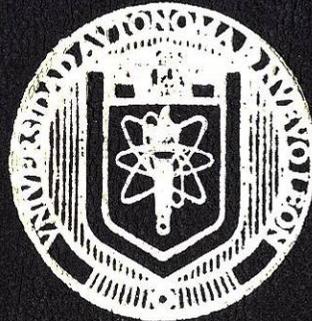


**UNIVERSIDAD AUTONOMA DE NUEVO LEON**  
**FACULTAD DE INGENIERIA MECANICA Y**  
**ELECTRICA**



**REDES DE AREA LOCAL**

**TESINA**

**QUE PARA OBTENER EL TITULO DE**  
**INGENIERO ADMINISTRADOR DE SISTEMAS**

**PRESENTA**

**PATRICIA OLGUIN GANDARA**

**MONTERREY, N. L.**

**NOVIEMBRE DE 1994**

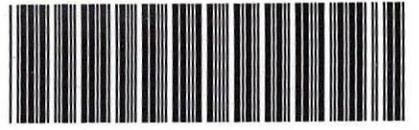
T

TK5105

.7

04

C.1



1080064402

UNIVERSIDAD AUTONOMA DE NUEVO LEON  
FACULTAD DE INGENIERIA MECANICA Y  
ELECTRICA



REDES DE AREA LOCAL

TESINA

QUE PARA OBTENER EL TITULO DE  
INGENIERO ADMINISTRADOR DE SISTEMAS

PRESENTA

PATRICIA OLGUIN GANDARA

MONTERREY, N. L.

NOVIEMBRE DE 1994

LIBRO DE REGISTRO  
UNIVERSIDAD AUTONOMA DE NUEVO LEON  
FACULTAD DE INGENIERIA MECANICA Y ELECTRICA  
NOVIEMBRE 1994

T  
TKS 105  
.7  
04



Biblioteca Central  
Magna Solidaridad

F. Fesú



U L  
FON O  
TESIS LICENCIATURA

## **AGRADECIMIENTOS**

**A MI FAMILIA QUIENES SIEMPRE ME APOYARON , MIL GRACIAS.**

**A TI QUE ERES LA PERSONA QUIEN ME INSPIRA EL DESEO DE SUPERARME DIA A DIA COMO PROFESIONISTA Y COMO MUJER,**

**A TI TE DEBO TODO MI AGRADECIMIENTO .....**

**CON TODO MI AMOR PARA TI EDGAR.**

# INDICE

INTRODUCCION A LAS REDES LOCALES -----	1
RED DE AREA LOCAL-----	2
CLASIFICACION DE LAS REDES -----	2
ELEMENTOS FUNDAMENTALES DE UNA RED -----	3
1.    SERVIDOR -----	3
TIPOS DE SERVIDORES-----	3
CLASIFICACIÓN DE SERVIDORES -----	4
CONSIDERACIONES PARA SELECCIONAR UN SERVIDOR -----	6
2.    ESTACIONES DE TRABAJO -----	9
3.    IMPRESORA -----	10
4.    TARJETAS DE INTERFASE -----	10
5.    CABLEADO -----	10
6.    ELEMENTOS ADICIONALES DE SEGURIDAD -----	11
7.    FUENTE ININTERRUMPIBLE DE PODER -----	11
8.    UNIDAD DE RESPALDO -----	11
EL MODELO CLIENTE-SERVIDOR -----	12
ELEMENTOS DE LA ARQUITECTURA CLIENTE-SERVIDOR -----	13
MODELO OSI. OPEN SYSTEM INTERCONNECTION -----	14
LAS CAPAS DEL OSI -----	16

