá revisar periódicamente los parámetros de seguridad del Software de la **RED**, así como vigilar que el cableado tanto de comunicación como el de suministro eléctrico, estén en perfectas condiciones para su uso.

Además de las revisiones periódicas, el Supervisor tendrá que adecuar cuando sea necesario, las restricciones de uso de los archivos, usuarios y grupos de usuarios.También deberá reportar las fallas en el Hardware cuando éstas ocurran, o sí es posible repararlas en el momento de su ocurrencia.

Las tareas del Supervisor referentes al mantenimiento de la **RED**, pueden ser auxiliadas si se llevan controles escritos.

La utilización de Bitácoras son de gran ayuda, ya que éstas, servirán como apoyo al Supervisor para poder tener un perfecto control de la situación actual de la **RED**, así como los cambios que ha sufrido la **RED** desde que está en operación; así mismo, será posible realizar un análisis de:

a) La utilización de la **RED** por usuario.
b) El promedio de uso de cada nodo.
c) El promedio de fallas en la **RED**, tanto de Hardware como de Software etc.

Sobre Todo el Objetivo primordial del Mantenimiento de la **RED**, es el poder medir constantemente "Performance" (rendimiento) de la **RED**, para poder mantenerla en óptimas condiciones de operación.

Otra recomendación que se puede dar, es el de tener una persona que en un momento dado, pueda sustituir al Supervisor en caso de que éste no se encuentre.

FUNDAMENTOS DE CONECTIVIDAD

FUNDAMENTOS DE CONECTIVIDAD

Desde hace algunos años y cada día en mayor grado, se escucha hablar de "conectividad". IBM con el lanzamiento de sus nuevos equipos PS/2, maneja el término "conectividad" en casi todos sus folletos y propaganda, y la misma revista PC-Magazine ha incluido una sección, cuyo nombre es precisamente "Connectivity".

Conectividad es la capacidad de conectar computadoras o equipos de igual o diferente naturaleza.

Existen diversas maneras de conectar equipos entre sí, pero las que más interesan para los fines del capítulo son aquellas que involucran una o más **REDES LOCALES**, y desde este punto de vista, se tienen las siguientes posibilidades:

Bridge o "Puente"

Se define como un *"Bridge"* a la conexión de una **RED LOCAL** a otra. Para tal efecto, se utiliza el server o alguna estación de trabajo que actué como *"Puente"* entre ambas **REDES**. Los bridges pueden ser internos o externos, entre **REDES** del mismo tipo o de diferentes carcterísticas, e incluso pueden permitir el "platicar" con protocolos de comunicaciones diferentes. Este último sería el caso cuando conectamos una minicomputadora directamente a la **RED**. Posteriormente se ampliarán los conceptos sobre puentes.

Emulación de Terminales

En la emulación de terminales, se contempla una sola PC que se conectará a un equipo mayor llamado anfitrión o "Host", para hacer las veces de una terminal de dicho equipo.

Dependiendo del equipo al cual se realice la conexión, puede ser necesario el uso de Software y Hardware, o sólo de Software.

De entre las emulaciones más simples, se encuentran las de terminales de un equipo VAX:VT-100.

Cuando se desea esta emulación, solamente hay que usar un programa de Software de este tipo (existen más de 100 en el mercado americano), por ejemplo Crosstalk y conectar nuestra PC a través del puerto serial al cable que vien de la VAX.

En este caso la solución es muy simple porque tanto la forma de conexión, como los códigos y protocolos utilizados en una VAX y en una PC son básicamente iguales (se utiliza un puerto serial RS-232 y código ASCII).

Sin embargo en otro tipo de conexiones es necesario realizar algunas conversiones adicionales, por lo que se debe utilizar una tarjeta especial.

Por ejemplo, para conectarse a equipos IBM grandes, como son las 4381, 3031 y en general las familias 43xx y 30xx, es necesaria una tarjeta de Hardware como la ya muy conocida tarjeta IRMA y además ciertos programas que permiten que la PC emule una terminal de esos equipos. (el modelo de la terminal es 3278 ó 3279, genéricamente son llamadas 3270's ó 327x).

Debido a que un 3278/3279 se conecta al computador por un cable coaxial y a través de ese cable la terminal "platica" con un controlador especial que atiende a varias terminales, la tarjeta de conexión deberá realizar las funciones de conversión de protocolos para que se establezca la comunicación.

Gateway

Un *"Gateway"* es una extensión del concepto de emulación revisado en los párrafos anteriores y aplicado a una **RED LOCAL.**

El objetivo de un *"Gateway"* es lograr la comunicación de una **RED LOCAL** a otro ambiente, a través de una sola línea. Lo anterior hace posible que desde cualquier estación de trabajo de la **RED**, se pueda accesar a otro ambiente, que regularmente es un equipo mayor.

Por ejemplo, si se tuviera un *Gateway* de una **RED** de ocho micros a un equipo *UNIVAC/100*, entonces cualquier PC conectada a la **RED** podría accesar a la *UNIVAC* tan solo con tener el Software apropiado, y de hecho podrían hacerlo al mismo tiempo todas las PC's.

Con lo expuesto anteriormente podría seguir la siguiente pregunta interesante:

¿Por qué la necesidad de *Gateways*, si ya existen las tarjetas emuladoras y son ya muy conocidas?

Existen dos razones de mucho peso para que sí se desea enlazar una **RED LOCAL** a un *"Host"* se realice a través de un *Gateways* y no con tarjetas emuladoras clásicas:

1.- Economía

Es mucho más económico adquirir la tarjeta de *Gateway* y el Software necesario para las estaciones de trabajo, que comprar una tarjeta emuladora para cada PC que necesite conectarse.

2.- Facilidad de Líneas

Casi siempre es más sencillo conseguir una sola línea para el *Gateway*, que una línea para cada PC emulando.

Tipos de Gateways

Existen actualmente, tres divisiones principales de *Gateways* en el mercado:

+ *Gateways* que utilizan enlace sincrónico a computadores: *IBM43xx* y *30xx*, *IBM medianos* (familia *34/36/38*) a otros equipos mayores (v.gr.*UNIVAC*).

+ *Gateways* que utilizan enlaces asincrónicos a computadores: también llamados server de comunicaciones.

+ *Gateways* que utilizan protocolo *X.25* a **REDES** públicas (como telepac).

De estos tres tipos, solo hablaremos en las líneas siguientes, de aquellos que se encuentren en la primera categoría.

Para que se comprendan las principales características de los Gateways, es necesario definir el término de SESION.

Una sesión es el establecimiento de una conexión lógica entre un dispositivo y el computador. Por ejemplo, en el momento en que una PC sea capaz de emular una terminal 3278, se tendrá una sesión con el Host, ahora bien, si se tuviera la capacidad de poder correr dos programas del Host al mismo tiempo (abriendo ventanas) y además tener asignada una impresora, entonces se tendrían tres sesiones en uso. En el lenguaje de IBM existen, también el concepto de unidad lógica (LU), que en términos concretos puede ser una terminal o una impresora (un dispositivo con el cual establecer una sesión).

Los términos anteriores son importantes porque normalmente las capacidades de los *Gateways* a equipos mayores, están medidas en su capacidad de LU's, lo cual es sinónimo del número de sesiones que pueden manejar.

Gateways a IBMs 43xx y 30xx

De forma similar a una tarjeta emuladora 3270, el objetivo del *Gateways* es hacer posible que varias estaciones de trabajo puedan conectarse al equipo anfitrión o *"Host"* a través de una sola conexión. Aunque desde el punto de vista del usuario, el funcionamiento del *Gateways* es igual a tener varias tarjetas emuladoras; internamente y en su conexión existen diferencias importantes.

+ El *Gateway* consta de una tarjeta similar a una emuladora 3270, pero con una gran difrencia: para el *"Host"*, el *Gateway* emula un controlador de terminales 3274, en vez de una sola terminal.

Esto indica que el *Gateway* normalmente se conecta (como si fuera una 3274) a un controlador de comunicaciones 3705 o 3725.

+ Apartir del equipo donde se encuentra la tarjeta del *Gateway* -- que puede ser el server o una estación de trabajo -- las demás estaciones pueden simultáneamente emular terminales *3278/3279*, tan solo con el Software necesario y aprovechando las conexiones de la **RED**.

+ Debido a que sólo existe una línea de comunicación hacia el *Host*, la tarjeta del *Gateways* debe ser capaz de manejar varias señales a través de la misma línea, es decir, hacer algún tipo de multiplexaje de igual forma que un 3274.

Existen algunos *Gateways* (los menos) que en vez de sustituir un 3274, se conectan a él. Este tipo de *Gateways* se llaman **DFT's** (Distributed Function Terminal) y se conectan a un puerto del 3274 que sea declarado **DFT**.

La característica de estos puertos es que son capaces de manejar varias sesiones por la misma línea. La principal limitante de este tipo de *Gateways* es que sólo soportan hasta 5 LU's, mientras los otros *Gateways* pueden soportar hasta 64 LU's.

Por otra parte, la ventaja principal es que la velocidad de transmisión entre el 3274 y la tarjeta *Gateway-DFT*, es muy alta (similar a las velocidades internas de la **RED LOCAL**).

Dependiendo del fabricante del *Gateway*, es posible tener enlaces a estos equipos bajo protocolo *SNA/SDLC* o *BSC*. Bajo el pimer tipo, se tiene una arquitectura mucho más completa de protocolos, que el mismo IBM ha estado tratando de uniformizar a partir de 1974.

También dependiendo del fabricante, del modelo del *Gateway* que se adquiera variará el número máximo de sesiones que se pueden trabajar, e igualmente el fabricante del *Gateway* definirá como una máquina dedicada o podrá seguir actuando como otra estación de trabajo más.

Gateways a IBMs 36/38

En la área de las minicomputadoras, sin lugar a dudas que alguna de las máquinas más comerciales son las del Sistema 36 de IBM, y en menor escala -- pero como equipo de mayor potencia -- es el Sistema 38.

A pesar de lo anterior, los *Gateways* para este tipo de equipos son mucho menos comunes, y de hecho, sólo existen cuatro o cinco fabricantes que hacen este tipo de *Gateways*.

La mayoría de los *Gatewaysde* este tipo, se deben conectar de forma remota, debido a que emulan una terminal 5251-12.

Es por ello que de parte del sistema 36 ó 38 debe existir la opción de comunicaciones (el Hardware y el Software necesarios para soportar teleproceso).

De forma similar a los *Gateways-3270's*, este tipo de *Gateways* permiten que a través de una sola línea, varias estaciones de la **RED** puedan accesar al equipo mayor. Sólo que en estos casos, el número máximo de sesiones puede ser de 8 ó 9 para los Gateways remotos, y solo cinco para los locales.

Por su forma de conectar, los locales utilizan el mismo cableado que las terminales 5251:twinax (coaxial doble) y los remotos, se conectan hacia un modem sincrónico a través del conector de la tarjeta *Gateway* (conector de 25 pastas:2b-25).

Comentarios Generales acerca de los Gateways

Aunque los *Gateways* son una solución ideal para muchos casos, tienen ciertas limitaciones inherentes a su forma de conexión, de igual forma que las tarjetas clásicas de emulación.

Cuando se desean transferencias continuas de archivos de volúmenes considerables, (arriba de 2 megabaytes) los tiempos de transmisión para pasarlo a la **RED** pueden ser considerablemente grandes; incluso se está hablando de horas.

Por otra parte, vale la pena comentar que los Gateways regularmente platican de "igual a igual" entre las estaciones de trabajo de la **RED** ("peer to peer"), lo cual significa que es el tipo de aplicaciones que NO NECESITA PASAR por el server para realizar sus funciones, a menos de que la tarjeta de Gateway haya sido instalada en el propio server, o de que se tenga una **RED** de tipo estrella.

Como base del Software estandar que permite el establecer una sesión de igual a igual en la **RED** es NETBIOS, la mayoría de los Gateways se anuncian como NETBIOS-compatibles.

Para quien haya trabajado un poco con NetWare de Novell, le podrá surgir la pregunta ¿pueden funcionar estos Gateways NETBIOS-compatibles bajo Novell-NetWare?

Exisiten dos posibles respuestas:

En general, la mayoría de los Gateways SI van a funcionar bien bajo Novell-NetWare pero antes de utilizar el Software del Gateway, hay que MONTAR el emulador del Netbios que Novell suministra.

La segunda respuesta es que si bien la mayoría de los Gateways están hechos sólo para Netbios, existen algunos pocos que pueden trabajar directamente para IPX.

La ventaja de estos últimos es que Netbios NO PUEDE TRABAJAR en ambientes de varias **REDES**, es decir cuando existen puentes o "bridges"; mientras que IPX soporta perfectamente este tipo de conexiones.

Otra ventaja es que IPX es más rápido -- en general -- que Netbios.

Gateways de CXI

- CXI posee Gateways/3270, permite remotos de 16 o 64 sesiones, y **LOCALES** tipo DFT (5 estaciones) y otro tipo llamado COAX-MUX, que se conecta a una interface 3299 de un controlador de terminales 3274 o 3174, y permite hasta 40 sesiones concurrentes en una **RED** vía Gateway local.

- En todos sus productos 3270 o 5251, permite realizar File Transfer sin problemas.

- En el modelo de Gateways/5251, es compatible con el PC Support 36 y 38, de forma que ya no se necesitan las utilerias de File Transfer.

- En los Gateways 3270, es posible a partir de agosto de 1987, escoger la opción SPX, para soportar el protocolo nativo de Novell:IPX, y así tener Gateways a través de varias **REDES**, y tener un mejor tiempo de respuesta

Es conveniente señalar que CIX corp. fabricante de estos tipos de Gateways es una compañía que fué fundada por Novell.

Gateways Asíncronos

Un Gateway Asíncrono consiste en una combinación de Hardware y Software, que permite a las estaciones de una **RED** compartir uno o varios modems.

Por ejemplo de un Gateway Asíncrono es el llamado por Novell ACS: Asynchronous communication Server. El ACS consta en Hardware de tarjetas WNIM, cada una de las cuales soporta la conexión de 4 modems. Se pueden tener hasta 3 tarjetas WNIM en equipo, totalizando 12 salidas a modems.

El ACS tiene dos funciones: Una de ellas es funcionar como Gateway Asíncrono, permitiendo que cada modem se conecte a líneas que van hacia una minicomputadora que posea capacidad de conexión asincronica RS-232, por ejemplo una VAX. (De hecho si el enlace hacia la mini se hace en forma **LOCAL**, no son necesarios los modems).

La otra función es permitir, a través de Software, que cualquier estación de trabajo utilice alguno de los modems disponibles, y "entre en sesión" con la minicomputadora, emulando una de sus terminales.

Adicionalmente, el ACS permite que se enlacen nodos remotos, usando los modems que se conectan al WNIM en la **RED LOCAL**, y para que dichos nodos remotos tengan tiempos de respuesta razonablemente rápidos, utiliza un Software adicional (anyware), que "esclaviza" una PC de la **RED LOCAL**, y la hace actuar como espejo de la remota: todos los comandos o instrucciones que se den en la PC remota, son duplicados en la **LOCAL**, y **SOLAMENTE** viajan por el modem los cambios en el monitor. De esta manera, es posible usar en forma remota prácticamente cualquier aplicación de la **RED**, teniendo respuestas casi iguales a las de una estación de trabajo **LOCAL**.

Puentes o "Bridges"

Un puente consiste en enlazar dos o más **REDES LOCALES**, de manera que a ojos del usuario, se forma una **RED** más grande.

Para formar un puente se requiere equipo (que puede ser el server o una estación de trabajo) que posea 2 tarjetas de **RED** (por lo menos), para enlazarse a cada una de las dos **REDES**. De hecho la **RED** 1 y la 2 pueden ser de muy diferente topología (por ejemplo Ethernet y Token Ring).

Además, el sistema operativo de la **RED** debe de tener la capacidad de permitir que la máquina "puente" reconozca las 2 tarjetas de **RED**, y configurarse de acuerdo a ellas.

Los puentes cubren tres necesidades básicas:

1.- Por una parte, permiten que **REDES LOCALES** ya instaladas sean unidas entre sí, este es el caso de la mayoría de los usuarios: ya se tienen 2 o más **REDES LOCALES**, resolviendo problemas de áreas específicas, típicamente departamentos dentro de una empresa. De esta forma, podríamos tener una **RED** en el departamento administrativo, otra **RED** en el departamento de Ingeniería, y a través de un puente, podemos lograr que ambas **REDES** se comuniquen, y que los usuarios en cada una de ellas, puedan accesar los recursos de ambas (claro respetando las seguridades y restricciones manejadas por el administrador de la **RED**).

2.- Por otro lado, cuando se decide aumentar los nodos de una **RED**, los puentes aseguran un mejor rendimiento que el crecer en una **RED** individual.

Supóngase, por ejemplo, que se tiene una **RED** de 12 nodos que se utiliza para aplicaciones administrativas, y que los tiempos de respuesta son perfectamente satisfactorios. Por crecimiento de la empresa, es necesario enlazar otros 10 nodos, ¿Qué conviene hacer? no importa que tipo de Hardware de **RED** se tenga, el que se esté satisfecho con 12 nodos, no es garantía de que con 22 se puedan seguir teniendo tiempos de respuesta satisfactorios lo que conviene hacer en esos casos, es establecer otra **RED**, que incluso puede tener el mimo server, en este caso dicho server tendría 2 tarjetas de **RED**, una para cada **RED**.

Tendencias

Tanto en los países industrializados como en el nuestro, es notable el incremento de **REDES LOCALES** de microcomputadoras, y la demanda creciente de su conectividad hacia otros ambientes.

Hasta hace algunos años, en México prácticamente ningún usuario pedía o tenía instalado un puente.

En los últimos meses de 1989, algunas empresas que se dedican a las **REDES LOCALES** aumentaron el número de **REDES** que desean crecer con puentes, o necesitan de enlaces hacía otros ambientes, y los proyectos para 1992 son muchas veces superiores en número.

Actualmente se existen ya algunos proyectos de 100 o más nodos para ser instalados en Empresas e Instituciones mexicanas y transnacionales durante 1991. Empieza a surgír un movimiento, apoyado por el mismo personal de sistemas, hacía estrategías de toda la empresa para estandarizar el uso de micros, popularizar la utilización de **REDES**, y uniformizar el Software que se adquiere.

BIBLIOGRAFIA

Libros:

Brooner, EG.
"The Local Area Network Book"
Howard Sams & Co; 1990

Durr Michael.
"Networking IBM PCs a Practical Guide"
Director, 1988

Archer, R.
"The Practical Guide to Local Area Networks"
Mc Graw Hill, 1989

Lehrman, S.R.
"Local Area Networking with Microcomputers"
(A Guide for the Business Decision-Maker)
Prentice Hall, 1988

Reiss.
"Introduction Local Area Networks with Microcomputers Experiments"
Prentice Hall, 1989

Teanenbaun, A.
"Computer Networks"
Prentice Hall, 1988

Ing. Juan F. Magaña C.
"La Microinformática y la Tendencia a las Redes"
Artículo Publicado

Memorias:

"PRIMER SIMPOSIUM DE REDES LOCALES Y CONECTIVIDAD"
Computadoras Micron S.A. y distribuidores.
Febrero 1988

"CURSO REDES LOCALES Y CONECTIVIDAD"
Comper S.A.
Marzo 1991

Revistas:

Lan-Times.
Editada por Novell Inc.
Varios Números

Pc-Magazine
Números: Julio 90 a Diciembre 91

SISTEMAS OPERATIVOS Y HARDWARE PARA REDES

INTRODUCCION

Este capítulo tratará sobre los conceptos del Sistema Operativo para una **RED** y sus funciones.

Por la importancia que han cobrado en el mercado internacional , se mencionan:

* **NetWare de Novell.**
* **LAN-Manager de Microsoft.**

Tambien se hará referencia a **IBM PC/LAN** como el primer Sistema Operativo para **REDES LOCALES** y por su penetración en el mercado se mencionará también a .

En la segunda parte del capítulo se tratarán los diversos elementos de Hardware de una **RED**, los principales tipos de tarjetas, las opciones en cuanto a tipo de cables, así como los tipos y características de los Servers.

Es saludable mencionar que parte de este material se apoyó y/o fué proporcionado por los fabricantes o representantes de los diferentes productos que aquí se conectan, y en las distintas notas que los observadores del medio escriben, por lo que es recomendable que se consideren con las reservas del caso, ya que los primeros por lógica, ubican sus productos como de lo mejor, y los segundos comentan según la corriente inductiva, contraria o imparcial en que se manejen.

Como el objeto es proporcionar al participante los marcos de comparación básicos, a efecto de que norme su criterio y pueda elegir los productos con más propiedad y conveniencia, según sus requerimientos particulares, y sin la idea de desmentir a nadie, dado el caso, se harán los comentarios que se consideren más prudentes. Sobre el particular, se abundará más adelante.

También se aclara que cuando se menciona el término de **RED**, este se refiere a una **RED DE MICROCOMPUTADORAS** entendida tal y como se definió en los capítulos anteriores.

Sistemas Operativos para RED

Se puede decir que el Sistema Operativo de una **RED**, es el conjunto de programas que regulan el funcionamiento de ésta, proporciona los elementos para la interface con el usuario, controla y define los niveles de seguridad, se controla como se comparten los recursos, etc.

Las funciones o tareas más importantes del Sistema Op

* **Compartir Recursos.**- De discos duros, y su programas. Para poder compartir archivos es nece sistema de bloqueo tanto de registros como de archi locking, respectivamente); que serán de sui desarrolladores de Software.

También debe controlar la forma de compartir ir mediante un manejo de colas de impresión residente

* **Niveles de Seguridad.**- El Sistema Operativo det necesario que otorgue y/o limite el uso de recurs jerarquía del mismo. Es decir, controlar los derech usuarios autorizados.