TOPOLOGIAS -----	17
TOPOLOGIA ANILLO -----	18
TOPOLOGIA ESTRELLA -----	19
TOPOLOGIA BUS -----	20
PROTOCOLOS Y ESTANDARES -----	21
ESTANDARES DE REDES LOCALES -----	21
PROTOCOLOS DE COMUNICACION -----	22
TIPOS DE PROTOCOLOS -----	22
ETHERNET -----	22
TOKEN RING -----	24
ARCNET -----	27
TIPOS DE CABLEADO -----	29
COAXIAL -----	29
PAR TORCIDO -----	30
FIBRA OPTICA -----	31
COMUNICACION ENTRE REDES -----	32
REPETIDORES -----	32
PUENTES -----	32
RUTEADOR -----	33
GATEWAYS -----	35

INSTALACION DEL NETWARE -----	36
GENERACION DEL SOFTWARE DE RED DE LA ESTACION -----	38
EJECUCIÓN DEL SOFTWARE DE RED DE LA ESTACIÓN -----	41
EJEMPLOS DE ARCHIVOS AUTOEXEC.BAT PARA ACCESAR A LA RED -----	42
CLASIFICACION DE LOS USUARIOS DE LA RED -----	43
ESTRUCTURA DE LA RED -----	43
SEGURIDAD -----	44
NIVELES DE SEGURIDAD -----	44
COMANDOS UTILIZADOS PARA EL MANEJO DE ATRIBUTOS -----	46
COMANDOS UTILIZADOS PARA ACCESAR EL SISTEMA -----	48
COMANDOS PARA MANEJO DE IMPRESIONES -----	49
COMANDOS UTILIZADOS PARA MANEJO DE ARCHIVOS -----	49
COMANDOS UTILIZADOS PARA MANEJO DEL SERVIDOR -----	50
COMANDOS UTILIZADOS PARA MANEJO DE DIRECTORIOS Y VOLUMENES -----	51
COMANDOS UTILIZADOS PARA EL MANEJO DE LA CONSOLA -----	51
MENUS DE UTILERIAS -----	53
UTILERIAS PARA LA CREACION DE CUENTAS DE USUARIOS -----	58
BIBLIOGRAFIA -----	60

## **INTRODUCCION A LAS REDES LOCALES**

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

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

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

Hacia la mitad de la década de los 70's la tecnología del Silicio y la integración en miniatura permitió a los fabricantes de computadoras construir mayor inteligencia en máquinas más pequeñas. Estas máquinas llamadas microcomputadoras descongestionaron a las viejas máquinas centrales. A partir de ese momento cada usuario tenía su propia microcomputadora en su escritorio.

A principios de la década de los 80's las microcomputadoras habían revolucionado por completo el concepto de computación electrónica así como sus aplicaciones y mercado. Los gerentes de los departamentos de informática fueron perdiendo el control de la información puesto que el proceso de la misma no estaba centralizado. (Las aplicaciones en el proceso centralizado residen exclusivamente en la computadora central y al ser invocadas por las terminales, ésta se ocupa del proceso y requerimientos del programa, el procesador es compartido y tiene que dividir el tiempo de proceso entre todos los usuarios).

Sin embargo de alguna manera se había retrocedido en la forma de procesar información. Había que "acarrear" la información almacenada en los diskettes de una micro a otra y la relativa poca capacidad de los diskettes hacía difícil el manejo de grandes cantidades de información.

*A ésta época se le denomina "La era del floppy disk".*

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

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

## ***DEFINICION DE RED DE AREA LOCAL***

Una Red de Area Local es un conjunto de dispositivos electrónicos interconectados con el objetivo de comunicarse entre sí y compartir recursos tales como impresoras, discos duros, datos, aplicaciones, etc.

El objetivo principal es, el de compartir hardware y software disponible para lograr un mejor rendimiento en los sistemas de información mediante la optimización de tiempo y costo.

Una red sencilla ( ó básica) se compone de:

- Un servidor de archivos
- Estaciones de trabajo
- Impresora.

Las conexiones físicas entre estaciones y el servidor está compuesta de tarjetas de red, cables y conexiones de cable. El software de conexión entre estaciones y el servidor es el Netware de la estación de trabajo y el servidor.