* **Facilidades Opcionales.**- Dependiendo de las nece la **RED**, las siguientes características serían altam mejor rendimiento de ésta :

- Declaración específica de usuarios y passwor
- Facilidades de comunicación para establecer p comunicación a equipos grandes, comunicacio a **RED** ó de **RED** a **RED**, etc.
- Sistema de mensajes o correo electrónico inteç
- Ayudas en líneas para facilidad de operación.
- Instrucciones por medio de menús.
- Integridad de la Información.- Garantía al información fue correctamente grabada, etc.

Conforme aumenta el nivel de aplicación de una **RED** empresa, también aumenta la dependencia hacia ella, confiabilidad en la misma, debe ser máximo. Esto indispensable que debe tener toda **RED**.

Por la importancia que tienen los Sistemas Operati conveniente ponderar las siguientes dos características comportan los mismos:

Sistema Operativo Servidor de Discos

Un sistema operativo servidor de discos, simplem operativo de la estación de trabajo (generalmente el D está accesado un disco compartido por la **RED**.

Sistema Operativo Servidor de Archivos

Un sistema operativo servidor de archivos, resuelve el problema de la administración de archivos en la **RED**, con un Software especializado.

Dicho Software servidor de archivos, administra el acceso al disco duro compartido y a la información que contiene. El Software de referencia, está desarrollado específicamente para **REDES** y construido a efecto de poder compartir archivos en un ambiente multiusuario. Entiéndase por multiusuario, la utilización de un mismo archivo por más de un usuario a la vez.

El almacenamiento de datos compartidos se controla por el Software del servidor de archivos, (El Server). Las estaciones no manejan sus propias entradas y salidas, sino que envían requerimientos de alto nivel al server y éste administra el acceso al disco. Debido a este control centralizado, los sistemas operativos servidores de archivos, brindan a la **RED** la integridad de datos como la dan las minicomputadoras y mainframes.

Todos los Sistemas Operativos, en la actualidad trabajan bajo el concepto de servidores de archivos, el cual es la evolución de los servidores de discos; el próximo paso, sobre el que actualmente se comienza a trabajar; son los *"Database-Server"* ó servidores de Bases de Datos, mismos que se tratarán en su momento.

Este cambio de Sistemas Operativos de servidores de disco a servidores de archivo, se pudo dar gracias a la aparición de la versión 3.1 del MS-DOS, que a diferencia de las versiones anteriores ya está orientado a soportar tareas de tipo multiusuario; este paso fué de suma importancia porque abrió el camino y sentó las bases para la definición de los estándares de **REDES LOCALES** que actualmente existen.

Los Estándares en REDES LOCALES

En 1984, la liberación del MS-DOS 3.1, el IBM-PC Network Program y Microsoft Networks, fueron definitivos para establecer los estándares más sólidos en la industria de las **REDES DE ÁREA LOCAL (LAN)** y el efecto ha sido bastante benéfico. Debido a que los estándares fueron implementados en base al Software, la lucha por la estandarización con base al Hardware para REDES LOCALES, ha desaparecido.

El sistema operativo de RED está ahora reconocido como el componente más importante de una RED.

MS-DOS 3.1

El MS-DOS 3.1 ha dado a los desarrolladores, un estandar en el cual ellos pueden generar Software para aplicaciones multiusuarios, que puedan correr a través de una variedad de **REDES LOCALES**. Este soporte ha seguido estandarizado con las versiones 4 y 5 de MS-DOS.

NETBIOS

NETBIOS (Network Basic Input Output System), sistema básico de entrada-salida para **RED**, es una interface que recide en la tarjeta de **RED**. Originalmente era un **"Firmware"** (Hardware-Software), actualmente ésta interface es exclusivamente Software.

IBM tenía que ser quien estableciera esta importante interface y lo hizo en su *"PC Network Program"* que acompaña al Hardware en su **RED LOCAL** *"PC Network IBM"*, también conocida como *IBM PC/LAN.*

Para ser compatible con IBM, una **RED** debe emular al **NETBIOS**, de la misma forma en que una computadora personal compatible con IBM, emula el **BIOS** de una IBM PC.

Las funciones principales del **NETBIOS** es establecer una liga virtual entre los usuarios en la **RED** y la transferencia de información en la misma.

La mayoria del Software de aplicación está escrito para MS-DOS 3.1. Sólo algunas de estas están escritas para NETBIOS, no obstante pocas resultan importantes, pues incluyen productos de conectividad, como **GATEWAYS** a mainframes. Este tipo de aplicaciones requiere la comunicación directa con el Hardware, y se logra a través del NETBIOS.

Objetivos de IBM en NETBIOS

Para el diseño global de la interface de **NETBIOS** y el *PC Network Program*, IBM al liberarla, publicó la siguiente lista de objetivos clave.

1.- La **RED** debe estar abierta para la industria y las interfaces clave, deben ser publicadas.
2.- La **RED** debe ser expandible.
3.- La **RED** no debe requerir de ningún tipo de **HOST** (equipo anfitrión), la comunicación debe ser de igual a igual.
4.- El Firmware de la **RED** deberá estar de acuerdo a los estándares de la industria, si es posible y deberá estar dividida en capas de protocolos.
5.- Las funciones de la **RED** deberán ejecutarse en la tarjeta de interface y la PC se encargará de la interacción de bajo nivel con la **RED.**

IBM ha seguido de cerca estos objetos. Por ejemplo. creando un emulador de NETBIOS para su **RED** Token Ring, donde pueda correr el *PC Network Program*.

La estrategia pone algunas limitaciones en las REDES, una de ellas estriba en que la comunicación punto a punto contemplada por NETBIOS, complica la formación de Inter-**REDES**, es decir, complica la habilidad de interconectar diferentes tipos de Hardware en una **RED**.

El NETBIOS fué escrito asumiendo que cada recurso en la **RED**, tiene un nombre propio y se le reconoce con él. De esta forma, cada nodo pasa a ser parte de una gran **RED**, conversión que dificulta el soporte a Inter-**REDES**.

MS-DOS 3.1

El MS-DOS 3.1 fué el catalizador que generó un cambio de importancia en los estándares de sistemas operativos para **RED**, ya que al principio, la mayoría de los fabricantes, utilizaban como estandar, el enfoque de *Servidores de Discos* (Disk Server) y actualmente, se ha adoptado como estandar, el concepto de *Servidor de Archivos* (File Server).

Este sistema operativo, el cual provee una interface estandar para aplicaciones multiusuario, requiere un ambiente de servidor de archivos. Para ser compatible con el estandar, los fabricantes de **REDES LOCALES** deben proveer Software de servidor de archivos compatible con MS-DOS 3.1.

Antes del DOS 3.1 la mayoría de los fabricantes usaban esquemas propietarios de bloqueo de archivos y registros, requiriendo que los desarrolladores de Software de aplicación, escribieran una versión diferente para cada **RED**, en la cual querían que su Software operara.

Ya que desde 1983, cerca de 140,000 aplicaciones de Software han sido escritas para el estandar MS-DOS de Microsoft, es racional aprovechar lo aplicable a **REDES**.

Diferentes productos de **RED** (bastantes), han crecido soportando al Hardware y Software de MS-DOS. Pero la habilidad de conectar máquinas para DOS, es la única cuestión en común que tienen diferentes **REDES**. La falta de un estandar forzó a cada fabricante de **REDES** a seguir su propio conjunto de reglas. Esta falla de estándares creo muchos problemas, el más serio de ellos es que dicha falla, inhibió el desarrollo de Software de aplicación multiusuario para **REDES**.

Antes del MS-DOS 3.1, cada fabricante de **REDES** tendía a utilizar sus propias técnicas de bloqueo, de registros, archivos y funciones multiusuarias. Esto requería que los desarrolladores de Software de aplicación tuvieran que escribir versiones diferentes de sus paquetes para cada **RED LOCAL**. Los gastos que esto implica alejó a muchas empresas del desarrollo de productos para **RED**.

La introducción del DOS 3.1 cambió esta situación ya que fué mejorado con los primitivos del multiusuario que controlan el acceso entre la aplicación y la **RED**, brindando la interface estandar que se necesitaba.

Cualquier paquete de Software multiusuario escrito con los estándares del DOS 3.1 correrá en cualquier **RED** que soporte esta versión de DOS, permitiendo una sola versión de Software para todas las **REDES** compatibles con DOS.

A partir de esta estandarización, la mayoría de las empresas de Software han introducido sus productos en versiones multiusuario para **REDES**.

Otro cambio importante ha surgido con *Windows 3.0* y proximamente con *Windows PM*, donde según los observadores de la indusrtia darán otro giro importante a las **REDES LOCALES** con sus aplicaciones y nuevas estrategias de conectividad.

Actualmente *Windows 3.0* se está perfilando como el nuevo estandar en la industria microinformática tanto a nivel PCs como de **REDES LOCALES.**

Implementaciones de Microsoft Network (MS-NET)

Microsoft liberó a principios de 1985 su producto Microsoft de soportar el sistema. En la actualidad, hay cuatro corporaciones de EE.UU., que están enviando implementaciones *MS-Net, IBM, AT&T, 3COM y URGEMANN-BASS.* En México, Computadoras Micron también ofrece este producto.

La versión de IBM se conoce como el *"PC Network Program"* más conocido como *"IBM-PC/LAN"* la implementación de *3Com* se conoce como *"3+"*. *AT&T* está usando la implementación del Software *"3+"*. *Ungermann-Bass* y Computadoras Micron están usando y enviando una implementación pura del *Ms-Net*. De acuerdo a sus estudios de Future Computing, hay aproximadamente 50,000 nodos instalados (hasta mediados de 1986) de *MS-Net* en todo tipo de implementaciones.

NetWare de Novell

De acuerdo al mencionado estudio de Future Computing, hay cerca de 300,000 estaciones de trabajo utilizando el sistema operativo NetWare de Novell. Existen varias razones para esta gran diferencia. NetWare ha sido distribuido desde 1983 y recientemente, IBM fué el único proveedor enviado una implementación de *MS-Net* el *PC-Network Program.*
Hasta la fecha, 23 proveedores han obtenido licencia para usar NetWare como el sistema operativo de **RED** para su Hardware, debido a su excelente tiempo de respuesta, permanencia en el mercado, soporte múltiple de **REDES** y servidores y la gran base de usuarios, actual, que tiene instalada.

Nueva Generación de Características de Software de RED

A continuación se mencionan las nuevas carcterísticas que tienden a ofrecer y desarrollar, los sistemas de **RED LOCAL.**

- **Interconexión de REDES LOCALES**

  La interconexión de **REDES LOCALES**, es la habilidad de "puentear" entre diferente Hardware de RED, para formar una RED transparente o inter-

Debido a que no hay estándares de Hardware, **REDES** diferentes pueden formar parte de una inter--**RED**. Lo anterior hace importante la habilidad de interconectar sistemas diferentes.

La llave para esta interconexión es la independencia del Hardware en los sistemas operativos de **RED**, y ayuda también a evitar la obsolencia del Hardware de **REDES LOCALES**.

*** Modo Protegido de Operación**

El microprocesador Intel 80286, el cual se utiliza en la IBM AT y sus compatibles, puede operar en dos modos: **Protegido y Real.**

En el modo Real, el chip emula al 8088 pero con una mayor velocidad, permitiéndole correr MS-DOS y Software de aplicación compatible. A semejanza con el 8088, el 80286 en modo real, está limitado a 640 Kb. de memoria y 70 Mb. de almacenamiento en disco; el único beneficio de este modo, es sólo una velocidad más rápida de procesamiento.

Mientras el Software de aplicación se modifica para romper esta barrera, con la especificación de memoria expandida de Lotus-Intel-Microsoft (LIM-EMS), los sistemas operativos de **RED** corriendo en modo real, están limitados a 640 Kb. en la memoria del servidor.

En el modo Protegido, el 80286 puede direccionar hasta 16 Mb. de memoria en algunos casos y esta operación permite mejorar significativamente la eficiencia del servidor compatible con IBM-AT.

Puede manejar en memoria virtual hasta 2 Gigabytes. (falta que existan los dispositivos físicos de estas magnitudes).

*** Disponibilidad e Integridad de Datos**

La disponibilidad e integridad del sistema es importante en cualquier instalación, pero tan pronto como las **REDES LOCALES** se mueven a un ambiente de procesamiento de datos cada vez más demandante, estas características se hacen aún más críticas, debido a la creciente dependencia y a que las pérdidas incurridas por una falla del sistema, crecen también.

Una **RED** debe incluir protección contra estas fallas, que causan pérdida de datos, tiempo, tiempo fuera del sistema o ambos.

Las protecciones que un sistema operativo de **RED** debe tomar en cuenta son las siguientes: Falla del sistema, Falla del medio magnético y corrupción de datos.

A continuación, se comentarán las principales características de sistemas operativos para **RED**.

3.1 NETWARE DE NOVELL

Descripción general

Novell Advanced NetWare es un sistema operativo de **RED** independiente del Hardware, por lo cual puede correr en una gran variedad de **REDES**. Ha estado en el mercado desde 1983 y es el sistema operativo ampliamente más usado.

Novell desarrolló originalmente el NetWare como el sistema operativo para el equipo Novell-S Net. Una **RED** que utiliza una topología de estrella y un servidor propietario basado en el microprocesador Motorola MC 68000. Debido a que este microprocesador no tenía ningún sistema operativo estandar, Novell decidió desarrollar el suyo partiendo de cero, y lo optimizó para **REDES**; diseñando de paso todas sus características , alrededor de la funcionalidad de la **RED**. Novell es una compañía norteamericana la cual fabrica el sistema operativo para **REDES** (LANs) más popular; "NETWARE".

Introducido por primera vez en el mercado en 1983 NetWare de Novell es el sistema operativo para **REDES** más conocido en el mercado. NetWare de Novell tiene una base instalada sobre 7 millones de usuarios, 700,000 NetWares vendidos y el mayor porcentaje del mercado compartido de **REDES**.(Fig.3)

Estadísticas realizadas por Fortune en 1991 nos muestran que Novell tiene la mayor base instalada en Sistema Operativo (Fig.1) para **RED** (LANs) y las perspectivas para 1992 son incrementar el porcentaje de esa base instalada (Fig.2).

La estrategia que Novell ha seguido para sus sistema operativo es:

* Independencia de Interfaz.
* Independencia de Protocolo.
* Independencia de S.O. de la estación de trabajo.
* Ser el Estandar de Estándares del futuro.

Cuando comenzó el éxito de las PCs, los autores de NetWare, viendo que este Software está escrito con C, podría fácilmente convertirse a la arquitectura de la familia Intel 8088 y que podría soportar virtualmente cualquier **RED** en el mercado; debido a que el ROM BIOS de la IBM PC XT, fue diseñado para un sistema operativo (DOS) de un solo usuario, con la deficiencia para ambiente multiusuario ya que el NetWare es particularmente multiusuario, los programadores de NetWare decidieron ignorar el ROM BIOS y decidieron comunicarse directamente con el Hardware, para eliminar efectivamente cualquier limitación.

Lograron con ello, permitir a NetWare procesar requerimientos de otra estación de trabajo.

La única desventaja de esta forma de operar, es la imposibilidad de NetWare de utilizar las interfaces (drivers) del DOS, para disco duro. Novell surte estas interfaces para discos compatibles con IBM y muchos fabricantes surten sus propios drivers para NetWare.

NetWare prácticamente no tiene interface, como el ROM BIOS o el DOS cuando se utiliza como servidor de archivos, lo cual permite una mayor de velocidad y un mayor grado de seguridad y tolerancia a las fallas. Esto resultaría imposible si se utilizara la estructura de archivos de **DOS**.

Componentes y Arquitectura

NetWare utiliza cuatro componentes mayores de Software:

* El sistema operativo huésped (DOS).
* La interface "SHELL" con DOS.
* El Software del servicio de archivos.
* Las utilerías de la **RED**.

El sistema operativo huésped que corre en la estación de trabajo, puede ser cualquier versión de MS-DOS a partir de la 2.0 en adelante.

El ***"SHELL"*** de NetWare provee también en la estación de trabajo, la liga de comunicación entre la estación y/o aplicación y el Software del Servidor de Archivos.

Este ***"SHELL"*** ofrece además, la compatibilidad del NetWare con el DOS y utiliza todas las interfaces estandar establecias por MS-DOS 3.1 y NETBIOS. Si la aplicación requiere un servicio de Netbios, se puede comunicar directamente con el emulador de éste, mismo que pasará la información al IPX.

Por otro lado si la llamada es LOCAL, el ***"SHELL"*** la transfiere al DOS para que este la ejecute. De lo contrario la llamada es pasada a algunas de las implementaciones de *MS-Net*.

El Software de servidor de archivos de NetWare no se corre como una aplicación de DOS en la máquina servidora de la **RED**.

El ***"SHELL"*** también permite a NetWare poder operar con las versiones MS-DOS 2.0 en adelante y no solo 3.0 ó mayor, como es el caso de *MS-Net*.

El Software de Servidor de Archivos de NetWare está diseñado específicamente para **REDES** y es multiusuario, lo que significa que una tarea no tiene que esperar hasta terminar, para iniciar otra. A las diferentes tareas se les asigna distintos niveles de prioridad, a efecto de realizar rápidamente lo de mayor importancia.

En el caso de la operación de un servidor de archivos *NO DEDICADO*, el DOS corre en el server, como una tarea del sistema operativo de **RED**.

La importancia de los estándares establecidos por IBM y Microsoft, ha sido mostrada en las secciones anteriores de este material. Novell provee compatibilidad completa con estos estándares en su producto Advanced NetWare 2.0a.

NetWare es compatible con DOS y en Advanced NetWare 2.0a agregó compatibilidad completa con DOS 3.1. Advanced NetWare, además también brinda compatibilidad con versiones 2.0 en adelante y reduce al costo de actualización a nuevas versiones del mismo. Se acota que, mientras el DOS 3.1 es requerido por algunas aplicaciones multiusuarios, el DOS 2.1 utiliza menos memoria y tiene un tiempo de ejecución más rápido.

El Advanced NetWare 2.0a también provee un 100% de compatibilidad con NETBIOS mediante el emulador que posee. Esto garantiza compatibilidad con los adaptadores de **RED**, tales como Token-Ring y Pc Network. El emulador de NETBIOS también brinda operación en modo protegido.

Hardware Soportado

El Advanced NetWare 2.0a viene con drivers para 14 diferentes adaptadores de **RED**. Estos 14 drivers permiten hasta 35 diferentes configuraciones de Hardware. Una lista de los drivers incluidos en el paquete es:

* 3Com Etherlink.
* A&T Starlan.
* Corvus Omninet.
* IBM PC Cluster.
* IBM Token Ring.
* Novell S-Net.
* Standard Microsystems ARCNET
* 3Com Etherlink Plus.
* Allen Bradley Vista LAN/PC.
* Gateway G-Net.
* IBM PV.C Network.
* Nestar Plan 2000.
* Orchid PC-Net.
* Proteon ProNET.

Interconexiones de **REDES**

NetWare provee capacidades extensivas para la formación de Inter-**REDES**. El punto interno de NetWare que viene incluido en Advanced NetWare 2.0a, le permite a un server soportar simultáneamente hasta 4 diferentes topologías, sin tener que dejarlo con dedicado, es decir, que éste podrá procesar otros trabajos simultáneamente; NetWare soporta varios servidores de archivos y cada servidor puede actuar como un puente. También se soportan puentes externos múltiples.

Seguridad

La seguridad de NetWare se basa en el manejo de USUARIOS autorizados. El supervisor de la **RED** establece derechos a un usuario autorizado y le asigna recursos específicos de la **RED**.

Dichos recursos pueden ser en Hardware: impresoras y servidores, y en Software: programas y archivos de datos localizados en directorios y subdirectorios.

Los privilegios de acceso de un usuario a las áreas de directorios pueden ser asignadas de acuerdo a ocho derechos:

R- Lectura.
W- Escritura.
O- Apertura de archivos.
C- Creación de archivos.
D- Borrado de archivos.
P- Parental (Controlar y crear subdirectorios).
S- Búsqueda (Poder ver archivos en directorios).
M- Modificación (De atributos de archivos).

Además de la seguridad ofrecida por los derechos del usuario, la seguridad a nivel de archivo también puede definirse con atributos, ya que los archivos pueden marcarse como compartidos, no compartidos, de lectura solamente o de lectura y escritura.

Usando este tipo de seguridades, una persona hace un "LOGIN" a la **RED** mediante un nombre de usuario y un password. Una vez que esta entrada se ha completado, la persona tiene acceso transparente a todos los recursos actualizados para él.

Operación en Modo Protegido

Los usuarios de NetWare pueden hacer uso de toda la capacidad del microprocesador Intel 80286 cuando utiliza una IBM AT o compatible, permitiéndole al servidor de la **RED**, utilizar hasta 16 MB. de memoria y hasta 2 GB. (Gigabytes) de almacenamiento en disco.

Sistema de Archivos

El sistema de archivos está diseñado específicaamente para la administración de **REDES** y no tiene las limitaciones de los archivos del DOS, aunque es completamente compatible con él.

NetWare tiene su propia estructura de manejo de archivos (plana), que se conserva en memoria y en disco (con doble copia), e implementa cuatro características adicionales, que hacen que funcione rápidamente en el manejo de archivos.

a) Directory Caching
b) Directory Hashing
c) File Caching
d) Elevator Seeking

Disponibilidad e Integridad de Datos

El sistema de archivos de NetWare utiliza varias medidas preventivas para asegurar la disponibilidad e integridad de los datos, a saber:

* Verificación de lectura después de escritura, sin excepción cada escritura al disco se lee nuevamente verificando que sea leído.

* Duplicidad de directorios, si un directorio falla el duplicado se utiliza.

* Tablas duplicadas de alojamiento de archivos (FAT), esto prevee que la contaminación del FAT provoque un disco inutilizado.

SFT NetWare

Novell también ofrece una actualización para Advanced NetWare que brinda protección adicional a los datos. Estas versiones mejoradas del sistema operativo, se conocen System Fault Tolerant NetWare (SFT) (Sistema Tolerante de Fallas).

Hay tres niveles de implementación del SFT:

NIVEL I.-Permite detectar bloques dañados del disco en la operación normal del sistema. Estos bloques son marcados para evitar su uso futuro. La información contenida en ellos pasa a otras localizaciones de disco.

NIVEL II.-Este nivel permite mantener discos en *"Espejo"*, es decir que se tiene en todo momento un disco de respaldo actualizado totalmente, a fin de evitar pérdidas de información en caso de una falla del disco original.

También se cuenta con la posibilidad de tener discos *"Duplicados"*. Estos discos son espejos entre si, pero además se cuenta con duplicados de controladores de disco, cables y fuente de poder.

NIVEL III.- En este nivel se tienen dos servidores de archivos como respaldo uno del otro, conectados entre si con un bus de transferencia de alta velocidad.

Hasta antes de 1988, prácticamente todas las versiones de NetWare de Novell que se tenían, estaban pensadas para **REDES** grandes o medianas; pero a partir de enero de 1988, se liberó la versión *ELS (Entry Level Solution)* para **REDES** pequeñas, y en 1991 se liberan nuevas versiones:

- NetWare 2.20 con licencias para 5, 10, 50 y 100 usuarios
- NetWare 3.11 para 10, 20, 100 y 250 usuarios
- NetWare Lite para aplicaciones pequeñas.

En seguida se resumirán los puntos más importantes de cada versión y se darán algunas recomendaciones sobre el número de estaciones de trabajo que debe tener cada versión, para obtener el mayor rendimiento de la **RED**.

No obstante cada caso será diferente, por lo que habrá que tomar en cuenta si el tráfico en la **RED** es muy ligero o muy pesado, con lo cual las cifras podrán tomarse con un poco más de holgura.

Características Principales de NetWare

I.- Soporta todos los comandos de DOS lo cual es una ventaja para los usuarios de las PCs, ya que no tienen que apernder comandos nuevos. Trabajar en **RED** para ellos es completamente transparente.

II.- Tiene sus propios comandos los cuales tendrán que ser manejados por un administrador ó Supervisor del sistema para optimizar, y controlar la funcionalidad de la **RED**. Estos comandos pueden ser fácilmente manejados por medio de Menus.

III.- Optimización del acceso a disco duro.

a) Directory Caching: Es el proceso de almacenar en memoria RAM las tablas de direcciones de los archivos (F.A.T). De esta manera cuando existe una requisición de algún archivo el servidor no lee estas tablas del disco duro sino en RAM para encontrar las direcciones de los archivos requeridos.

Las estaciones de trabajo de la **RED** pueden leer o escribir hasta 100 veces más rápido de lo que serían si leyeran las tablas F.A.T. directamente del disco duro.

b) Directory Hashing : Es el proceso de indexar F.A.T. Esto permite al servidor encontrar las direcciones correctas sin examinar todos los datos de las tablas, la ventaja que esto ofrece es la disminución del tiempo de acceso a un archivo hasta en un 30% en comparación con las tablas F.A.T. no indexadas.

c) File Caching : Es el proceso en el cual se almacenan en memoria RAM los archivos que se usan con mayor frecuencia.

Cuando se hace la penetración de un archivo este se baja a memoria RAM donde es almacenado para subsecuentes peticiones.

El servidor realiza una serie de estadísticas sobre cuáles son los archivos que son solicitados con más frecuencia y estos son bajados a memoria RAM. Las subsecuentes peticiones del mismo archivo son atendidas hasta 100 veces más rápido que cuando el archivo no esta en RAM.

d) Elevator Seeking : Es el proceso por medio del cual los requerimientos de entrada y salida de información del disco duro están ordenados de acuerdo con la posición física de las cabezas del disco. Esta característica ofrece mayor velocidad de acceso y mayor duración de los discos duros.

IV.- Alta seguridad: NetWare permite al Supervisor de la **RED** configurar los niveles de seguridad de ésta. Estos pueden ser tan simples o sofisticados como se desee. La seguridad que proporciona NetWare está definida en 4 niveles: Clave de acceso, derechos de usuario, derechos de directorios y atributos de los archivos.

En sistemas con gran cantidad de usuarios es muy importante cuidar al máximo la integridad de la información que se maneja en éste.

a).- Clave de acceso (Log-Password Security). Es el primer nivel de seguridad en el que para poder entrar al sistema se tiene que especificar un nombre de usuario y una clave de acceso asignados previamente por el Supervisor del sistema.

b).- Derechos de Usuario (Trustee Rights Security). Controla la habilidad individual de los usuarios para trabajar con archivos en determinados directorios. Para hacer esto contamos con 8 derechos de usuario que son:

R - Leer archivos **W**- Escribir archivos
O - Abrir Archivos **C** - Crear archivos
D - Borrar archivos **M** - Modificar atributos de archivo
P - Parental (Crear, Renombrar, Borrar directorios. Asignar Derechos)
S - Buscar directorio

c).- Derechos de Directorios (Directory Security). Controla los derechos que todos los usuarios tienen asignados con excepción del Supervisor en un directorio dado. Cuando un directorio es creado tiene los mismos derechos que son aplicados a los derechos de usuario (**R, W, O, C, D, P, S, M**), para poner en efecto seguridad a un directorio dado el Supervisor borrará de éste los derechos necesarios para prevenir el uso indebido de los archivos que éste contenga. Los derechos de directorio tienen mayor jerarquía que los de usuario y no se extienden a subdirectorios.

d).- Atributos de los archivos (File Attributes Security). Controla si un archivo individual puede ser compartido o modificado. Particularmente ayuda para proteger archivos de información pública leidos por muchos usuarios. Los atributos son:

Compartido -- Shareable
No Compartido -- Non Shareable
Solo lectura -- Read Only
Lectura/Escritura-- Read Write

V.- Correo Electrónico : NetWare incluye un paquete de correo electrónico sin costo adicional en el cual se puede mandar desde sencillos mensajes hasta complejos memorándums a cualquier usuario de la **RED** gracias a su editor de textos integrados.

VI.- Independencia de protocolo y Hardware. Nos permite tener sistemas heterogéneos interoperables debido a la independencia de protocolo y Hardware así podemos tener un sistema tan complejo que tenga PC's IBM, Macintoshs, PS/2, compatibles y Host (Mainframes y minis) corriendo *DOS, OS/2 MAC, VMS,UNIX,* etc. , con diferentes tipos de interfaces, ETHERNET, ARCNET, TOKEN RING, etc. NetWare soporta más de 100 tarjetas de interface en el mercado. (Fig.4).

VII.- Comunicaciones Remotas y Gateways : NetWare nos permite tanto comunicaciones locales como remotas a través de los Gateways, así podemos tener una **RED REMOTA** a través de un Puente (Bridge) o un mainframe, por medio de un protocolo X-25 o mediante un Gateway SNA a un sistema IBM 43 XX etc. Gateway es una función que permite que varias PCs en una **RED** pueden tener comunicación con un Host (maiframe-mini), a través de ellas emulando terminales del Host (Fig.5).

Versiones de NetWare

Advanced NetWare 86 V2.0

Un sistema operativo diseñado para trabajar con microcomputadoras construídas con microprocesador 8086 u 8088 compatibles con las IBM'S PC XT.

Características *Novell Advanced NetWare 86 V2.0*

* Soporta hasta 100 estaciones de trabajo.
* 160 MB de almacenamiento en disco duro.
* 5 impresoras compartidas.
* 640KB de memoria en el file server.

Advanced NetWare 286 V.2 OA.

Un sistema operativo diseñado para trabajar con microcomputadoras construídas con microprocesador 80286 en el cual se aprovechan características como el direccionamiento de memoria virtual trabajando en el modo protegido.

Características *Novell Advanced NetWare 286 V2.0a*

* Soporta hasta 100 estaciones de trabajo.
* 15000 MB de almacenamiento en disco duro.
* 3 impresoras compartidas.
* 16 MB de memoria RAM el file server.
* Mayor velocidad de procesamiento de datos.
* Existe en versiones dedicada y no-dedicada.

Entry Level Solution Nivel I (SFT I) ELS I.

Es un sistema operativo Advanced NetWare 286 V2.OA preconfigurado a 4 usuarios.

Características *Novell ELS I NetWare SFT I*

* Soporta hasta 4 estaciones de trabajo.
* Tiene las mismas características del 286 V2.OA.
* Características adicionales.
* Protección de datos contra defectos en la superficie del disco
* HotFix
* Read after write verification.

Hot Fix. Es una característica de NetWare que previene la escritura de datos sobre sectores dañados en el disco. Cuando el *Hot Fix* es activado sobre el disco duro, crea una área de redirección (aproximadamente el 2% de la capacidad total del disco) donde serán redirigidos los datos cuando es encontrado un sector dañado en el disco. (Fig 6).

Read After Write Verification. Cuando un dato es escrito sobre el disco duro inmediatamente se ejecuta una lectura a memoria para comparar la integridad del dato escrito. Si esta comparación es exitosa se libera la localidad de memoria y se ejecuta otra operación. Si la comparación no es exitosa después de varios intentos, el dato es enviado por el *Hot Fix* a la área de redirección y el sector es marcado como dañado y enviado a la tabla de defectos del disco. (Fig 6).

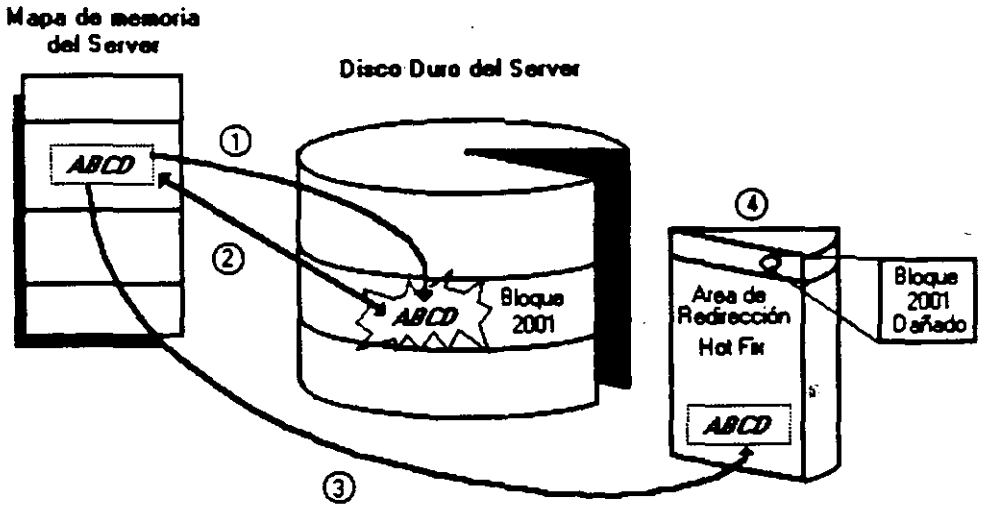


Fig.6 Hot Fix
Read After Write Verification

Entry Level Solution II

Características ***Novell ELS II NetWare***

- Es el segundo nivel del ELS I.
- Sistema Operativo 286 V2.12 preconfigurado a 8 usuarios.
- Soporta hasta 8 usuarios.
- Mismas características de la versión 2.12.

Advanced NetWare 286 V2.1X (2.11, 2.12)

Características ***Novell Advanced NetWare 286 V2.1X***

- Mismas características de la versión 286 V.2 OA.
- UPS Monitoring.
- Hot Fix.
- Read after write verification.
- Manejo en capacidad de disco 2 GB
- Soporta 5 impresoras, 2 seriales, 3 paralelas.
- Soporta 5 canales para disco.
- Hasta treinta y dos discos.
- Duplicado de Directorio.
- Duplicado de FAT.
- Soporta hasta 100 usuarios.
- Maneja una consola virtual (Fconsole).
- Value added process VAP'S.- Accounting.
- Manejo de cola de impresión por menu (Pconsole).
- Dedicado y No-dedicado.
- Maneja Rutinas de Diagnóstico

Recomendaciones:

* De 6 a 15 estaciones--Usar AT con disco rápido y 2 Mbytes de memoria.
* De 16 a 25 estaciones--Usar AT con disco rápidos y mas de 2 Mbytes de memoria.
* Más de 25 estaciones o más de 20 con trabajo pesado usar Server 386 con más de 2.5 Mbytes de memoria.
* Más de 40 estaciones o de 25 con trabajo pesado dividir en dos REDES usando un puente.

Advanced NetWare 286 V2.15

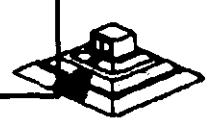
Características ***Novell Advanced NetWare 286 V2.15***

- Mismas características 286 V2.12.
- Soporta la interfase para estaciones de trabajo Macintosh.

NetWare SFT 286 V2.1 X (2.11, 2.12)

Características ***Novell Advanced NetWare SFT 286 V2.1X***

- Es un sistema tolerante a fallas de disco duro.
- Disk Mirroring. - Disk Duplexing.
- TTS. - Dedicado
- Mismas características 286V2.12.0.



NetWare SFT 286 V2.15

Características *Novell Advanced NetWare SFT 286 V2.15*

- Mismas características SFT V2.12.
- Soporta la interfase para estaciones de trabajo Macintosh.
- Soporte a OS/2.

Rutinas de Diagnóstico

Están incluidas en el paquete, rutinas que cuentan con funciones intrínsecas para facilitar el diágnostico para **REDES** realmente grandes, (imáginese una **RED** de más de 200 nodos, con 5 o 10 puentes).

UPS Monitoring : UPS (NO-Break) es una fuente de poder ininterrumpible la cual proporcionará al servidor de archivos y a cualquier unidad de discos externos energía a través de un sistema de baterías en caso de una interrupción en la alimentación de energía comercial. El UPS monitoring es una función de control de Advanced NetWare 286 la cual dará de baja el Servidor de archivos si la alimentación de energía comercial no se restablece en una cantidad de tiempo predeterminada.

VAPs : Procesos de valor agregado, es una herramienta que permite a los desarrolladores de Software crear aplicaciones que puedan ser ejecutadas dentro del servidor de archivos. En las versiones anteriores de sistema el único proceso que podía correr en el servidor de archivos era el sistema operativo. El UPS monitoring es un ejemplo de VAP.

Accounting : Es una nueva característica del Advanced NetWare 2.1 que nos permite hacer cargos por el uso de los recursos de la **RED**. Los cargos pueden variar por hora o por día. El Supervisor puede asignar límite de credito y hacer que el sistema monitor de usuarios haga un balance de cuenta y saque del sistema a los usuarios que han sobrepasado su límite de crédito.

- Poner un límite de crédito a cada usuario.
- Monitorear el estado de cuenta de cada usuario..
- Generar una estadística del uso del sistema.

Los cargos por uso del sistema pueden hacerse por:

- Tiempo de conexión al sistema.
- La cantidad de tiempo que el usuario está dentro del sistema.
- La cantidad de datos (programas/información) que el usuario requiere, que el servidor de archivos lea desde su disco.
- La cantidad de datos (programas y/o información) que el usuario requiere que el servidor de archivos escriba sobre su disco.
- El número de accesos que el usuario hace al file server.
- La cantidad de espacio en disco usada.
- Los cargos se hacen cada 1/2 hora.

Incrementa la Seguridad del Sistema

- Restringe el horario de acceso al sistema a cada usuario.
- Restringe por estación de trabajo el acceso al sistema.
- Restringe el número de conecciones concurrentes por usuario.
- Monitor de detección de intrusos al sistema bloqueando la estación de trabajo por la cual se quiere accesar al sistema.

FConsole

Es una utilería del sistema operativo la cual crea una consola virtual que puede ser ejecutada por cualquier estación de trabajo en la **RED**. Permite controlar la mayoría de los recursos de la **RED**. Cualquier usuario de la **RED** puede usar *FConsole* para accesar diferentes servidores de archivo, ver información de los *LAN-DRIVERS* y ver la versión de sistema operativo sobre la cual se está trabajando.

El Supervisor puede usar *FConsole* para enviar mensajes, revisar archivos, analizar información de conexión de los usuarios, alterar el status del servidor de archivos, ver las estadísticas del funcionamiento del servidor de archivos. También puede dar de baja el servidor de archivos y borrar la conexión de cualquier usuario.

FConsole Es una utilería del Sistema Operativo que nos permite controlar la cola de impresión, con esta utilería se puede crear, nombrar y borrar una cola de impresión.

Spool

Cuando se ejecuta un comando de impresión, los datos a ser impresos serán enviados a una cola de impresión en el disco duro antes de ser dirigidos a la impresora, la cola de impresión mantiene los datos hasta que la impresora está lista.

Disk Mirroring

Una falla mecánica de disco duro puede significar una total y permanente perdida de datos almacenados sobre el disco duro. SFT NetWare proporciona protección contra falla de disco duro permitiendo tener duplicado de información de un primer disco sobre un segundo disco en el sistema. Esta característica llamada *DISCO EN ESPEJO*, nos permite tener dos discos juntos en el mismo canal, los datos son escritos al disco primario y duplicados sobre el disco secundario con lo cual siempre se tiene respaldo de datos. Si alguno de los dos discos llegara a fallar un mensaje de precaución aparecería en las estaciones de trabajo indicando la falla (Fig. 7).

Disk Duplexing

Debido a que los discos en espejo solo protegen datos contra falla de disco duro y no contra falla de controlador, SFT NETWARE, tiene otra característica que se llama *Disk Duplexing* que permite tener respaldo de datos en dos discos conectados a diferente controlador (Fig.8).

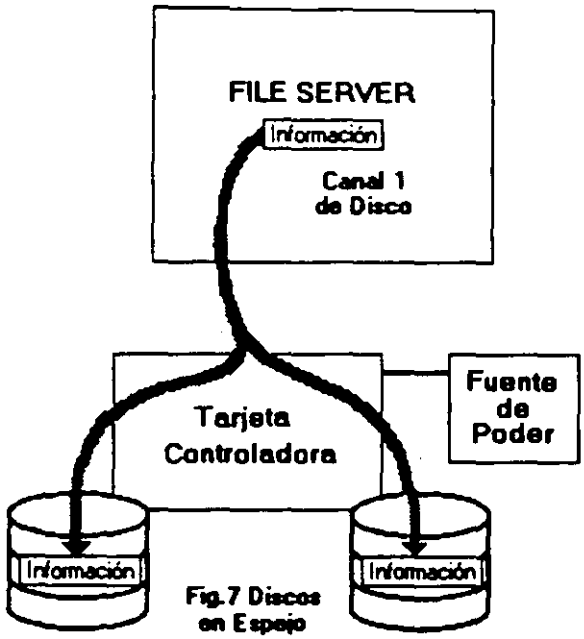


Fig.7 Discos en Espejo

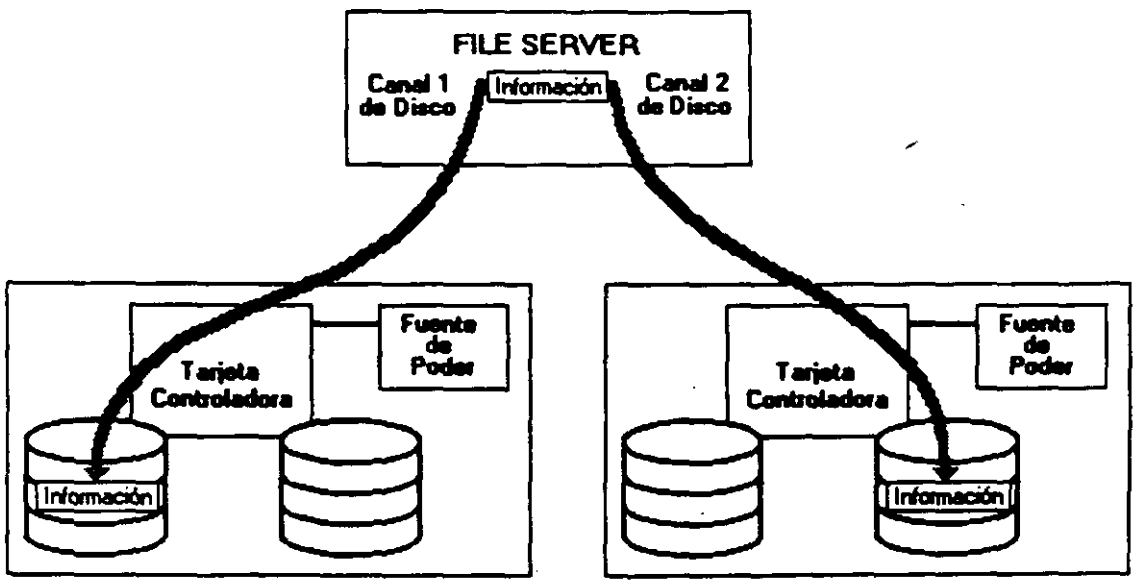


Fig.8 Discos Duplicados

TTS.- Transaction Tracking System

Esta característica previene corrupción en bases de datos, si el sistema falla mientras se esta haciendo una transacción.

En una transacción los datos no son escritos sobre la base de datos hasta que la transacción se termina si una falla ocurre antes de que la transacción termine los datos no son escritos y permanecen en su estado original con lo cual la información en la base de datos es consistente; por ejemplo:

Cuando desde un programa se actualizan varios archivos, ya sea que esté hecho en Pascal, Cobol, Open Access, Dbase III, etc., existe un problema potencial: ¿Qué pasa, si cuando todavía no se han terminado de actualizar todos los archivos, sucede algún imprevisto (se fué la corriente, alguién apagó el server, se desconectó la **RED**, etc.), por lo que algunos archivos se quedaron abiertos y no complementaron su actualización, mientras otros si acabaron el proceso?.