### *Clasificación de las Redes:*

- *LAN:*  
Redes de Area Local (Local Area Network)
- *MAN:*  
Redes de Area Metropolitana
- *WAN:*  
Redes de Area Amplia (Wide Area Network)

## ***ELEMENTOS FUNDAMENTALES DE UNA RED***

Al seleccionar una red es importante conocer los elementos que la componen, ya que se requerirá que la red responda a nuestras necesidades.

Entre éstos elementos contamos con: Servidor, Estaciones de Trabajo, Tarjetas de Interfase, Cableado para interconectar los equipos, y el Sistema Operativo.

No existe una regla específica sobre cual de todos los elementos hay que escoger como el primero. Son nuestros requerimientos los que nos guiarán en tal decisión.

### ***Elementos Básicos:***

#### **1. SERVIDOR**

Es la computadora central que nos permite compartir recursos y es donde se encuentra alojado el sistema operativo de red, a fin de controlar la red de computadoras.

Todos los archivos disponibles para los usuarios de la red se almacenan en el disco duro del servidor. Comparte y organiza información, vigilando siempre el nivel de autorización del usuario, protegiendo la seguridad del sistema y la integridad de los datos.

Es la computadora donde arranca la red; puede ser Dedicado (solamente se puede utilizar como Servidor) y No-dedicado (se puede utilizar como ambos Servidor y Estación de Trabajo).

Para tener una mejor idea de los antecedentes de los servidores, se hará un poco de historia. En las épocas de los *mainframes*, todas las actividades de computación se encargaban a un gran procesador, que tenía tareas múltiples o podía manejar varias operaciones a la vez. Este mismo manejaba la lectura y escritura en el disco, la escritura en una cinta de respaldo, corría todas las bases de datos (contabilidad, inventario, personal), proporcionaba procesamiento de palabras y coordinaba el flujo de información hacia todas las estaciones de trabajo enlazadas. Este procesador único dividía sus recursos entre cada una de tales tareas.

Con un servidor para redes, todas estas actividades no se corren en un solo procesador grande, sino que se efectúan en conjunto en una red de computadoras con un procesador más pequeño.

Los procesos que en el pasado se combinaban en un *mainframe*, se dividen y se distribuyen entre computadoras individuales; algunos ejemplos son la impresión, las bases de datos y el manejo de archivos.

#### ***Tipos de Servidores***

Antes de proseguir, cabe aclarar que los servidores se distinguen en comunes o tradicionales, como son los de archivos, y en servidores de aplicaciones. A continuación se enumeran las clasificaciones más importantes y se hace una pequeña descripción de las características de cada una.

Con la posible excepción de un servidor tradicional de archivos, los servidores de aplicaciones por lo común requieren los servicios de otros servidores de aplicaciones para operar en forma adecuada. Esto implica que, en una red, deben integrarse varios tipos de servidores de aplicaciones que trabajen en "equipo" y dependan unos de otros. Si la selección de las diversas tareas y su asignación al servidor adecuado se efectúa cuidadosamente, los usuarios obtendrán magníficos tiempos de respuesta.

## **Clasificación de Servidores:**

- **Servidor de Archivos**

La función principal de un servidor de archivos es permitir acceso al disco desde las estaciones de trabajo en la red. Con Netware, por ejemplo, se aconseja que este servidor sea una máquina dedicada (no puede funcionar como estación de trabajo).

La tarea principal de la máquina dedicada es ofrecer E/S de archivos para los usuarios coordinando todo acceso a los controladores de disco de la red. Además, los servidores de archivos de Novell también ofrecen otros servicios tales como supervisar a los usuarios, administrar los recursos de la red y proveer mayor seguridad.

Un proceso de servidor que requiera una máquina dedicada se denomina con frecuencia proceso Cliente-Servidor.

- **Servidor de Impresión**

Los servidores de impresión también pueden requerir máquinas dedicadas o estar dispersos en toda la red en diferentes estaciones de trabajo. Las funciones básicas de un servidor de impresión son coordinar, supervisar y ejecutar la impresión. Debe ordenar los trabajos en colas de impresión, así como asignarlos a las diferentes impresoras con que cuenta la red.