Normalmente lo que se hace en una microcomputadora es, o hacer un programa que "revise" el estado de los archivos y nos avise si existen diferenciales, o hacer el proceso a anos; o bien, no hacer ninguno de los dos y atenernos a las consecuencias. *TTS* está orientado a prevenir y en su caso resolver esos problemas.

Si los archivos que se van a actualizar por los programas, los definimos como tipo "T" (bajo ambiente Novell-NetWare y suponiendo que tenemos *TTS*), entonces *TTS* se encarga de vigilar que cuando comience un bloque de actualizaciones (transacciones), éste se realice completamente.

Si algo pasara el server se re-encienda, *TTS* revisa un bloque de actualizaciones, y si no se realizó en su totalidad, le da marcha atrás (roll-back) a todo lo que estaba a "medio-terminar", quedando los archivos como estaban antes de empezar dicha actualización. Hasta antes de *TTS* este tipo de manejo de transacciones, sólo se tenían en computadoras mucho mayores.

Realmente la manera en que *TTS* se entera de que empieza una transacción, es porque el lenguaje con el que trabajamos soporta las instrucciones: Begin Transaction y End Transaction (llamadas explícitas), o porque *TTS* detecta el primer record locking a un archivo tipo "T" y comienza la transacción y termina cuando se encuentra el unlock correspondiente del primer registro marcado con el record loking.

Entre los ambientes que son compatibles con *TTS* están entre otros: Dbase-III Plus, QuickSilver, Turbo-C, Turbo-Pascal (versión 4.0), B-trive y en general cualquier ambiente que tenga la capacidad de record locking.

Soporte a OS/ 2

La versión 2.1 es el primer sistema operativo para RED, que puede ser usado para un nuevo OS/2 de Microsoft e IBM.

Para poder relizarlo existen dos formas básicas: bajo la primera, las estaciones de trabajo están en OS/2 (de hecho unas pueden estar en OS/2 y otras en MS-DOS) y el server está bajo Advanced NetWare de Novell 2.1. En este caso solo es necesario un programa de Software llamado **NetWare-Requester.**

En la segunda forma, en el server podrán estar tanto OS/2 como Novell Advanced NetWare 2.1 pero en este caso esnecesaria una tarjeta especial (Coprocessor-board) fabricada por Novell.

Advanced NetWare 286 V2.20

Sustituye prácticamente a todas las versiones anteriores, tine las mismas características de la version 2.15 además de permitir:

- Instalación mucho más sencilla (No necesariamente mejor).
- Permite Servidores de Impresoras (Print Servers).
- Existe en versiones para 5, 10, 20 y 100 usuarios.

Advanced NetWare 386 3.11

Características ***Novell Advanced Netware 386 V3.11***

* Soporta 250 Usuarios Lógicos
* Maneja 100 archivos abiertos simultáneamente
* Utiliza 32000 Registros de Directorio por Volumen
* Puede manejar 32 Volumenes por Servidor
* Soporta 32 Drives Lógicos por Volumen
* Tiene una Capacidad de almacenamiento de 32 TB
* Maneja 4GB de memoria RAM
* El tamaño máximo dee cada archivo pude ser hasta de 4GB

NetWare Portable

El NetWare Portable es una versión transportable del NetWare tradicional diseñado para correr en microcomputadoras y mainframes, siendo totalmente independiente del tipo de Hardware y protocolos usados. El NetWare Portable permite a los usuarios de PC y Macintosh sobre una **RED LOCAL-NetWare** compartir datos, servicios de impresión y aplicaciones con los usurios del host (Minis ó mainframes).

Este producto ofrece una solución al dilema de como integrar mainframes, minis, **REDES LOCALES**, PC, macintosh y otro tipo de estaciones de tabajo.

El NetWare para VMS fué el punto de partida para este producto, debido a la gran aceptación que tuvo en el mercado por la transparecia de integración de **RED LOCAL** -Host.

El primer sistema operativo de host destinado en el desarrollo del NetWare portable es Unix y corre eventualmente bajo VMS, VM, MVS.

El NetWare portable esta escrito en lenguaje C y es implementado como una aplicación en el host (Minis ó mainframes) de la misma forma què el NetWare para VMS en una DEC VAX.

El siguiente ejemplo nos muestra como el NetWare Portable funciona en el host. Usaremos Ethernet para propósitos ilustrativos, pero cualquier tipo de interfase para **RED** soportada por NetWare puede ser usada (figura 14).

NetWare Lite

Descripción General

NetWare Lite es un sistema fácil de usar y soportar. Se le concibió con el objeto de que cualquier usuario promedio de computadoras personales, con un conocimiento relativo del sistema operativo DOS, esté en condiciones de utilizarlo. El mercado que se establece con este producto es muy interesante, ya que brinda la posibilidad técnica y económica a cualquier negocio, por muy pequeño que sea, que cuente con computadores personales, de establecer una pequeña y sencilla RED LOCAL.

NetWare Lite se ofrece a los usuarios con base en una copia por cada nodo que se esté instalando, contrariamente a las versiones por número de usuarios del NetWare tradicional, el precio por cada nodo coloca al producto competitivo en el mercado internacional.

La misión principal de NetWare Lite es provocar un crecimiento de la industria de las **REDES LOCALES** a un potencial máximo y favorecer un cambio permanente en la forma en que los negocios pequeños efectúan su automatización.

Es importante remarcar que este producto es totalmente nuevo, no una adaptación de la actual línea de productos de NetWare.

De hecho no constituye un sistema operativo en su totalidad como lo es el NetWare actual, sino más bien un enlace de **REDES** que funciona con base al sistema operativo DOS, bajo la filosofía *PEER TO PEER* (cliente-cliente) para compartir los discos duros y los dispositivos de impresión.

Sin embargo, los usuarios observarán al sistema con la misma filosofía de interfase de usuarios que el NetWare actual, permitiendo una fácil migración a los sistemas de **RED** más sofisticados conforme evolucionen las empresas y sus necesidades de información.Los resultados de las pruebas que se han efectuado demuestran un rendimiento hasta del 120% superior al de los productos que funcionan con alguna filosofía similar.

El hardware que se requiere es mínimo en cuanto a los requerimientos de memoria de las estaciones de trabajo/servidores. La comunicación, al igual que sus hermanos mayores es con base en IPX.

NetWare Lite cosiste en tres programas núcleo:

* Un programa de servidor que procesa requisiciones sobre la **RED**.
* Un programa de cliente que redirecciona las requisiciones sobre la **RED** al servidor apropiado.
* Un conjunto de drivers DOS ODI, LSL y ODI IPX.

La implicación más importante de este conjunto de drivers es que el producto funcionará perfectamente con cualquiera de las topologías de **RED** más populares: Ethernet, Arcnet y Token Ring. Adicionalmente, NetWare Lite contará con varios programas de utilería que efectuarán las siguientes funciones:

* Administración de la **RED**
* Operación de los usuarios.
* Diagnóstico y detección de fallas.
* Aplicaciones de **RED**.

Es importante establecer las principlaes diferencias entre este nuevo producto y el NetWare que existe actualmente.

La utilización del sistema ***"PEER TO PEER"***, contrariamente al sistema de cliente-servidor que utiliza NetWare 2.2. ó 3.11 tiene menor rendimiento.

Es decir, NetWare Lite se basa en DOS mientras que NetWare 2.2. y 3.11 son un sistema operativo completo, que toma control total sobre las facilidades de cómputo, un proceso que se utilice en el NetWare Lite tomará más tiempo que el mismo proceso en el NetWare tradicional.

El rendimiento general de la **RED** disminuirá más rápidamente en NetWare Lite que en el NetWare tradicional al incrementar el número de estaciones, de tal forma que, en el momento que un cierto número de ellas utilicen NetWare Lite, lo más aconsejable será, dependiendo del tráfico en la **RED**, la migración al NetWare tradicional.

Por el momento, NetWare Lite no soporta funciones de ruteo de datos, ni es independiente del protocolo de comunicaciones, ya que soporta solamente

No utiliza las utilerías del NetWare normal, ni los procesos distribuidos de cómputo tales como el enfoque cliente-servidor.

Al ser un sistema basado en DOS, NetWare Lite no soporta ambientes operativos que no se basen en él.

Sin embargo, los sistemas más populares, como Windows y Deskview si están basados en este ambiente, por lo que se les puede utilizar.

En resumen, NetWare Lite es un producto que se ha pensado para hacer factible las **REDES** más sencillas, en un ambiente operativo con posibilidades muy interesantes de expansión.

Características ***Novell NetWare Lite***

*Tecnología "Peer toPeer" para compartir archivos e impresoras.
* Cierre de archivos y registros (vía DOS SHARE) DOS 3.1.
* Soporte para todos los drivers ODI DOS.
* Soporte para DOS 3.x y 4..x.
* Soporte para cache de disco escrito por terceros.
* Spooling de impresión múltiple.
* Reasignación y eliminación inmediata de spooling.
* Visión global de los recursos de la **RED** (discos, impresoras, usuarios).
* Control de acceso a recursos compartidos.
* Registros de auditoría de eventos significativos.
* Utilería de instalación.
* Utilería de verificación de comunicación.
* Utilerías de supervisión con interfase de usuario en toda la pantalla.
* Utilerías de supervisión de seguridad.
*Utilerías de usuario en formato de comando y en interfaces de pantalla.
* Ayuda en línea.
* Hasta 255 archivos abiertos por servidor.
* Hasta 25 usuarios simultáneos por servidor.
* Hasta 25 servidores por **RED**.

Hasta aquí, el análisis de las versiones de NetWare de Novell, sus pros y contras se comentarán en el capítulo de Ponderación entre sistemas Operativos.

3.2 LAN-MANAGER MICROSOFT

A continuación se incluyen las especificaciones que el propio Microsoft establece para su producto.

LAN-Manager de *Microsoft*

TABLE OF CONTENTS

Overview 3

Microsoft OS/2 LAN Manager/IBM LAN Server Interoperability 5

Workstations 6

Servers 6

Security 8

Structure of LAN Manager Security System 8

Structur of LAN Server Security System 9

Heterogeneous Networks Composed of LAN Manager and LAN Server Components 10

LAN Manager/LAN Server Coexistence 10

Sharing Resources on the Mixed Network 10

Enabling Users to Enumerate Resources Available on Servers of the Opposite Type 11

Summary of Security Administration on Mixed Networks 12

Network Command Interfaces 13

LAN Manager/LAN Server Command-Line Interface 13

Issuing Command-Line Commands That Affect Resources on the Opposite System 15

Remote Administration Facility 15

Using the Command-Line Interface on DOS Workstation 16

LAN Manager Extensions to the LAN Manager/LAN Server Command Set 17

Full-Screen Interface 18

Print Spooler 20

OVERVIEW

IBM[R] LAN Server and Microsoft[R] OS/2 LAN Manager workstation and server components may be mixed and matched on the same physical network and interoperate with one another, as illustrated by the diagram on the following page. Workstation and server components include all OEM implementations of Microsoft OS/2 LAN Manager such as 3Com[R] 3+ Open[TM] LAN Manager and Net/One[R] LAN Manager.

Microsoft LAN Manager and IBM LAN Server interoperate because they share the same core software technology and the same systems interfaces. In 1987, IBM licensed Microsoft LAN Manager technology to use as the basis for IBM LAN Server. LAN Manager and LAN Server both use OS/2 on the server, the SMB network protocol, the NetBIOS interface, and the NetBEUI/DLC network transport stack. As a result, customers will be able to mix and match LAN Manager and LAN Server networking products just as they today mix and match PCs from companies such as Compaq, Tandy, and Zenith with IBM PCs and PS/2[r] computers.

Microsoft OS/2 LAN Manager and IBM LAN Server are interoperable in the following essential respects:

- Workstations of one type may access resources on servers of the other type, provided that they have adequate security permissions. This means, for example, that LAN Server workstations can share files, print queues, modems, etc. on LAN Manager servers, and vice-versa.
- Network command-line commands are compatible across a mixed network -- that is, commands may be issued from a requestor of one type to a server of the other type. For example, a LAN Manager workstation user can issue a "net copy" command to copy files between the workstation and a LAN Server server, or vice versa. The LAN Server command-line interface is a proper subset of the LAN Manager command-line interface -- in other words, all command-line commands in LAN Server are in LAN Manager.
- Workstations of one type may run a command remotely on a server of the opposite type -- that is, workstation users can perform remote administration. For example, a LAN Manager workstation user may peruse or reset an audit trail on a LAN Server server (via the "net audit"

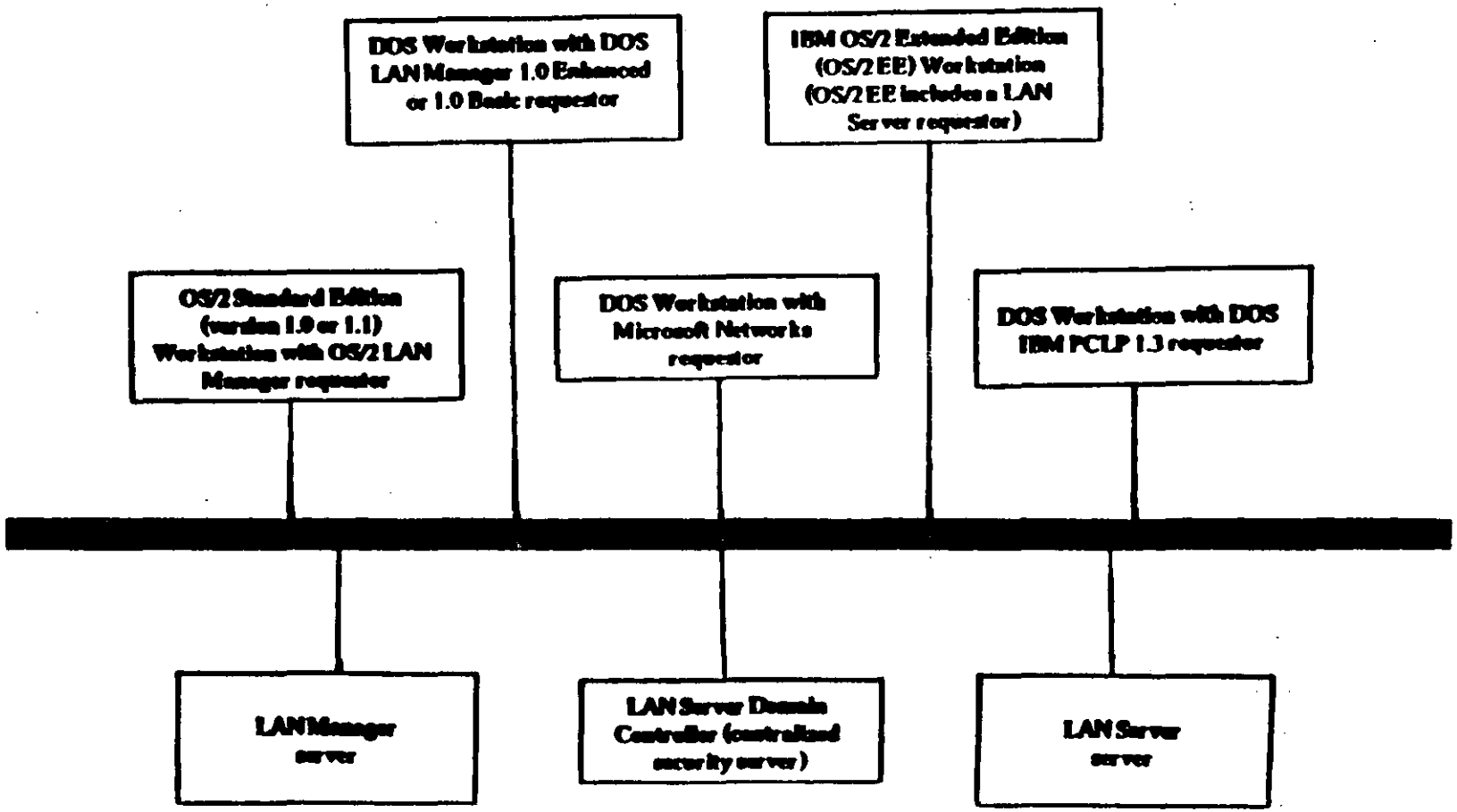
command), assuming the user has administrative privileges on LAN Server. The opposite, a LAN Server workstation performing remote administration on a LAN Manager server, is possible as well.

- LAN Manager network applications, such as SQL Server and front-end applications that use SQL Server, can be run on LAN Server systems.

The Microsoft OS/2 LAN Manager and IBM LAN Server are different in a few important respects. However, these variations do not preclude interoperability. They simply involve a little extra administrative overhead.

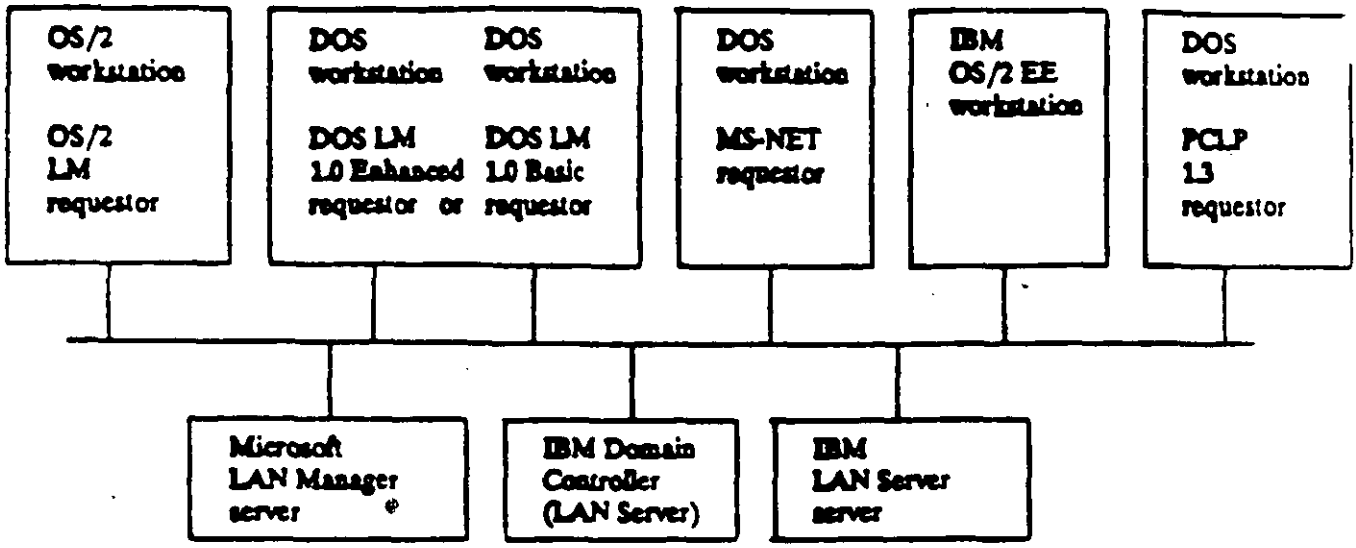
- The Microsoft OS/2 LAN Manager and IBM LAN Server utilize different security systems for specifying, storing, and authorizing network access permissions. This has two important ramifications. First, it means that a few simple steps must be taken in order to administrate security on mixed networks. For example, user accounts must be set up on both LAN Manager and LAN Server so users can access resources on both systems. Second, the security system differences place some limits on the commands that may be issued to a server of the opposite type. For example, it makes no sense to issue the LAN Manager commands dealing with security (such as net access, net password) to a LAN Server server.
- In addition to the command-line interface, LAN Manager and LAN Server include full-screen interface programs (with pull-down menus and dialog boxes) for issuing network commands. Though visually similar to each other, the full-screen interface programs included with the two products are different. As a result, the full-screen interface programs are somewhat limited in what kinds of network operations they are able to perform on the opposite system. However, users can issue commands through the command-line interface or full-screen interface on the system they wish to manage.
- LAN Manager and LAN Server use different print spoolers. As a result, the functions a LAN Manager workstation user may perform on LAN Server print queues are somewhat limited.

MICROSOFT OS/2 LAN MANAGER/IBM LAN SERVER INTEROPERABILITY



6

WORKSTATIONS



SERVERS

Workstations:

- OS/2 Standard Edition (versions 1.0 or 1.1) workstation with OS/2 LAN Manager requestor
- DOS workstation with DOS LAN Manager 1.0 Enhanced redirector (supports most of the features of the OS/2 LAN Manager redirector) or DOS LAN Manager 1.0 Basic redirector (MS-Net level redirector with the added features of auto-reconnect and Uniform Naming Convention support)
- DOS workstation with MS-NET redirector
- IBM OS/2 Extended Edition workstation (Extended Edition includes a LAN Server redirector)
- DOS workstation with DOS IBM PCLP 1.3 requestor

Servers

- LAN Manager server
- LAN Server domain controller (centralized security server)
- LAN Server server

SECURITY

The Microsoft OS/2 LAN Manager and IBM LAN Server utilize different security systems for specifying, storing, and authorizing network access permissions. Despite this difference, LAN Manager and LAN Server components can coexist on the same network. Network resources can be accessible across the different product types as long as security administration is handled correctly.

To understand the security implications of combining LAN Manager and LAN Server components on the same network, network administrators need an overview of the two security systems.

Structure of LAN Manager Security System

Microsoft OS/2 LAN Manager has two types of security: share-level security and user-level security. Under share-level security, each server resource (such as a directory on a hard drive) is assigned a password and only users who need access to the resource are given that resource's password. Share-level security is compatible with older MS network products and is most appropriate for local area networks that mix old and new network software.