Originalmente, su función se limitaba a iniciar y detener los trabajos de impresión, o bien, a redireccionarlos a una impresora específica, y funciones tales como la administración de los tipos (*fonts*) y de las formas recaían en el usuario.

Además, han comenzado a salir al mercado algunos paquetes que permiten, por ejemplo, una opción de contabilidad que da al administrador de la red una visión precisa de la actividad de la impresión de ésta; proporcionan datos tales como quién está imprimiendo, en qué tipos de impresoras o la cantidad de papel que se utiliza en un día. Esta información puede ayudar al administrador a planear el crecimiento de la red, en cuanto a equipos de impresión y orientarlo en la compra de equipo con respecto a la velocidad y las características adecuadas de éstos.

En la mayoría de los casos se enlazarán a una estación de trabajo una o dos impresoras, a la cual se denominará servidor de impresión. El desarrollo en la tecnología del servidor de impresión permite correr el software del servidor de impresión en el servidor de archivos y hacer que la impresora esté conectada directamente al cable de red a través del puerto para impresora de la red. Algunas nuevas impresoras tienen el adaptador integrado.

- **Servidor de Base de Datos**

También se ha advertido una evolución en los servidores de bases de datos. Tradicionalmente éstos han sido máquinas dedicadas que contienen toda la base de datos. El motor de base de datos, las tablas y las herramientas de investigación residen en el servidor, mientras que toda o parte de la interfase del usuario se encuentra en la estación de trabajo del cliente. El papel del servidor de base de datos no está muy claro cuando hay servidores múltiples o cuando hay varios servidores de base de datos esparcidos en la red.

- **Servidores de Comunicaciones**

Estos ofrecen una puerta hacia y desde la red local para la entrada/salida de comunicaciones sincrónicas y asincrónicas, módems, redes X.25, computadoras *host* y otras redes, siendo éstas sólo algunas de sus posibilidades de conexión.

- **Servidores de Administración**

Algunos fabricantes han introducido este concepto al mercado a través de productos que se fundamentan en una serie de "servidores inteligentes distribuidos" para recopilar, analizar y procesar información que se relaciona con la administración para segmentos individuales de red.

De ésta manera, la información basada en el servidor puede accesarse a través de consolas de administración de ubicación central, donde el administrador de la red puede analizarla.

Estos servidores se han diseñado para ubicarse en forma permanente en un segmento de la red, desde donde continuamente supervisan y analizan el tráfico de la red.

Uno de los beneficios más importantes de su enfoque basado en el servidor de aplicaciones es que minimizan el tránsito de la red que se relaciona con la administración. Esto se debe a que los servidores distribuidos analizan los datos en forma local, de tal manera que únicamente el análisis (y no todos los recopilados) se envían del servidor a la consola.

- **Servidores de Respaldo**

Como su nombre lo implica, los servidores de respaldo se dedican a la provisión de facilidades centralizadas de archivo de datos y de recuperación. Algunos de los que ya existen en el mercado se han elaborado con base en *software* de cliente-servidor y este último corre en uno o más servidores de respaldo. El *software* cliente, que corre en cada PC de la red, determina los archivos a respaldar y los enruta a través de la red hacia el servidor, administra los medios de respaldo (cintas por lo general) y mantiene un índice de respaldos previos y de sus volúmenes asociados de medios. Este sistema permite a los servidores respaldar los archivos de cualquier cliente de la red.

El índice en línea de la historia de los archivos de respaldo también simplifica las operaciones de recuperación: a medida que los usuarios recorren el índice, observan posiciones históricas del sistema de archivos de la red, a momentos específicos. De esta manera es posible identificar y recuperar un archivo perdido con rapidez.