User-level security provides user validation and access rights to individual resources on a server. Under LAN Manager user-level security, each server has user-account files containing entries for user name, password, user's group memberships, and a list of the resources that that user may use. The user first logs on to the network. Any time the user attempts to use a resource on a server, the server checks its user-account files to see if the user in question has permission -- in other words, has a valid user name and password.

If a user does not have an account on a LAN Manager user-level security server, he/she may log on as a "guest." Guest users are granted a set of permissions on a server as specified by a systems administrator. For example, an administrator may grant guest users on a particular server permission to submit jobs to a particular print queue. However, the administrator may decide that all users on this server require user accounts to access any server resources beyond this one printer queue.

LAN Manager also has a "centralized log-on server" option. When this feature is activated, all network users are validated through the centralized log-on server at network log-on time. To use the network, users must have an account on the centralized log-on server. In addition, users must have accounts on any of the user-level LAN Manager servers they wish to access. If the local area network is made up of share-level security servers, a central log-on server can serve as the method of user name and user password validation.

Structure of LAN Server Security System

IBM LAN Server also uses a user-level security scheme -- that is, each user has a set of permissions for various network resources. Users can use only resources they have explicit permission to use. However, the IBM LAN Server security system is based on a "domain controller," a server that must be running on a network to validate user log-on and administer security. The domain controller is the centralized hub of the security system -- without it, no one can log on to the LAN Server network, let alone access network resources.

Before a user can log onto the network and access network resources, a user account must first be created on the domain controller. All users that log on using an IBM LAN Server requestor are validated against the security accounts on the domain controller. If the user account exists on the domain controller and the correct password is given, then the user is logged on and can access network resources. If a user does not have an account on the domain controller or if the domain controller is not operational, the user cannot access any network resources.

Conceptually, all access permissions for network resources can be thought of as residing on the domain controller. An administrator must go through the domain controller in order to alter access permissions for any resource on any LAN Server server in the network. In actuality, the domain controller maintains local-access permission tables on each LAN Server server on the network so the domain controller does not have to be explicitly involved every time permissions on network resources must be checked.

Heterogeneous Networks Composed of LAN Manager and LAN Server Components

The following describes what happens to security when LAN Manager and LAN Server components are connected on the same network. The first section describes how the two systems are able to coexist on the same physical network without interfering with each other. The second section explains how to administrate security on the combined LAN Manager and LAN Server network so all users may share resources on servers of either type. The third section describes how to make the combined system user-friendly by enabling LAN Manager users to see resources on LAN Server servers and vice versa. The final section summarizes the administrative steps necessary for administering security on a mixed network.

LAN Manager/LAN Server Coexistence

If LAN Manager and LAN Server systems are connected to the same physical network without any knowledge of the other, the two systems can function as if they are the only systems on the wire. In other words, when placed on the same physical network, LAN Manager and LAN Server components do not interfere with one another in any way. Having a Microsoft OS/2 LAN Manager server on a network containing LAN Server components does not affect the functioning of the LAN Server system. All IBM LAN Server requestors (workstations) still log on to the network using the domain controller for security validation. As is true for networks comprised solely of LAN Server components, the mixed network requires an IBM LAN Server domain controller for LAN Server workstations to log on to the network and access network resources.

Similarly, using an IBM LAN Server domain controller on a network with LAN Manager components does not affect the functioning of LAN Manager. All Microsoft OS/2 LAN Manager workstation users (who wish to access LAN Manager resources exclusively) log on to the network as if the IBM LAN Server domain controller did not exist.

Sharing Resources on the Mixed Network

Though LAN Manager and LAN Server use different security systems and maintain separate security databases, users may access resources on servers of the opposite type -- as long as they have appropriate security permissions on that system.

For a LAN Manager workstation user to access LAN Server resources, the user must have a valid account on the IBM LAN Server domain controller. This account should contain the appropriate permissions for the LAN Server resources he/she wishes to access.

The LAN Server workstation user who wishes to access LAN Manager resources must have user accounts on each LAN Manager server he/she wishes to access. However, it is an absolute requirement that the LAN Server workstation user also have an account on the LAN Server domain controller. The LAN Server requestor (workstation) software requires that the user first log on to the LAN Server security system before connecting the user to the network. This connection is essential -- the LAN Server workstation cannot access any network resources (including LAN Manager resources) without first connecting to the network via the LAN Server log-on sequence.

Enabling Users to Enumerate Resources Available on Servers of the Opposite Type

Setting up user accounts on LAN Manager servers and on the IBM domain controller enables users to access resources on either system. However, LAN Manager users must know the name of the LAN Server server that contains the resource they wish to use and vice versa. Users can't look up this information. For example, issuing a Net View command from a IBM LAN Server workstation will only list the LAN Server servers available on the network -- it will not list any LAN Manager servers.

This situation is akin to two communities in different phone districts with directory service (area code-555-1212) disabled. People within their own community can consult their local phone book to call anyone in their town. However, unless people already have the phone number of persons in the other phone district, they could not call since they would have no way of finding out the phone number.

The reason for this LAN Manager/LAN Server information barrier is really quite simple. Both IBM LAN Server and Microsoft LAN Manager operate under the concept of a community of machines. Under LAN Manager, the community is called "langroup" and under LAN Server it is called "domain." When users issue a Net View command to see what servers are available on their network, they only see the servers available in their own langroup/domain. However, they still may access server resources outside their langroup/domain if they know the name of the server (and have the appropriate permissions, of course).

Two simple steps are required for users to "see" servers and resources beyond the border of their own langroup/domain. These steps basically set the langroup equal to the domain -- that is, all LAN Server servers are defined as part of the langroup and all LAN Manager servers are defined as part of the domain. Once these steps are performed, a Net View command issued from either type of workstation will list all LAN Manager and LAN Servers on the network -- in other words, it will list a global directory.

The first step makes LAN Server servers "visible" to LAN Manager users. All Microsoft OS/2 LAN Manager workstations should have the langroup parameter in their lanman.ini files set to the name of the IBM LAN Server domain controller (with a "$" appended to the end of the domain controller name). Doing this causes the LAN Manager software to consider all the LAN Manager servers and all the LAN Server servers as part of the same langroup.

The second step adds the LAN Manager server names to the list of servers in the domain. This list is stored on the domain controller and may be modified using the IBM full-screen network administrator tool.

Summary of Security Administration on Mixed Networks

In summary, several simple steps allow IBM LAN Server workstation users to access Microsoft OS/2 LAN Manager resources and also to tell that the LAN Manager servers exist via the Net View command. In addition, the steps below allow LAN Manager workstation users to access IBM OS/2 LAN Server resources and also to tell that the LAN Server servers exist using the Net View command:

- create a user account on IBM LAN Server domain controller for each Microsoft OS/2 LAN Manager workstation user
- create user accounts on the Microsoft OS/2 LAN Manager servers for each IBM LAN Server requestor user (and on the centralized log-on server if that mode is used)
- define the Microsoft OS/2 LAN Manager servers as part of the domain on the IBM LAN Server domain controller
- set the "langroup" of each Microsoft OS/2 LAN Manager server and workstation to the name of the IBM LAN Server domain controller (with a "$" appended)

NETWORK COMMAND INTERFACES

Both Microsoft LAN Manager and IBM LAN Server support two network interfaces: a command-line interface and a full-screen interface with pull-down menus and dialog boxes.

The two command-line interfaces are almost identical. Command-line commands issued on LAN Manager workstations interoperate with LAN Server servers and vice versa. Furthermore, commands may be remotely administered on servers of the opposite type. The remote administration feature allows an administrator working from any computer on the LAN to issue commands as if they were actually typed on the remote server.

The LAN Server net commands are in fact a proper subset of the Microsoft OS/2 LAN Manager net commands -- all of the command-line net commands in LAN Server are part of the LAN Manager command set as well. However, a few LAN Manager net commands are extensions to the LAN Manager/LAN Server command-line command set. Most of these commands are used for security administration.

The LAN Manager and LAN Server full-screen interface programs have been developed separately and fundamentally differ as a result. Under LAN Manager, all functionality available through the full-screen interface is also fully supported through the command-line interface. On LAN Server, this is not the case: Certain kinds of network commands must be executed through the IBM full-screen interface since they have no command-line equivalent.

LAN Manager/LAN Server Command-Line Interface

LAN Manager and LAN Server support a common set of network commands. These commands are listed below.

Command	Description
AT	Schedules a program or command to run at a later date and time on a server. It also displays the list of programs and commands scheduled to be run.
Compact	Reorganizes disks, joins all fragmented files and subdirectories, and eliminates deleted entries from directories.

Net	Displays the LAN Manager Screen.
Net Audit	Displays or clears the audit-trail entries for a server.
Net Comm	Controls and displays information about shared communication-device queues.
Net Config	Displays information about or changes the configuration of a workstation or server.
Net Continue	Continues LAN Manager services suspended by the net pause command.
Net Copy	Copies files on a workstation or shared directory.
Net Device	Lists device names and controls shared printers and communication devices.
Net Error	Lists the most recent local area network errors and the times that they occurred.
Net File	Displays the names of all open shared files and the number of locks, if any, on each file. It also closes shared files and removes file locks.
Net Forward	Reroutes incoming messages to another user's alias.
Net Log	Starts or stops saving messages to a file or printer or displays information about message logging.
Net Logoff	Ends a computer's connection with the local area network and logs a username off from the local area network.
Net Logon	Logs on a username to LAN Manager and sets the user name and password for the user's Workstation.
Net Move	Moves files on a Workstation or shared directory.
Net Name	Displays, adds, or deletes the aliases defined in a workstation's list of aliases.
Net Pause	Suspends a LAN Manager service or connection with a shared resource and frees up memory used by a service.

Net Print	Displays and controls the contents of a shared printer queue
Net Run	Runs a program or command on a remote server.
Net Send	Sends messages and files to other users.
Net Session	Lists or disconnects sessions between the server and other computers on the local area network.
Net Share	Makes a resource available to workstations.
Net Start	Starts LAN Manager services.
Net Stats	Displays and clears a server's list of usage statistics.
Net Status	Displays a server's computer name, spool directory, and configuration settings.
Net Stop	Stops a LAN Manager service.
Net Use	Redirects a workstation's local devicename to a server's shared resource.
Net View	Displays the computername of all local area network servers in a LAN group or displays the resources being shared by a server.

Issuing Command-Line Commands That Affect Resources on the Opposite System

Command-line commands issued on LAN Manager and LAN Server workstations interoperate with servers of opposite type. For example, commands that take a server name as parameter, such as "net view \\server_name," can be executed on a LAN Manager workstation to determine the resources available on a LAN Server server. Or, an administrator on a LAN Server workstation can use the "net comm\\server_name" command to display information about shared communication-device queues on a LAN Manager workstation.

Remote Administration Facility

A feature of the command-line interface is that most commands that can be executed directly on a server can also be executed remotely. The remote administration feature allows an administrator working from

any computer on the LAN to issue commands as if they are actually typed on the remote server. The administrator must have admin-privilege on the server that will be administered remotely.

Commands may be remotely administered on servers of the opposite type. For example, an administrator on a LAN Manager workstation can perform remote administration on a LAN Server server -- assuming the appropriate permissions.

There are two basic limitations on remote administration across a mixed network. First, a small group of commands do not support remote execution; the command a user wants to remotely administer cannot be in this group. Two commands that do not support remote execution are "compact" and "net" (which initiates full screen interface). Second, the command must be valid on the target system. For example, an administrator on a LAN Manager workstation can't remotely administer a "net group" command on a LAN Server server. The net group command is one of the LAN Manager extensions to the LAN Manager/LAN Server command set -- net group is not supported on the LAN Server system. See LAN Manager extensions section below.

Using the Command-Line Interface on DOS Workstations

There are two versions of Microsoft MS-DOS® LAN Manager. DOS LAN Manager 1.0 Enhanced (1.0 E) is essentially OS/2 LAN Manager workstation functionality mapped to a DOS workstation. The DOS LAN Manager 1.0 E requestor supports a large subset of LAN Manager command-line commands. DOS LAN Manager 1.0 Basic (1.0 B) is a scaled-down version of the DOS LAN Manager Enhanced requestor. It is simply a Microsoft Networks level redirector with the additional features of auto-reconnect, uniform naming convention support, and enhanced performance. DOS LAN Manager 1.0 Basic does not support any LAN Manager/LAN Server net commands beyond what is in Microsoft Networks.

The IBM DOS PCLP 1.3 redirector is an upgrade to existing PC LAN products, with a few performance enhancements and support for a limited number of the LAN Manager/LAN Server command-line commands.

LAN Manager Extensions to the LAN Manager/LAN Server Command Set

A few net commands exist in LAN Manager but are not supported by LAN Server. These are listed below:

Makeacc

Growacc

Net Access

Net Admin

Net Console

Net Group

Net Load

Net Password

Net Save

Net Separator

Net User

Makeacc, Growacc, Net Access, Net Group, Net Password, and Net User are security administration commands in LAN Manager. Because of differences in security systems, these commands are not valid on LAN Server. To perform security administration on LAN Server, administrators must use the IBM full-screen network administration program. See Full-Screen interface section below.

The LAN Manager Net Save and Net Load command-line commands also are not supported by LAN Server. Net Save creates a profile file containing the workstation's current local area network connections for later use. Net Load uses the contents of the profile file to configure the workstation's local area network connections as they were when the Net Save was executed. Under IBM LAN Server, user profiles are stored on the domain controller and are not accessible through the command-line interface.

The Net Admin command starts an administrative version of the LAN Manager full-screen network interface program. The Net Console command starts the console version of the LAN Manager full-screen

network interface. The console version is designed for use on unattended servers that are publicly accessible but need to be secure. LAN Server has its own full-screen interface, which is invoked using the Net command. See the Full-Screen Interface section below.

The Net Separator command causes the LAN Manager spooler to print a separator page between each print job (in a specified printer queue). LAN Manager and LAN Server use different spoolers; as a result, the Net Separator command is not supported by the LAN Server software. However, under LAN Server, one can cause separator pages to be inserted between jobs through a different mechanism -- the Presentation Manager spooler. See print spooler section below.

In addition to the security-oriented commands for Microsoft OS/2 LAN Manager that are invalid under IBM LAN Server, some valid commands have parameters that specifically affect the Microsoft OS/2 LAN Manager share-level security ("net share sharename=c:\ password" for example). These parameters are not valid parameters under IBM LAN Server since LAN Server does not support a share-level security scheme. In all cases, the LAN Server command line interface treats the parameters as ordinary syntax errors and recovers cleanly.

Full-Screen Interface

IBM LAN Server and Microsoft LAN Manager each have their own separate full-screen interface program.

The IBM LAN Server full-screen interface allows a user or administrator to access the security database on the domain controller. However, the full-screen interface is the only way a user or administrator may access may perform security operations -- all security functions must be done through the full-screen interface on either the domain controller or on a LAN Server workstation. There are no command-line equivalents for these security functions.

Under Microsoft OS/2 LAN Manager, however, all functionality available through the full-screen interface is also fully supported through the Net Command interface.

The full-screen interfaces are invoked slightly differently in the two products. In LAN Server, the Net Command initiates the full-screen program. If the workstation is logged on as an administrator, the

administrator version of the LAN Server full-screen program activates. If the workstation is logged on as a user, the user version of the full-screen program (a scaled-down version of the administrator edition) is activated.

In Microsoft OS/2 LAN Manager, the Net command starts the full-screen interface for user functions, while the Net Admin command starts the full-screen interface for administrator functions. The Net Console command starts the console version of the LAN Manager full-screen network interface. The console version is designed for use on unattended servers that are publicly accessible but need to be secure.

PRINT SPOOLER

LAN Manager and LAN Server use different spoolers. LAN Server uses the OS/2 1.1 (Presentation Manager) spooler, extended to allow network printing. LAN Manager uses a built-in print spooler.

Under LAN Server, most operations affecting print queues must be done from within the Presentation Manager spooler control panel rather than from the network full-screen or command-line interfaces. For example, holding/releasing queues, adding/deleting queues, and setting queue options (such as the time period during the day when the print queue can send jobs to a printer) must be performed through the Presentation Manager spooler interface program.

Because the Presenation Manager spooler control panel must run on the machine with the print queues, LAN Manager workstations are limited in the extent to which they can manipulate LAN Server print queues. In contrast, LAN Server workstation users with administrative privileges on LAN Manager may perform any type of administration on LAN Manager print queues via the remote administration facility.

#########

3.3 IBM PC NETWORK PROGRAM (IBM-PC/LAN)

Descripción General

IBM liberó el PC Network Program en marzo de 1985 como el sistema operativo para su **RED PC Network**, ya hace unos años , IBM liberó la versión 1.3.

Adicionalmente IBM está usando este sistema operativo para su nueva **RED** Token-Ring mediante un emulador del NETBIOS.

Este sistema operativo de **RED** permite hacer **Servidor de RED** a cualquier microcomputador que posea disco duro y corre como una aplicación de DOS.

A cada recurso de la **RED**, tales como microcomputadores, discos, impresoras, periféricos, etc; se le asigna su nombre lógico y un password mediante el cual otros usuarios de la **RED** lo accesan.

Para entrar a la **RED** no se requiere de un procedimiento de "LOGIN".

Componentes y Arquitectura

PC Network Program consta de cuatro componentes básicos: El PC DOS 3.2 ó 3.1, el Redirector de Microsof, el Software de servidor de archivos y las utilerías de la **RED**.

El sistema operativo de la estación de trabajo, se comunica con el servidor de archivos de la **RED** mediante el DOS y el Redirector. Las llamadas de la aplicación son interceptadas por el DOS, si la llamada es para la **RED**, el DOS la transfiere al Redirector, el cual trasmite al servidor de archivos de la **RED** mediante el NETBIOS.

Dado que DOS es un sistema para un solo usuario, la velocidad de respuesta para esta **RED** no es muy rápida. El DOS debe completar una tarea antes de comenzar otra.

En el caso de operar el servidor de la **RED** en modo no dedicado, el redirector y la aplicación también corren como aplicaciones de DOS el tiempo de ejecución del DOS estará dividido lo cual reduce el tiempo de respuesta.

Las acciones que IBM tomará para mejorar estos inconvenientes serán limitadas, pelro predecibles. La siguiente versión de DOS será probablemente multiusuaria y correrá en modo protegido en un ambiente 80286.

Soporte de Estandares

Como se mencionó en la descripción de la arquitectura del PC Network, el PC DOS es un componente clave del mismo. El PC Network Program es compatible con los estandares establecidos por MS-DOS 3.1.

Obviamente , este programa soporta el estandar NETBIOS.

Hardware Soportado

El PC Network y Token-Ring, aunque puede correrse en todo el Hadware de **RED** que soporte NETBIOS y MS-DOS 3.1.

Por ejemplo la **RED** Micronet o la X-net,, pueden correr este programa debido a que se cuenta con el emulador de NETBIOS necesario.

Interconexión de Redes

Debido a que el sistema operativo PC Network Program corre bajo DOS, las características para formar inter-**REDES** son limitadas.

Existe la posibilidad de formar una inter-**RED** entre PC Network y Token-Ring. No más de dos sistemas pueden ser puenteados y este puente requiere de un microcomputador dedicado.

Seguridad

NETBIOS asigna a cada recurso (tal como una impresora, un disco, etc.), de la **RED**, un nombre único mediante el cual los usuarios de la **RED** lo accesan. Por lo anterior no se requiere de un procedimiento de "LOGIN" para entrar a la **RED**.
Cada recurso, ya sea un archivo de datos, un directorio, un programa o una impresora, tiene un nombre. A cada nombre se le asigna un password que permite su utilización bajo el esquema de seguridad. Se permiten tres privilegios con el password: Lectura, Escritura y Creación.

Lo anterior requiere que el usuario conozca una gran variedad de passwords. Por otra parte el servidor de archivos de la **RED** no se encuentra protegido por passwords o cualquier otro tipo de seguridad. Si una persona tiene acceso fijo al servidor, todos los datos pueden ser accesados con comandos de DOS.

Operación en Modo Protegido

Debido a que el PC Network Program corre como una aplicación de DOS, el producto no puede proveer un modo protegido de operación en su forma actual.

Esto limita al servidor de archivos a 640 Kb. de memoria y 70 Mb. de almacenamiento de disco.

Sistema de Archivos

El PC Network Program utiliza la estructura de archivos de DOS, la cual es jerárquica. La ventaja de este tipo de estructura es que se pueden organizar los datos en la manera en que van a ser usados.

Mientras que la implementación de esta estructura permite un crecimiento dinámico de subdirectores, el precio de esta ventaja es un bajo tiempo de respuestas. En la Estructura de DOS, los subdirectorios se implementan como archivos en directorios.

Como resultado, la apertura de archivos, varios niveles abajo en la estructura jerárquica, puede consumir bastante tiempo, debido a que se tienen que abrir varios archivos y se deben efectuar varias búsquedas secuenciales.

Debido a la naturaleza de un solo usuario de DOS , no se pueden implementar algunas de las características que posee NetWare de Novell, tales como búsqueda de elevador, búsqueda simultánea y códigos hash en directorios. El DOS proveé un Cache para discos limitado a través del manejo de Buffers en el CONFIG. SYS.

Disponibilidad e Integridad de Datos

La mayoría de fabricantes de discos duros prueban sus unidades y los defectos son marcados como "Bad blocks" de forma que estos no se vuelven a utilizar durante la operación del disco.

El DOS es capaz de detectar estos "Bad blocks" y no utilizarlos. Pero después de un período extendido de uso, otras áreas del disco pueden presentar problemas. Si lo anterior sucede El DOS no evita que se vuelvan a usar esas áreas por lo que este riesgo puede afectar a PC Network Program.

A continuación enumeraremos las principales características del sistema operativo IBM-PC Network:

-Opera con MS-DOS 3.1 en adelante.

-Trabaja en dos formas: Menús o Comandos, permitiendo al usuario escoger el de su preferencia.

-Permite alternar la operación entre el programa de la RED y los programas de aplicación que se estén manejando.

-Permite enviar y recibir mensajes hasta de 60000 caracteres a todos los usuarios de la RED o a un usuario en especial.

-Tiene protección de bloqueo de archivos y registros, siempre y cuando el ambiente de la aplicación maneje este facilidad (Record locking , File locking).

-Puede ser instalado en todo tipo de PC's.

-Puede compartir hasta 150 recursos al mismo tiempo por cada configuración "server" de la **RED**.

-Opera en monitores monocromáticos y de color.

-Permite manejar "colas" de impresión.

Una de las principales ventajas de IBM-PC/LAN es su bajo costo comparado contra otros sistemas como el Novell-NetWare. Ampliaremos sus pros y contras en la sección de Ponderación entre sistemas operativos.

3.3 OTROS SISTEMAS OPERATIVOS PARA RED.

En el mercado internacional existen otros sistemas operativos para **RED**, por orden de importancia en base a su penetración de ventas, se mencionan a los siguientes:

1.-**Novell Advanced NetWare** en sus diferentes versiones, que anteriormente ya se mencionaron.

2.-**Viness (Virtual Network System) de BANYAN. Este sistema** operativo es el competidor más importante de Novell-NetWare, y el más cercano en cuanto a su rendimiento (Performance).

Cada día son más los tipos de tarjetas de **RED** que los soportan., y tenía hasta el mes de agosto algunas ventajas sobre novell en cuanto a comunicaciones, pero con las nuevas versiones 2.1', las diferencias se han reducido incluso superado. Hasta este momento Vines no se distribuye en nuestro País.

3.-**MS-NET y su familia** : *IBM PC/LAN Program y 3COM+, Share*, dado que todos estos sistemas operativos están basados en el *MS-NET*, se han agrupado en este inciso. Quizá la mejor implementación es la de *3COM*, si bien la versión 1.2 de *IBM-PC/LAN* trae algunas mejoras en cuanto a rendimiento. (Ya se ha analizado este sistema).

4.-**TORUS-Tapestry** : Está enfocado a usuarios no experimentados y su forma de operación está basada en íconos (tipo Macintosh) y ventanas de diálogo. En Europa ha logrado más aceptación que en los EE.UU., y al igual que Viness, no se vende en nuestro país, aunque una Compañía de Monterrey le interesa su distribución.

La principal desventaja , es que se tiene que adquirir un paquete por cada estación de trabajo, lo cual en **REDES** medianas y grandes incrementa mucho el costo.

5.- **Otros** :Los cuatro anteriores son sistemas más comunes, en buena parte porque no solo funcionan para un tipo de Hadware de **RED**. Sin embargo , varios fabricantes de tarjetas tienen su propio sistema operativo, por ejemplo: AT&T para su **RED Starlan**, Corvus para **RED Omninet** (PC-nos), etc.

También existen algunos sistemas operativos como el *NETWORK-OS*, que lo representa una casa muy seria aquí en México, por su aceptación en el mercado nacional se incluyen las notas que proporciona el representante sobre sus características e instalación. *Network-OS* es de muy fácil instalación por medio de menús.

En cuanto al material invitamos al lector que ponga especial interés en como se planea la **RED**.

NETWORK/OS

NETWORK-OS

INTRODUCCION

Network-OS es un sistema operativo de redes locales para PC, PC/XT. PC/AT y compatibles. Network-OS es compatible con NETBIOS y DOS 3.1 en adelante, lo cual significa que puede correr cualquir aplicacion compatible para DOS 3.1. Ademas Network-OS soporta el bloque de archivo y de registros de Novell.
Otro punto importante es que con Network-OS llena sus necesidades actuales y las del futuro ya que puede comenzar teniendo una red pequeña de 2 o 3 usuarios e irse expandiendo hasta un maximo de 255 estaciones de trabajo, ademas con Network-OS no tiene limite en el numero de SERVER'S que desee tener con la ventaja de que estos son de uso no dedicado.
Network-OS es facil de utilizar debido a que su instalacion es a traves de menus, con lo cual no tendra que aprenderse numerosos comandos como en otros sistemas operativos de red. Network-OS esta diseñado para trabajar de acuerdo a como usted piensa. Simplemente asigne nombres familiares de hasta 16 caracteres de longitud para identificar cada uno de los recursos de la red y posteriormente con ayuda de los menus de Network-OS usted podra seleccionar cuales de los recursos podran ser utilizados y por que usuario ya que Network-OS consta de un sisterna de registro de usuarios el cual le brinda seguridad en la informacion que podra accesar cada uno de ellos.

REQUERIMIENTOS DE NETWORK-OS

HARDWARE:

- Computadora PC, PC/XT, PC/AT o compatibles.

SERVER:

- Un disco duro de 10Mb
- 1 unidad de disco de 360Kb
- 512Kb de Ram
- Memoria utilizada por el sistema 180Kb
- Espacio en disco utilizado por el sistema 800Kb mas espacio para el spooler de impresion.

ESTACION:

- 1 unidad de disco de 360Kb
- 256Kb de Ram
- Memoria utilizada por el sistema 80Kb
- Espacio en disco utilizado por el sistema 200Kb

FUNCIONES DEL NETWORK-OS

Network-Os le permite accesar en forma transparente los recursos de otra computadora asi como los propios. El compartir recursos tiene muchas ventajas, por ejemplo el mover archivos de un sistema a otro o accesar archivos que se encuentran en otro sistema, ademas de que le permite realizar un mejor aprovechamiento del espacio en disco de sus maquinas. Por ejemplo en lugar de tener cuatro copias de su base de datos, se podra accesar de una sola maquina. Las impresoras tambien se pueden compartir, es decir, varios usuarios podran compatir la misma impresora o posiblemente quiera compartir una impresora de calidad y una impresora de alta velocidad.

FUNCIONAMIENTO DEL NETWORK-OS

Como ya se ha mencionado con Network-OS las Estaciones de Trabajo van a poder hacer uso de los Recursos compartidos por los Server's de la red.
Network-OS permite a las Estaciones de Trabajo accesar los recursos que se estan compartiendo en la red atraves de la **redireccion** de los recursos especificados.
Uno de los recursos especificados podria ser el disco duro C: o cualquiera de las letras disponibles para designar a un disco. Para una impresora el recurso esta especificado por LPT1, LPT2 o LPT3.

Para comprender el concepto de **redireccion** suponga que se tienen dos computadoras en donde una es el Server y la otra la Estacion de Trabajo.
El Server y la Estacion de Trabajo tiene dos unidades de disco flexible A: y B: y un disco duro C: . Si el Server va a compartir su disco duro C: a la estacion de trabajo Network-OS nos permite redireccionarlo por ejemplo como el disco D: en la estacion de trabajo debido a que ya tiene disco C:, de no hacerlo asi y direccionarlo como C: el disco C: de la estacion de trabajo quedaria deshabilitado.

Otro de los puntos que hace poderoso al Network-OS es el Sistema de registro de usuarios, el cual provee control de acceso por medio una clave de entrada al sistema personificada la cual le dara acceso a los recursos que se le estan compartiendo desde cualquier Estacion de Trabajo.

PLANEACION DE LA RED

El proposito de esta seccion es facilitar la instalacion del programa del sistema. Esta planeacion le ayudara a organizar, documentar e implementar su red. Para llevar a cabo la planeacion de la red se diseñaron 4 formas:

- Server Recursos Compartidos
- Estacion Recurso Usados
- Cuentas
- Archivo de Usos

Si se va a utilizar el Sistema de registo de usuarios se tendran que llenar las siguientes formas:

- Server Recursos Compartidos
- Cuentas
- Archivo de Usos

Si no se va a utilizar el Sistema de registro de usuarios se llenaran las formas:

- Server Recursos Compartidos
- Estacion Recurso Usados

Server Recursos Compartidos.- Provee una lista completa de los recursos a compartir en la red. Se necesitara una forma por cada Server dentro de la red. Esta forma requiere de la siguiente informacion:

- Nombre del Server
- El nombre del recurso
- El nombre de red asignado a dicho recurso
- El tipo de acceso permitido
- La clave de acceso al recurso si es que se desea

Server Recursos Compartidos
Nombre del Server _____

DOS Path/ Nombre	Nombre Corto	Acceso Permitido	Clave de Acceso	Comentarios

Nombre del Server.- Cada Server debera de tener un nombre propio y debera de ser unico para cada uno de estos. El nombre podra contener cualquier caracter entre A y Z, 0 a 9 y el caracter "_" y podra tener una longitud maxima de 15 caracteres.

El **nombre del recurso.**- Le indica a Network-OS *que recurso va a ser* compartido como por ejemplo:

Para indicar:	Nombre del recurso:
El disco duro	C:
Impresora Paralela	LPT1 o PRN
El subdirectorio WS en D:	D:\WS

El nombre corto de red asignado a dicho recurso.- Para cada recurso que se desea compartir se le necesita asignar un nombre corto para ser identificado. Dicho nombre podra contener cualquier caracter entre la A y Z, 0 y 9 y el caracter "_" y con una longitud mmaxima de 15 caracteres.
Como ejemplo tenemos:

Recurso:	Nombre asignado:
El disco duro C:	CDRIVE
El subdirectorio WS en D:	WordStar
La impresora	Impresora

El tipo de acceso permitido.- Por medio de este punto se determinara el tipo de acceso permitido por las estaciones. Los diferentes tipos de acceso permitidos se muestran a continuacion:

R para solo lectura.
RW para lectura y escritura.
RWC para lectura, escritura y creacion de nuevos archivos.
W para solo escritura.

La clave de acceso.- Este es un campo opcional. Usted es quien decide si se necesitara una clave de acceso para cada recurso. Solo usuarios que se sepan la clave correcta podran accesar dicho recurso. La clave puede ser de 15 caracteres como maximo y puede contener los mismos caracteres descritos en el nombre corto de red para designacion del recurso.

Estacion Recursos Usados.- Provee una lista de los recursos utilizados por una Estacion de Trabajo. Se necesitara llenar una forma por cada estacion de la red.
Esta forma requiere de la siguiente informacion:

- Nombre de la Estacion de Trabajo
- Nombre del Server a accesar
- El nombre corto del recurso
- El designador atraves del cual se accesara el recurso
- La clave de acceso

Estacion Recursos Usados

Nombre de la Estacion _____

Nombre del Server	Nombre Corto	Designador del recurso	Clave de Acceso

Nombre de la Estacion de Trabajo.- Cada Estacion de Trabajo debera de tener un nombre propio y debera de ser unico para cada uno de estas. El nombre podra contener cualquier caracter entre A y Z, 0 a 9 y el caracter "_" y podra tener una longitud maxima de 15 caracteres.

Nombre del Server a accesar.- En este punto se anota el nombre del Server que se va a accesar.

El nombre corto del recurso.- Se anota el nombre corto del recurso a utilizar. Este nombre se definio previamente en la forma del Server.

El designador atraves del cual se accesara el recurso.- En este punto se define el drive o designador a ser utilizado para el recurso a utilizar.

La clave de acceso.- Si se definio una clave de acceso para el recurso a utilizar, en este punto se puede anotar dicha clave y el usuario tendra acceso inmediato, si se desea que el usuario introdusca la clave bastara con poner un asterisco, entonces cada vez que se accese este recurso preguntara por la clave de acceso.

Cuentas.- Provee una lista de todas las cuentas de la red. Se llenara una forma para todas las cuentas de la red.
Esta forma requiere de la siguiente informacion:

- Identificador del usuario
- Nombre del usuario
- Clave de acceso del usuario
- Nombre del archivo de Usos

Cuentas

Identificador de usuario	Nombre del Usuario	Clave de Acceso	Archivo de Usos

Identificador del usuario.- La identificacion del usuario es un codigo unico que debera de introducir el usuario en su estacion de trabajo para poder entrar a la red.

Nombre del usuario.- Este es un campo opcional para documentacion y puede tener cualquier nombre que se desee.

Clave de acceso del usuario.- Asi como el identificador del usuario, la clave de acceso debera de introducirse para poder accesar la red. Esta clave puede tener un maximo de 15 caracteres.

Nombre del archivo de Usos.- El sistema de registro de usuarios puede ser por estaciones o por usuarios.
Por estaciones.- introdusca un asterisco en la columna de nombre del archivo de usos. Cuando instale el sistema de registro de usuarios, se creara un archivo de usos. El nombre de cada estacion debera de ser unico.
Por usuarios.- introdusca el nombre del archivo de usos para este usuario.

Archivo de Usos.- Provee una lista de todos los recursos utilizados por cada usuario. Se necesitara llenar una forma por cada archivo de Usos.
Esta forma requiere de la siguiente informacion:

- Nombre del Archivo de Usos

- Nombre del Server
- Nombre corto del recurso
- El designador atraves del cual se accesara el recurso
- La clave de acceso

Archivo de Usos

Nombre del Archivo de Usos_____

Nombre del Server	Nombre Corto	Designador del recurso	Clave de Acceso

Nombre del Archivo de Usos.- Nombre del archivo de usos previamente definido en la forma de cuentas.

Nombre del Server.- Nombre del server a ser accesado.

Nombre corto del recurso.- nombre corto del recurso a ser utilizado por este usuario.

El designador atraves del cual se accesara el recurso.- En este punto se define el drive o designador a ser utilizado para el recurso a utilizar.

La clave de acceso.- Clave de acceso que tendra este usuario, si se desea que el usuario lo introdusca en el momento de iniciar su sesion se introducira un asterisco en este punto.

INSTALACION

Para efectuar la instalacion del Network-OS se necesitan seguir los siguientes pasos:

1.- Obtener un respaldo de sus discos originales de Network-OS.
2.- Haber efectuado la instalacion de la tarjeta de la red en sus maquinas.
3.- Haber efectuado los pasos de planeacion de la red.
4.- Instalacion del software en un Server o en una Estacion de Trabajo.

Para instalar el software ya sea en un Server o en una Estacion de Trabajo, se necesita introducir el disco 1 de Network-OS en el drive A de su computadora y ejecutar

NWINSTAL

y la siguiente pantalla sera desplegada.

```
---------------------------------------------------------------------------
Network-OS                                                    Installation
---------------------------------------------------------------------------
                      PC/MS DOS COPIES VERIFICATION

  Copyright laws require that each user have an individual PC/MS DOS
  license (i.e. 1 copy per computer on the network).
------------------------------------------------------------- [Options] ---
                                                          [ YES ]
  Do you have adequate copies available?  YES             [ NO  ]
---------------------------------------------------------------------------
  Press [END] to scroll down & [HOME] to scroll up. [RET] to select.
---------------------------------------------------------------------------
```

En esta pantalla se nos pregunta si tenemos copias autorizadas de DOS para cada maquina. En la pantalla se nos presenta un menu de opciones con las opciones YES y NO, se podra seleccionar las opciones oprimiento las teclas de <Home> y <End>. La opcion de fabrica (default) es Yes por lo cual oprimiremos <Return>.

La siguiente pantalla sera desplegada.

```
Network-OS                                              Installation

                    COLOR or BLACK & WHITE Monitor In Use
If you have a black and white monitor attached to this computer, select
NO so that all Network programs may be displayed in black and white.
                                                              [ Options]
  Do you wish to display programs in COLOR mode? YES          [YES ]
                                                              [NO  ]
                    NETWORK-OS UPDATE INSTALLATIONS
If you have previously installed Network OS on this computer and you want
to keep all configuration, resource sharing, usage, and user registration
information, select YES. Otherwise, all configuration information will be
erased.
  Do you want to keep previous Network OS system files? YES

  Press [END] to scroll down & [HOME] to scroll up. [RET] to select
```

En esta pantalla se nos pregunta si queremos trabajar en color.
Responder segun sea el caso.
La siguiente opcion se refiere a si queremos conservar la configuracion efectuada con anterioridad si es que esta no es la primera vez que se efectua el proseso de instalacion.
En la siguiente pantalla se nos pregunta si la instalacion sera efectuada en disco duro o en un disco flexible como se muestra a continuacion.

```
Network-OS                                              Installation

                        TYPE OF INSTALLATION
The installation process will transfer Network-OS program files to the
target disk drive from the distribution diskettes.
The full system occupies about 800K Bytes of storage. If the target
system has a hard disk with more than a megabyte of storage, select the
HARD drive installation by selecting HARD.
If space is limited, as in a floppy disk, select partial installation
by selecting FLOPPY.FLOPPY installation transfers only the files necessary
to bring up Network-OS. Any other required utilities may be copied using
the DOS COPY Command. Consult the manual for list of files and functions.

                                                          Options
                                                            HARD
  INSTALLATION TYPE  :  HARD                              FLOPPY

  Press [END] to scroll down & [HOME] to scroll up. [RET] to select
Select FLOPPY for floppy installation, HARD for hard drive installation
```

Despues de esto el programa nos preguntara la unidad fuente de instalacion, la unidad destino, el nombre de la maquina, la trayectoria (path) inicial que tendra la maquina y si esta sera un Server o una Estacion de Trabajo como se muestra a continuacion. En este ejemplo supondremos que se esta configurando un Server.

```
---------------------------------------------------------------------------
Network-OS  Installation Type: HARD                        Installation
---------------------------------------------------------------------------
SOURCE PATHNAME:  A:\
DESTIN PATHNAME:  C:\NW
START-UP PATH     : C:\;C:\DOS;C:\NW
MACHINE NAME      :
CONFIGURATION     : NS
---------------------------------------------------------------------------
                                [ Help ]
Normally you will be logged onto the drive containing the distribution
diskette and the field will show the correct path-name. If, however, you
are running NWINSTAL from some other drive, please enter the id of the
drive and subdirectory, in which the distribution software is loaded.

Examples: B:\    or     A:\     or     C:\NW
---------------------------------------------------------------------------
```

Posteriormente la siguiente pantalla sera desplegada, en donde se nos muestran los parametros seleccionados previamente ademas del espacio en disco disponible, en la parte inferior de la pantalla el programa nos solicitara los discos que necesite para copiar los archivos que sean necesarios.

```
-------------------------------[ Network-OS Installation ]-------------------
---------------------------------------------------------------------------
Installation Type is: HARD -- Cr     lete Network-OS software installation
Source Path Name  is: A:\
Destination Path  is: C:\NW
Free space available:  17,401,856 Bytes  Machine Name is : SERVER
---------------------------------------------------------------------------
```

```
-------------------------------------[ Load Diskette ]---------------------
          Load Network-OS distribution diskette # 1 in drive A
                    Press a key when ready ....
---------------------------------------------------------------------------
```

Una vez terminado el proceso se nos indicara que dejemos el disco 3 en la unidad.

La siguiente pantalla sera la siguiente, en donde se nos da la opcion de pasar a la parte de configuracion de los recursos a compartir o saltarnos esta parte y dejarla para despues.

```
----------[ NetServer Resource Configuration ]----------
Since a NetServer configuration has been chosen, it is necessary to set
up the resources that this station can share. The SHARE's are stored in
a separate system file and accessed by the Network-OS startup programs.

The Resource File is maintained by a separate utility program, giving
you the ability to add/delete to the resources added at this time.
Optionally, you may skip this step and set up the NetServer's SHAREs
later.

The next screen contains all resources currently SHARED on this NETSERVER.

Press any key to set up the shared resources.
Press <ESC> to skip the Resource Configuration.
```

Si queremos configurar los recursos a compartir oprimiremos cualquier tecla para continuar y si no se quiere configurar en este momento se oprimira la tecla de <ESC>.

Suponiendo que queremos configurar los recursos la siguiente pantalla sera desplegada, en donde se nos muestran los recursos que ya estan configurados para ser compartidos.

```
----------[ Shared Resource List ]----------
 NETWORK NAME          DOS PATH/DEVICE NAME          RTS  PWORD
--------------------------------------------------------------------------------
SISTEMA        C:\                                   RWC  NO




--------------------------------------------------------------------------------
                          Hit a key to continue
                  End of file reached -- Press any key to Exit
--------------------------------------------------------------------------------
```

Al oprimir cualquier tecla la siguiente pantalla para la definicion de los recursos a compartir sera desplegada en donde se nos preguntan los siguientes puntos.

- Designador del recurso a compartir.
- Nombre corto del recurso.
- El tipo de acceso permitido.
- La clave de acceso.

Si el recurso es una impresora se configurara en la misma pantalla los siguientes puntos.

- El encabezado de impresion el cual puede ser:
  - None.- no imprime nada de encabezado.
  - FF.- Saca una hoja en blanco al principio de una impresion.
  - Banner.- Cada impresion saldra con una hoja indicando el nombre de la maquina que emitio la impresion.

- Impresion despues del trabajo enviado el cual tiene dos opciones:
  - None.- no imprime nada al terminar el trabajo.
  - FF.- Imprime un salto de hoja.

- Impresion de Form Feeds
  - Allow.- permite impresion consecutiva de varios Form Feeds.
  - Suppress.- Imprime un solo Form Feed si es que hay varios uno inmediatamente del otro.

- Tamaño de impresion de los tabuladores el cual puede ser de maximo 8 espacios.

- Permiso en los trabajos de impresion el cual puede ser:
  - Private.- Solo el Server puede efectuar cambios.
  - Public.- Cualquier usuario puede efectuar cambios.

- Impresion directa esta opcion es la ultima y tiene las siguientes opciones;
  - None.- No permite a ningun usuario accesar la impresora.
  - All.- Permite a cualquier usuario imprimir directamente.
  - Self.- Solo el Server puede imprimir en forma directa.

```
----------------------------------[Shared Resource Definition]----------------------------------
DOS PATH/DEVICE NAME     : C:\
NETWORK SHORT NAME       : SISTEMA
ACCESS RIGHTS            : RWC
ACCESS PASSWORD          :
PRINT JOBS' HEADER       :
PRINT JOBS' TRAILER      :
PRINT FORM FEEDS         :
PRINT TAB EXPANSION      :
PRINT JOB SETUP          :
DIRECT PRINT             :
------------------------------------------------------------------------------------------------
  F7! Cancel  F8! Edit  F9! Save & Continue  F10! Save & Quit
------------------------------------------------------------------------------------------------
```

Despues de introducir estos parametros en la ultima linea aparecera como se indica las funciones disponibles. Si queremos salvar el recurso dado de alta y continuar con la especificacion de recursos a compartir con la tecla F9 salvamos y una nueva pantalla igual a la anterior aparecera. Si queremos salvar la configuracion y pasar al siguiente paso en la configuracion con oprimir F10 nos aparecera la siguiente pantalla.

```
-----------------------------------------[ Workstation Use Set-up ]-----------------------------------
All workstations, including NetServers must specify USEs to redirect
local drives/devices to Shared drives/devices on the Network.

The Use File is maintained by a separate utility program, giving
you the ability to add/delete to the resources added at this time.
Optionally, you may skip this step and set up the workstation's USEs
later.
The next screen contains all resources currently USED by this machine.
Press any key to set up the USEs.
Press <ESC> to skip the USE Configuration.
-------------------------------------------------------------------------------------------------------
```

En esta pantalla se nos pregunta si queremos configurar los usos de esta estacion o dejarlos para despues. Si se van a configurar con oprimir cualquier tecla inmediatamente se nos presentaran los recursos que estan activos para ser utilizados por esta computadora como se muestra a continuacion.

```
-----------------------------------------[ WorkStation USE List ]-------------------------------------
        - DEV -    ---- NETSERVER ----    ---- NETWORK NAME ----
-------------------------------------------------------------------------------------------------------
```

```
------------------------------------- Hit a key to continue -------------------------------------
                    No Resources Used -- Press any key to Exit
-------------------------------------------------------------------------------------------------
```

Si hay recursos apareceran en la pantalla. Con oprimir cualquier tecla se nos presentara la pantalla para la definicion de recursos a ser utilizados en donde se nos preguntan los siguientes parametros.

- Nombre del Server a accesar.
- Nombre corto del recurso a utilizar.
- Designador del recurso a utilizar.
- Clave de acceso al recurso

Como se muestra a continuacion.

```
----------Network Resource Use----------

NETSERVER OWNING THE RESOURCE : SERVER
NETWORK SHORT NAME            : SISTEMA
USED BY WORKSTATION AS        : D:
ACCESS PASSWORD               :

F7 Cancel  F8 Edit  F9 Save & Continue  F10 Save & Quit
```

Al terminar en la ultima linea nos apareceran nuevamente las funciones disponibles. Si ya no tenemos mas recursos a utilizar que definir oprimiremos F10. Despues de esto el sistema creara el CONFIG.SYS y el AUTOEXEC.BAT que se requiere para cargar la red en forma automatica.

```
----------[ Configuration File Setup ]----------

Setting up NWCONFIG.SYS
Setting up sample AUTOEXEC.BAT

Network-OS has created CONFIG.SYS and AUTOEXEC.BAT files in the
system directory.  Please edit both of these files and insert system
specific commands.  Next copy both of these files into the boot
directory of this system
The next program is NWCONFIG.  The initial entry password is PASSWORD.

        Please press any key to continue.
```

Despues de que los crea oprimiremos cualquier tecla y automaticamente se ejecutara el programa NWCONFIG.EXE, el cual nos sirve para configurar el sistema. Este programa esta protegido con una clave de acceso la cual es **password** y puede cambiarse en este mismo programa.

```
----------[ Network-OS Configuration ]----------
Enter the Configuration password :
```

Una vez introducido la clave de acceso el siguiente menu de configuracion aparecera.

```
--[ Network-OS Configuration ]--
  Overall Network Configuration
  Share Resources
  Use Resources
  Registration Configuration
  Change Configuration Password
  Quit -- Exit to DOS
```

Set up General, Hardware, and Software Configuration Parameters

Overall Network Configuration.- Nos permite configurar los parametros consernientes al hardware y al software del sistema. Al seleccionar esta opcion el programa nos presentara otra pantalla para la configuracion.

```
----------[ Network-OS Configuration ]----------
Config  Quit
Set up machine name and configuration type
```

Posteriormente se nos preguntara el nombre de la maquina a configurar y si es un Server o una estacion de trabajo.

```
----------[ Network-OS Machine Name Assignment ]----------
        MACHINE NAME        :    SERVER
        CONFIGURATION TYPE  :    NS
---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]-------
Each machine is given a unique Network name, which Network-OS uses to
communicate with various nodes of the Network. Select a name of upto
15 characters. This name will be used in the Network-OS start up file
which is created by NWINSTAL. Please NOTE that some third-party
NETWORK SOFTWARE requires 2 unique digits at the end of the machine name.
Check the Network-OS installation manual for further explanation.
Examples: HOST_MACHINE  or  JACK01  or  SYSTEMSERVER
```

El programa nos desplegara entonces un submenu como se muestra a continuacion.

```
-----------------------------------[ NetServer Configuration ]-----------------------------------
General Hardware Software More Software Write File Quit
-------------------------------------------------------------------------------------------------
Assign NetServer Name and select general server options


-------------------------------------------------------------------------------------------------
```

La opcion GENERAL despliega la siguiente pantalla en donde se nos preguntan los siguientes parametros.

- Si la maquina es el Server de inicialisacion de las Estaciones de Trabajo sin disco (diskless).
- Si es el Server de Seguridad.- Esta opcion debera de ser YES si se esta utilizando el sistema de registro de usuarios.
- Si es el Server de mensajes.- Esta opcion debera de ser YES si se esta utilizando el sistema de mensajes y si queremos que este Server lleve el control de estos.
- El subdirectorio donde se encuentra el Network-OS.
- El subdirectorio a ser utilizado por el Spooler de Impresion.
- El subdirectorio para los archivos del sistema de registro de usuarios.
- El subdirectorio a ser utilizado para los mensajes.
- Los ultimos parametros son par fijar el tiempo de muestreo internos.

```
-------------------------------------------------------------------------------------------------
NetServer's GENERAL Set-up     NetServer's Machine Name: SERVER
-------------------------------------------------------------------------------------------------
 Is this a BOOT Server?  :     NO
 Is this a SECURITY Server?:   NO
 Is this a MESSAGE Server?:    NO

 Network System Directory      : C:\NW1
 NetServer Spool Directory     : C:\NW1\SPOOL

 NetServer Security Directory  : C:\NW1\NWUSERS
 NetServer Message Directory   : C:\NW1\NWMAIL

 Time Slice Allocation  :      INTERVAL: 10  Timer Ticks [~55 msecs]
                               SERVER    : 5     Timer Ticks
                               KEY POLL: 40  Times
-------------------------------------------------------------------------------------------------
----------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]-------
Enter <YES> if this server will be used to boot diskless workstations
on the network.
-------------------------------------------------------------------------------------------------
```

La opcion de hardware nos permite configurar el tipo de tarjeta de red que se esta utilizando, asi como los parametros que utiliza esta como se muestra a continuacion.

```
-------------------------------------------------------------------------------
                    NetServer Hardware Set-up
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
    Network Hardware Board Type       : BUSS
    BASE Port Address [Hexadecimal]   : 310
    Adapter Interrupt Channel Level   : 2
    I/O Buffer Segment Address [Hex]  :
    D M A  Channel for Adapter        : 1
    # of Personal Network Stations     :
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
  INTERRUPT CHANNEL for PRINTER PORT    LPT1 :  N
  INTERRUPT CHANNEL for PRINTER PORT    LPT2 :  N
  INTERRUPT CHANNEL for PRINTER PORT    LPT3 :  N
  INTERRUPT CHANNEL for PRINTER PORT    COM1 :  N
  INTERRUPT CHANNEL for PRINTER PORT    COM2 :  N
-------------------------------------------------------------------------------

---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]-------
Select the type of network board which you have installed into
this particular computer.  Please note that this must correspond
to the version of NETWORK-OS which you have purchased.
Press [End] to scroll down & [Home] to scroll up. [Ret] to select
-------------------------------------------------------------------------------
```

La opcion de software nos permite configurar parametros maximos de los Server's y de las Estaciones de Trabajo como se muestra a continuacion.

```
-------------------------------------------------------------------------------
                    NetServer Software Options
-------------------------------------------------------------------------------
----[ Server Parameters ]-----------------------------------------------------
MAX. Number of Users          : 16    Number of message buffers: 3
MAX. Number of Shared Resources: 8    Size of each msg. buffer : 4144
MAX. Number of Sessions       : 16    Buffer size for SHARE.EXE: 4096
MAX. Number of open files     : 255   MAX. Number of Locks     : 64
-------------------------------------------------------------------------------
----[ User Parameters ]-------------------------------------------------------
MAX. Number of Servers        : 4     Number of file buffers  : 2
MAX. Number of redir. drives  : 5     Close spool file after  : 0  Secs
MAX. Number of Network files  : 20    MAX. FCB type files     : 16
Highest redirected drive letter: Z    MAX. FCB directories    : 8
-------------------------------------------------------------------------------
---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]-------
This is the maximum number of users supported by this server.  This
number must be less than or equal to the number of users specified in
the license agreement with CBIS.  If a user above the limit tries to access
the network, the 'REMOTE COMPUTER NOT READY' message will be displayed
-------------------------------------------------------------------------------
```

En la opcion de More Software se nos preguntan los siguientes parametros.

- Si queremos que se instale el programa de mensajes al inicializar la red.
- El tipo de notificacion al recibir un mensaje, los cuales pueden ser 3 diferentes.
  - Una retroalimentacion auditiva para indicar que se ha recibido un mensaje.
  - Despliegue de una sola linea del mensaje recibido.
  - Despliegue de todo el mensaje recibido.
- Si esta permitido accesar una unidad de disco flexible y la red en forma simultanea.
- Si se esta utilizando el netbios de CBIS.
- La inhibicion del vector de interupcion 68h-6fh. Este parametro solo se aplica en PC/AT y debe de ser NO si el programa de aplicacion utiliza este vector de interrupcion.
- Si esta habilitado el sistema de registro de usuarios.
- Si queremos desplegar los programas en blanco y negro.

La pantalla asociada a estos parametros es la siguiente.

```
                    More Software Options

-----[ Network-OS Intercom Parameters ]----------------------------------
Install Intercom Program on Bootup          : NO
Notification to Give When Message Received  : BEEP ONLY
-------------------------------------------------------------------------
-----[ Special Options ]------------------------------------------------
Allow simultaneous floppy and network i/o   :    YES
Enable generic NetBios speed-up mode        :    NO
Inhibit use of Interrupt Vectors 68h-6fh    :    NO
Enable User Registration Option             :    NO
Always Display Programs in BW80 Mode        :    NO
-------------------------------------------------------------------------
---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]--------
Enter <YES> if you want to have the NETWORK-OS InterCom program installed
during the NWSTART procedure.
-------------------------------------------------------------------------
```

Por ultimo la opcion de WRITE FILE es para salvar la configuracion de los parametros escogidos. Al seleccionar esta opcion el programa nos preguntara si queremos salvar la configuracion y salir de esta. Debido a que se efectuan cambios al archivo NWCONFIG.SYS la maquina tiene que ser inicializada otra vez.

```
---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]--------
The NWCONFIG.SYS file has been updated. Reboot this machine for new para-
meters to take effect.

                        PRESS ANY KEY TO CONTINUE
-------------------------------------------------------------------------
```

Share Resources.- Nos permite configurar los recursos a ser compartidos por el Server asi como cancelar o editar los previamente definidos.

Use Resources.- Nos permite configurar los reoursos a ser utilizados por la estacion asi como cancelar o editar los previamente definidos.

Registration Configuration.- Nos permite configurar el sistema de registro de usuarios. En esta opcion se tiene el siguiente menu

User Setup Use File Quit

Con la primera opcion se tiene el siguiente submenu

Display Add Change Quit

Si seleccionamos Add la siguiente pantalla sera desplegada

```
----------[User Registration Set-up]----------
USER ID        : LUIS

USER NAME      : luis

USER PASSWORD  : X-NET          LEVEL :

USE FILE NAME  : LUIS
-----------------------------------------------
----------[ HELP WINDOW ]----------
Enter the file name (without the extension) for the file containing this
user's USE information.
Please note that you must create this file with the USE SETUP option of
this program.
-----------------------------------------------
```

En esta pantalla se nos preguntan los siguientes parametros.

- Identificador del usuario.
- Nombre del usuario.
- Clave de acceso del usuario.
- Nombre del archivo de Usos.

Posteriormente se nos desplegara el menu de funciones para Cancelar, Editar y Actualizar.

La opcion de Uses File nos permite crear el archivo de uso previamente definido en el punto anterior. En esta opcion se nos presenta el submenu

Display Select Edit Quit

El primer paso es seleccionar el Archivo a utilizar como se muestra a continuacion.

```
----------[USE File name Select]----------
  Enter USE Data Set File name : LUIS
-----------------------------------------
```

Despues de esto el programa desplegara las siguientes opciones.

Display Add Change Quit

Si seleccionamos Add la siguiente pantalla sera desplegada, en donde se nos preguntan los siguientes parametros.

- Nombre del Server a accesar.
- Nombre corto del recurso a utilizar.
- Designador del recurso por la estacion.
- Clave de acceso.

```
-------------------------------[Network Resource Use - Data Set: LUIS]----------------------
NETSERVER OWNING THE RESOURCE : SERVER

NETWORK SHORT NAME            : SISTEMA

USED BY USER'S WORKSTATION AS : C:

ACCESS PASSWORD               :
------------------------------------------------------------------------------------------
-------------------------------------------[ HELP WINDOW ]--------------------------------
Enter the password which was assigned for this resoure.
If no password was assigned, press ENTER.
Enter * if you wish the user to be prompted for the password when
this resource is used
------------------------------------------------------------------------------------------
```

Change Configuration Password.- Nos permite cambiar la clave de acceso a este programa.

Esta opcion del programa de configuracion y nos despliega la siguiente pantalla, en donde se nos presenta la clave de acceso actual. En este punto se puede teclear otra clave de acceso y posteriormente oprimiremos <CTRL><RETURN> para salvar los cambios.

```
-------------------------------[ Configuration Password Change ]----------------------------
    Enter new CONFIGURATION password : PASSWORD
------------------------------------------------------------------------------------------
```

```
---------[ HELP WINDOW -- PRESS CONTROL-RETURN to keep changes and quit ]-------
Enter a password of at least FOUR characters.  This is the password
used to gain entry to all configuration programs.
------------------------------------------------------------------------------------------
```

La opcion de Quit es para salirse de este programa.

SEGURIDAD INFORMATICA

HACKERS LOS REVIENTAORDENADORES

El objetivo: bancos de datos de centros militares, laboratorios científicos y multinacionales de cualquier lugar del mundo. Los herramientas: un ordenador personal y un teléfono. El reto: vencer los sistemas de seguridad que se interponen en el camino.

Iniciados a temprana edad en el mundo de la telemática, estos hackers del chip encuentran su máximo placer en reventar los passwords —códigos de acceso— que bloquean la entrada a grandes ordenadores.

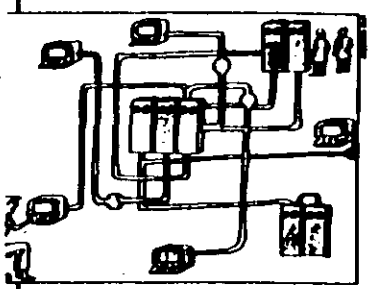
Son las dos de la madrugada. Fuera llueve. Luis lleva encerrado en su cuarto desde que salió del colegio, hace más de ocho horas. Los ojos le pican de tanto mirar la pantalla de su ordenador personal, pero no puede dejarlo. Está a punto de conseguir el mayor éxito de su carrera de hacker dentro de unos minutos va a entrar, por teléfono y de forma clandestina, en el ordenador central de la Sorbona, la universidad más famosa de París. Y no sólo eso. Piensa saltarse la clave del director del sistema y tomar personalmente el control del procesador.

Por fin lo ha conseguido. Le ha costado muchas semanas de barajar miles de nombres de identificación y palabras clave. Trabajo concienzudo que ahora se ve recompensado. Antes de cortar la comunicación, Luis escribe un mensaje que a la mañana siguiente aparecerá en la pantalla del director del sistema: «Te cacé, amigo. La próxima vez ten más cuidado». Y ahí acabó la aventura.

Luis es un hacker típico, incluso valdría como retrato robot. Cuando cumplió doce años, sus padres le regalaron un pequeño ordenador doméstico. A los pocos meses de manejar el aparato, el BASIC y el sistema operativo ya no tenían secretos para él. Al mismo tiempo le empieza a aburrir el intercambio de videojuegos con los amigos. Encuentra más divertido saltarse las protecciones de los programas e introducir nuevas variantes. Después de un par de años, vende el viejo ordenador doméstico y se compra, de

segunda mano, un aparato compatible con el estándar IBM. Poco a poco el juego se convierte en lebra. Con un *modem* —un dispositivo especial para conectar el ordenador al teléfono—, Luis establece contacto con otros fanáticos del teclado. Uno de ellos, con el que ya ha entablado amistad, le proporciona la clave de acceso del ordenador de una importante empresa de la ciudad. A partir de ahí quiere descifrar él mismo las claves para entrar en ordenadores ajenos. Es el gusanillo del *hacking*.

Pero existe otra manera de describir a un hacker, diciendo lo que no es. Un hacker no es un saboteador, no es un espía, no es un ladrón de programas, no es un informático malicioso, aunque al inglés lo que le mueve, la droga que le mantiene despierto por las noches, es el puro placer intelectual de saberse capaz de sortear las más difíciles barreras de seguridad que protegen los grandes sistemas informáticos, ya pertenezcan a multinacionales, universidades, centros de investigación o instituciones del Estado. El hacker cuenta sus éxitos por el número de veces que logra un acceso no autorizado, una cruceta más para apuntar en un lado del monitor.



A mayoría de los grandes sistemas informáticos se hallan conectados entre sí a través de kilométricas redes de datos, a las que también pueden engancharse ordenadores personales

Es ese sórdido deporte del *hacking* lo que atrae las simpatías del gran público por estos intrépidos espadachines del chip, especie de modernos Robin Hood que, armados únicamente de un teléfono y un modesto ordenador personal, se atreven a enfrentarse a los millonarios centros de cálculo del Estado y las multinacionales. Con sus acciones vienen a demostrarnos que la supuesta omnipotencia de estas supermáquinas no es para tanto, que a pesar de todos sus dispositivos de seguridad son, al final, vulnerables. En cierto modo se trata de la última y secreta satisfacción del débil al descubrir que el poderoso también tiene su talón de Aquiles.

Sin embargo, la imagen molestosa del hacker está comenzando a resquebrajarse. De hecho, en varios países se empieza a considerar esta actividad como un delito de *espionaje de datos*.

La razón hay que buscarla en ciertos hechos ocurridos en los últimos años que nada tienen que ver con el romanticismo del David en lucha contra Goliat, y que no deberían despertar sonrisas de complicidad. Así, el presidente del Gobierno belga Wilfried Martens no le hizo ninguna gracia descubrir, a finales del año pasado, que un hacker leía su correspondencia privada en el ordenador oficial. Y tampoco se echaron a reír los más de 6.000 usuarios de ordenadores de Estados Unidos cuyos aparatos quedaron inutilizados durante semanas enteras porque alguien, después de introducir diferentes claves de acceso, se ocurrió introducir un virus en la red de comunicaciones informáticas INTERNET, caso éste por el cual ha sido procesado recientemente su autor, el norteamericano Robert Morris.

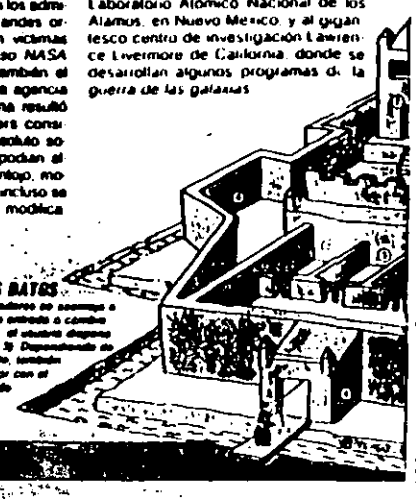
Robert Morris, autor del mayor desaguisado informático de la historia

Peor suerte corrieron los administradores de 135 grandes ordenadores que fueron víctimas del ya legendario caso NASA (llamado así porque también el centro de cálculo de la agencia espacial norteamericana resultó afectado). Los hackers consiguieron un control absoluto sobre los ordenadores, podían alimentarlos datos a su antojo, modificar los existentes, e incluso se dijo que podrían haber modificado las órbitas de algunos satélites. La siguiente mala noticia consiguió enlutar aún más la aureola romántica de los hackers auténticos.

La pasada primavera fueron detenidos en Alemania Federal tres jóvenes sospechosos de haber facilitado a los servicios secretos soviéticos, la KGB, información reservada sobre la OTAN, que habían obtenido ilegalmente desde sus casas por medio de un ordenador y un teléfono. Al parecer, la banda, que operaba desde 1985, cobraba 3.000 dólares por cada disquete con datos confidenciales, entre los que se encontraban las claves de acceso a la base de datos Optima del Pentágono, a una red de la NASA, al Laboratorio Atómico Nacional de los Alamos, en Nuevo México, y al gigantesco centro de investigación Lawrence Livermore de California, donde se desarrollan algunos programas de la *guerra de las galaxias*.

Utilizando métodos de los hackers Robert Morris se infiltró en la red de datos INTERNET y la contaminó con un virus maligno programado por él mismo. Más de 6.000 ordenadores quedaron inutilizados durante semanas

El equipo básico: ordenador, teléfono y modem. Este aparato sirve para regular la transmisión de datos



EL CASTILLO DE LOS DATOS

La arquitectura de los grandes ordenadores se asemeja a una fortaleza. El portero franquea la entrada a cambio del nombre y texto (1). Una vez dentro, el usuario dispone de miles para guardar sus datos (2 y 3). Dependiendo de las directrices que haya establecido, también puede usar programas (4), conectar con el exterior (5) o consultar el banco de datos (6). El System Manager (7) tiene todos los privilegios

Pero como actúan los hackers? Parece brujería que alguien pueda husmear con un sencillo ordenador personal en los grandes sistemas informáticos de multinacionales y organismos públicos, aunque estén en la otra punta del mundo. Sin embargo, conociendo mínimamente la organización de los modernos sistemas de proceso de datos, el misterio desaparece en el acto.

Un axioma irrevocable: si un hacker invade un ordenador desde el exterior, en el fondo es porque se le ha invitado a ello. El teleproceso funciona exactamente igual que una conferencia telefónica, por lo que del mismo modo que no se puede llamar a alguien que no tenga teléfono, si un ordenador no está conectado a ninguna red, ni el más genial de los hackers es capaz de invadirlo. Así de simple. Una conexión entre ordenadores, independientemente de la distancia que les separe, puede realizarse a través de la red telefónica o por medio de redes de comunicaciones especiales para datos electrónicos que entre otras ventajas admiten mayores velocidades de transmisión. Tampoco estos sistemas guardan ningún misterio: las redes de datos, al igual que las telefónicas, también son públicas. Cualquiera puede firmar un contrato de utilización, pagar los recibos mensuales y emprender el viaje con su ordenador por los vericuetos de las redes informáticas. A través de IBERNET (una red de datos española) se puede acceder fácilmente a otras del extranjero. Solo hace falta consultar la lista para ver qué ordenadores son accesibles desde cada red.

Este sistema de interconexión múltiple está propiciando la popularización creciente del correo electrónico. En lugar de escribir las cartas en papel y enviarlas en un sobre franqueado, el remitente instruye al ordenador para que transmita los textos a uno o más destinatarios a través de la línea telefónica o por una red de datos. Las grandes empresas e instituciones incluso disponen de redes propias para la distribución del correo: las máquinas implicadas utilizan los canales públicos de datos, pero trabajan con su propia estructura administrativa, que es la que decide quién recibe qué datos y por qué canal.

Tal método es especialmente apreciado por los científicos, pues en su trabajo necesitan intercambiar a diario grandes volúmenes de información. En todo el mundo las universidades y centros de investigación han constituido redes de ordenadores ramificadas miles de veces. En Europa, la principal red científica se llama EARN (*European Academic Research Network*, red europea de investigación académica). En Estados Unidos la red INTERNET conecta entre sí más de 10.000 centros de cálculo de universidades y empresas privadas. La red de cobertura mundial SPAN (*Space Physics Analysis Network*, red de análisis de física espacial), construida por la NASA, está especializada en laboratorios de investigación espacial y conecta entre sí más de 1.500 minordenadores científicos VAX. Por si la maña integración no fuera suficiente, las redes tienen además algunos puntos de contacto comunes. Así por ejemplo, un usuario de INTERNET puede acceder a EARN sin mayor problema.

No es de extrañar, pues que estos sistemas de redes, con sus innumerables ordenadores, constituyan un escenario ideal para los hackers. El consejo de administración de INTERNET llegó en una ocasión a considerar la posibilidad de implantar controles de acceso a la misma red, hasta

EL HACKER DESPIERTA LAS SIMPATÍAS DEL GRAN PÚBLICO, PORQUE CON SUS ACCIONES DEMUESTRA QUE LOS PODEROSOS TAMBIÉN TIENEN SU TALÓN DE AQUILES

Herlwart Holland, alias Wau, es el fundador del Chaos Computer Club de Hamburgo, la asociación de hackers más famosa y mejor organizada. Entre otras actividades, publican fanzines (abajo) con los últimos trucos para reventar passwords. Lo suyo, dicen, es un mero deporte

Centro de control de la NASA. Un error en la programación de los ordenadores VAX propició que un grupo de desconocidos pudiera manipular sus datos

ta que una mente práctica les abrió los ojos: sería como si los dueños de las casas, por miedo al robo, pusieran vigilantes en la carretera de entrada a la ciudad. Los grandes sistemas, al contrario que un ordenador personal, están a disposición de muchos usuarios: diversos terminales, con pantalla y teclado, aprovechan un único procesador central. Para que los usuarios no interfieran entre sí, acaso borrando o examinando (sin querer o a sabiendas) datos confidenciales de otra persona, es necesaria una administración de los recursos que imponga un orden.

El principio es sencillo: cada usuario tiene que presentarse al ordenador con un código de identificación (por ejemplo, su nombre) antes de cada sesión de trabajo. Así, el ordenador empieza preguntando, generalmente en inglés, *User id?* o *Login?* El interesado teclea entonces su *identificación*, e inmediatamente aparece la segunda pregunta: *Password?*

El *password*, la clave de acceso, es una *identificación* secreta privada. En cuanto ha sido tecleada, el ordenador comprueba si al *nombre* del usuario le corresponde exactamente esa palabra clave. En caso afirmativo, el ordenador le abre sus puertas. Este proceso es el mismo para todos, tanto si se encuentran ante un terminal en el centro de cálculo, como si se *comunican*, a través de una red de datos, desde otro punto del planeta. Sólo *quien* está registrado con nombre y password puede utilizar el ordenador. Está claro que, si una de estas claves de acceso, junto con su correspondiente código de identificación, cae en manos de un hacker, éste podrá solicitar los servicios del ordenador en nombre del usuario suplantado.

Sin embargo, una simple clave de *acceso* no permite a un hacker hacer cosas terriblemente prohibidas. Una vez establecida la comunicación con el ordenador, sólo puede realizar las mismas operaciones que se le autorizan al propietario legal de esa clave. Y éste también suele tener unos derechos bastante limitados. A cada usuario se le asignan unos privilegios que determinan qué puede hacer y qué no. Un usuario normal, por ejemplo, puede consultar el archivo central de clientes y escribir sus cartas con el programa de tratamiento de texto. Generalmente también dispone de espacio en los discos para almacenar sus datos. En cambio no le está permitido modificar direcciones del banco de datos, leer las cartas de otras personas, ni por supuesto andar fisgando en la organización interna del ordenador. Generalmente, de esto se encargan sólo unos pocos, que están en la cima de la jerarquía de privilegios de utilización: los *System Managers*, también *llamados superusuarios*.

El System Manager es responsable del correcto y ordenado funcionamiento del sistema, y por eso está autorizado a hacer cualquier cosa en él, absolutamente todo. Puede borrar, modificar o añadir datos y programas. El es quien determina qué privilegios tendrán los usuarios subordinados. Si un superusuario quisiera abusar de su poder, podría cerrar el acceso al ordenador a todos los demás, o mandar al garete la totalidad de los datos almacenados.

Visto esto, es fácil adivinar en qué consiste el máximo placer de un hacker. En primer lugar hay que sortear la barrera del código de identificación y del password para *enganchar*se a un ordenador. A partir de ahí, el reto reside en conseguir los derechos del System Manager. Si se logra, el ordenador quebrantado se presenta totalmente desnudo y vulnerable, todas la barreras de seguridad se han retirado del camino. Ahora el hacker ya puede ponerse los *laureles* y negarle al superusuario el acceso a su propio ordenador, eliminando sus derechos. Especialmente apreciada es la posibilidad de utilizar la conexión del sistema a la red como trampolín para comunicarse con otros ordenadores, cargando los costos en la cuenta de la víctima.

LOS MAS ORGANIZADOS TIENEN SUS PROPIOS ESTATUTOS, DONDE FIGURA UN CODIGO DE HONOR: ESTA BIEN ENTRAR Y FISGAR, PERO SIN HACER MAL A NADIE

En muchas ocasiones, los hackers consiguen introducirse ilícitamente en los ordenadores gracias a que sus usuarios y superusuarios legales se lo ponen bastante fácil, como lo demuestran las técnicas habituales para obtener una clave de acceso ajena. El ya mencionado caso del presidente del Gobierno belga se debió a un estúpido error, por lo que el señor Martens no debería quejarse de que le lean su correo personal. El intruso, según se demostró,

LA CLAVE DE LAS CLAVES

La elección de un buen password, la palabra clave que franquea el acceso a un ordenador, es esencial para salvaguardar la seguridad de los datos que contiene. Los expertos recomiendan las siguientes reglas básicas.

1. Un password ha de ser sencillo. Desde luego, la clave TMXKQGSW resulta bastante segura frente a hackers que lo intentan al azar, pero es muy difícil de recordar.

2. Un password no debe tener significado. Las palabras con significado son las más fáciles de reventar. Esto no excluye que sean sencillas de memorizar. Ejemplos: ZAZEMELI, PERPOLAS, RATOGARU.

3. Un password hay que memorizarlo, no apuntarlo. Dulen no se fie demasiado de su memoria a largo plazo, puede apuntar su palabra clave, pero nunca de manera que un extraño pueda reconocerla como tal. Así, nunca se le ha de escribir en la lista telefónica bajo CLAVE, SECRETO o COMPUTADORA. Es *mejor* garabatearla en la agenda junto al recordatorio del cumpleaños de la abuela. En ningún caso se debe dejar la nota escrita cerca del ordenador, bajo el teléfono o pinchada en el panel de corcho.

4. De vez en cuando conviene cambiar de password. Por si acaso alguien no autorizado ya lo conoce pero todavía no se ha decidido a usarlo. Tampoco es preciso cambiarlo muy a menudo: podría causarnos molestas equivocaciones.

5. Un password se teclea en privado. Al introducir la clave antes de comenzar una sesión de trabajo, hay que asegurarse de que nadie mire por encima del hombro. Las personas de confianza hacen honor a su nombre respetando la intimidad del propietario de la clave.

6. Ciertas palabras nunca han de servir de password.

—Nombres propios y apellidos.

—Apodos. El propio, jamás, pero tampoco el del perro o el gato.

—Palabras informáticas, como TEST, SYSTEM, CHECK, BYTE...

—Fechas de cumpleaños.

—Cadenas con método: ABCDEFGH, A1B2C3, QWERTY...

—Palabras de moda: SUPER, INCREIBLE, MAGNIFICO...

—Nombres de la mitología, la literatura o la ciencia-ficción: ZEUS, QUIJOTE, SPOCK, FRODO...

—La palabra clave por antonomasia: (ábrete) SESAMO.

era un ingeniero de software que participó en la instalación del sistema de correo electrónico de la Administración belga y había elegido personalmente la palabra clave de prueba para el jefe de Gobierno. Más de un año después, simplemente lo intentó... y funcionó, porque a nadie se le había ocurrido cambiar esa palabra por un nuevo password secreto.

En otros casos el punto débil en el sistema de seguridad se debe a un problema de memoria de los usuarios: no son capaces de recordar su palabra clave. Por eso la escriben en una nota y la pegan en el monitor. Los más cuidadosos la esconden bajo el teléfono o en un cajón. Un vistazo furtivo es suficiente... Algunos se dejan engañar inocentemente cuando un hacker llama por teléfono presentándose como servicio de mantenimiento, murmura algo sobre problemas del sistema y dice que necesita el password para unas supuestas reparaciones.

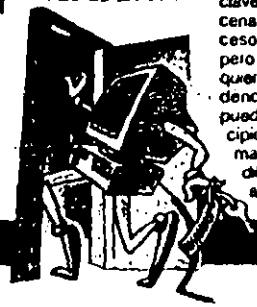
Para obtener una clave de acceso también se utilizan métodos asistidos por ordenador. Antiguamente, los hackers hacían que su ordenador personal llamara a los grandes centros de cálculo para probar uno a uno los probables passwords de una larga lista. Los encargados de seguridad pusieron freno a esta búsqueda a ciegas, que tarde o temprano solía dar resultado, obligando a cortar la comunicación al cabo de tres intentos erróneos. Ahora resulta más productivo buscar calculadamente grietas en los muros de seguridad.

Un hacker bien informado sabe, por ejemplo, que los ordenadores nuevos se suministran con una cuenta de usuario inicial, simplemente para poder empezar a trabajar con ellos. En un determinado modelo de ordenador, muy extendido, dicha cuenta tiene el nombre *system* y su clave de acceso es *manager*, y otorga todos los privilegios de utilización. Esta sencilla combinación ha franqueado el paso de muchos hackers a estos ordenadores, sólo porque a los responsables se les olvidaba eliminar este registro inmediatamente después de asignar los nombres y claves de acceso definitivos.

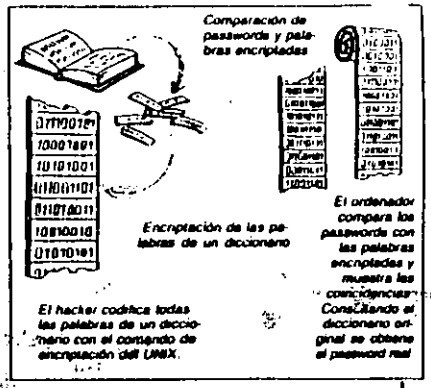
De fallar el ya famoso truco —entre los hackers— de teclear *system* para el identificador de usuario y *manager* como password, existen otros métodos. Algunos sistemas ofrecen la posibilidad de obtener, aunque de manera un tanto rebuscada, una lista con claves de acceso. Por ejemplo, hurgando en la arquitectura interna de los ordenadores con sistema operativo UNIX, considerada muy poco fiable por los especialistas. Gracias a una desafortunada característica del sistema, en poco tiempo un hacker medianamente hábil puede descifrar cierto número de palabras clave. El sistema UNIX almacena todas las claves de acceso en forma codificada, pero de tal modo que cualquier usuario, con independencia de sus privilegios, puede consultarlas. En principio no hay ningún problema, pues, debido a la codificación, los passwords aparecen ininteligibles

La pasada primavera fueron detenidos tres jóvenes alemanes acusados de facilitar a la KGB la clave de acceso a la red Optasis del Pentágono (arriba). A la derecha, el Kremlin, en Moscú.

A VECES EL JUEGO TOMA DERROTEROS PELIGROSOS: TRES JOVENES FUERON ACUSADOS DE VENDER A LA KGB CLAVES DE ACCESO DE ORDENADORES DE LA OTAN



Para decodificarlas se aplica una técnica bastante extendida entre los hackers. Primero se toma un diccionario en soporte magnético (se puede comprar) y se codifican sus miles de palabras según el mismo método con que se han codificado las claves de acceso, es decir, utilizando el comando de encriptación del sistema operativo UNIX. Un simple programa secuencial compara a continuación los passwords encriptados con las entradas del diccionario también encriptadas y extrae aquellas expresiones que concuerdan. Ya sólo falta averiguar a qué palabra corresponde la expresión codificada para disponer de la clave original. Por supuesto, este sistema sólo funciona si el usuario elige como clave de acceso una palabra corriente, de las que aparecen en los diccionarios. Algo que sigue sucediendo a pesar de los consejos de los expertos de utilizar palabras sin sentido como SIKUVERK o XATARAMA, o al menos distorsionadas, como SIISTEMM (ver recuadro).



HACKERS, CRACKERS Y WORMS

La popularización de los ordenadores personales ha propiciado la aparición de una generación de jóvenes fanáticos de la programación, capaces casi de desmontar y montar su equipo con los ojos vendados. Pero no todos dirigen sus pasos en la misma dirección... ni con las mismas intenciones. Los hackers puros gustan de reventar los códigos de acceso a ordenadores ajenos, pero cuando lo consiguen apenas hacen otra cosa que echar un breve vistazo al contenido de los ficheros violados. Sin embargo, algunos sucumben ante la tentación de los beneficios personales, y se convierten así en hackers espías, hackers chantajistas o hackers destructores.

La afición de los *crackers* consiste en romper los sistemas de protección anticopia de programas concretos, generalmente videojuegos. Una vez *destripado* el programa introducen en él instrucciones de cosecha propia para mejorarlo, por ejemplo, añadiendo más marcianos o dotándoles de nuevas y mortíferas armas. Al mismo tiempo, la desprotección también sirve para sacar copias ilegales del programa. En este caso, el *cracker* entraría ya de lleno en la categoría de pirata informático.

Por último, los *worms* utilizan técnicas propias de hackers y crackers para contagiar ordenadores ajenos con virus informáticos construidos por ellos mismos, bien sea camuflándolos en programas contenidos en diskettes o a través de redes de datos. En muchas ocasiones, los *worms* sólo propagan virus inofensivos, programados por ejemplo, para que hagan aparecer un mensaje gracioso en la pantalla de los ordenadores infectados. Pero también existe una variante perversa de estos manitas que se dedican a fabricar virus destructores de datos.

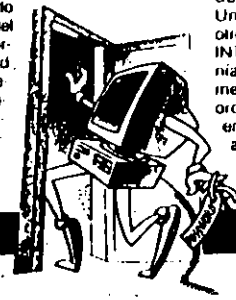
Las tretas de los hackers para hacerse dul control de ordenadores ajenos no conocen límites. Bastante malo es que la negligencia lo haga posible: por ejemplo porque un superusuario revele sin querer su palabra clave, pero mucho peor es que la ayuda provenga de un fallo del sistema o de la posibilidad de utilizar una puerta trasera. Esto es lo que ocurrió en los espectaculares precedentes, ya comentados, del virus de INTERNET y el caso NASA.

Los hackers del caso NASA aprovecharon un simple pero fatal error de programación que se había colado en las primeras versiones del sistema operativo de los ordenadores VAX de la red SPAN (ahora ya está corregido). Gracias a este *gazapo*, los usuarios podían solicitar determinados privilegios: el ordenador comunicaba que estaba prohibido, pero aun así concedía los derechos de utilización. Cualquiera que conociera este fallo podía así convertirse en autoproclamado superusuario. Precisamente el caso NASA muestra las repercusiones que pueden acarrear errores de este tipo. Los hackers modificaron el programa que pide la clave de acceso convirtiéndolo en un *caballo de Troya*: la nueva versión parecía perfectamente normal a los ojos de los ignorantes usuarios pero iba almacenando en un registro oculto las claves de acceso introducidas para dárselas a conocer posteriormente a sus creadores.

Si el caso NASA causó serios trastornos, el virus de INTERNET se considera el mayor desastre en seguridad informática de toda la historia. Consiguió invadir y destruir la información de más de 6 000 aparatos. Un virus informático es un microprograma, a veces completamente inocuo e inocente, pero otras maligno y destructor de datos, como el famoso *Viernes trece*, que actuó el día 13 del pasado mes de octubre.

El virus asesino de INTERNET funcionaba, a grandes rasgos, como sigue: su autor, Robert Morris, lo envió desde el ordenador de la Universidad de Berkeley a otro ordenador conectado a INTERNET. Desde ahí se ponía en marcha automáticamente y leía el directorio de ordenadores a los que podía emigrar. Por fin se enviaba a sí mismo a todos los ordenadores encontrados para volver a empezar el infernal juego desde el principio. En poco tiempo, cada vez más ordenadores ya sólo se ocupaban del virus: se llamaban mutuamente y se enviaban las mismas instrucciones una y otra vez.

PARADOJICAMENTE, LAS INCURSIONES DE LOS HACKERS HAN SERVIDO PARA QUE MUCHOS CENTROS DE CALCULO PUSIERAN AL DIA SUS PROTECCIONES

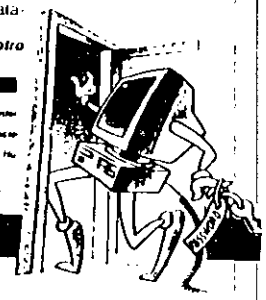


En vista de estos garrafales fallos de seguridad, uno se pregunta hasta dónde son capaces de llegar los hackers. ¿Existe, aunque sea teóricamente, la más mínima posibilidad de que, como en la película *Juegos de guerra*, accedan a ordenadores militares y desencadenen una tercera guerra mundial? Afortunadamente, la respuesta es negativa. Los militares utilizan para las comunicaciones secretas entre sus ordenadores unas redes especiales a prueba de pinchazos (embutidas a veces en tuberías con gas a presión, de manera que una intervención no autorizada provoque una subida descompresión que dispare la alarma), a las que, por supuesto, no se puede acceder desde la red telefónica.

En cualquier caso resulta muy difícil averiguar hasta qué punto los hackers -o los espías que utilizan sus métodos- tienen éxito en sus incursiones. Una empresa que sufre este tipo de problemas de seguridad informática se guarda mucho de dar publicidad al asunto. A lo sumo hacen publicidad de todo lo contrario, como la compañía telefónica japonesa NTT, que ofrece a bombo y platillo un millón de yenes (casi 8 000 dólares) al hacker que consiga descifrar el código de acceso a su nuevo sistema de comunicaciones.

Y mucho más cuestionables son los datos sobre los daños materiales supuestamente ocasionados por los hackers. ¿Cuánto cuesta un vistazo a un determinado *dossier*? Incluso si esto fuese evaluable, nunca se podría averiguar qué es exactamente lo que se ha examinado. Un símil: si alguien entra por la noche en un gallinero y toma fotos de 35 gallinas, ni el granjero ni la policía pueden saber cuáles han sido retratadas.

SIEMPRE EXISTEN RESQUICIOS POR DONDE SE PUEDE INTRODUCIR UN PROGRAMADOR HABIL, PERO, AUNQUE QUIERA, NUNCA PODRA DESATAR UNA GUERRA NUCLEAR



Angel Navalpotro

PARA SABER MAS

Informática y Poder. Colin Hines. Ed. Hermes. Barcelona.
Informática. Los Computadores en la Sociedad. Ruskin. Ed. McGraw Hill. México.
Manual de Hacker. Piratas Informáticos. Hispano Comercial. Anaya Multimedia. Madrid.