- **Servidores de Fax**

Los servidores de fax coordinan todas las transmisiones de fax para una red. Permiten a los usuarios de ésta enviar y recibir faxes en línea. Este tipo de servidores pueden proporcionar a cualquier usuario los números telefónicos correctos del destino. En ocasiones, pueden sustituir a los sistemas de correo regular y electrónico.

El servidor de fax es una combinación de *hardware* y *software* con conexiones tanto a la red (ésto puede ser a través de cualquiera de los conectores usuales Ethernet, Arcnet y Token Ring) como al sistema telefónico.

El servidor de fax trabaja junto con un servidor de archivos a fin de permitir a los usuarios enviar copias de sus archivos electrónicos en la red (documentos de hojas de cálculos o gráficas) directamente, a través del sistema telefónico a otra máquina de fax. En su aplicación, los usuarios especifican los archivos que desean se envíen, y el servidor accesa el servidor de archivos correspondiente para recuperar los archivos necesarios. Envía el fax por el sistema telefónico a través de su módem interno. Como resulta obvio, este proceso elimina varios pasos, como la impresión del archivo original en papel, su alimentación posterior a una máquina de fax para su transmisión. Además tiene ramificaciones de mayor alcance, en especial para organizaciones que necesitan enviar por fax copias múltiples de un solo documento.

Con el servidor de fax, el proceso de envío de faxes se puede automatizar, en forma muy semejante a una operación de *mail merge*. Esto significa, por ejemplo, que una compañía puede utilizar un servidor de fax para "publicar" docenas o incluso cientos de copias personalizadas de un boletín de prensa en forma electrónica, sin necesitar que alguien realice esta tarea en forma manual. Un servidor de fax requiere tener acceso a un servidor de archivos y a los servidores de procesamiento de palabra que se han almacenado en él cuando transmite información. Y es posible que requiera utilizar los recursos de un servidor de impresión para tener acceso a una impresora.

- ***Servidores de Correo Electrónico***

Estos servidores, a los que algunos han denominado "oficinas electrónicas de correo" controlan todo el correo entre los usuarios de la red.

Se han creado servidores especializados para otras aplicaciones importantes, como CAD (Computer Assisted Design; Diseño con ayuda de Computadora), visualización de documentos y planeación de proyectos.

Los servidores de procesamiento de imágenes permiten ingresar y conservar imágenes, que se han procesado en forma digital, tales como un cheque cancelado, a una base de datos.

Los de discos ópticos permiten el acceso a las enormes cantidades de información que se almacenan en los CD-ROM (Compact Disk Read-Only Memory)

Existen varias reglas que hay que tomar en cuenta para seleccionar el Servidor más adecuado, La más importante es que, éste sea compatible con el tipo de Sistema Operativo para red que se seleccione.

Adicionalmente, ésta máquina debe tener la suficiente capacidad de procesamiento para llevar a cabo las tareas de la red y contar con suficientes ranuras para expansión (tarjetas de expansión, tarjetas de interfase, etc.). El disco duro utilizado en el Servidor debe ser soportado por el Sistema Operativo de Red, ser del tamaño necesario para nuestra información pueda guardarse en él y además debe contemplar un posible crecimiento.

### ***Consideraciones para seleccionar un Servidor***

Cuando se considera el tipo de Servidor, solamente se toman en cuenta dos características, tipo de procesador (386,486) y velocidad de reloj (20, 25, 33, ó 50 Mhz)

Estos dos parámetros son importantes por sí mismos, son sólo dos de los muchos elementos que se deben considerar antes de tomar una decisión en cuanto al tipo de Servidor que requiere una red.

Elementos como el tipo de disco duro, controladora, número de ranuras (slots) de expansión disponibles, puertos seriales y puertos paralelos, memoria total, fuente de poder, capacidad de crecimiento, elementos de seguridad de hardware y otros, son tan importantes como el procesador y la velocidad que utiliza la computadora, para obtener el mejor rendimiento y confiabilidad de la red

### ***Tipo de Procesador***

El tipo de Procesador que utilice el Servidor está estrechamente ligado con el Sistema Operativo de Red. El Procesador ideal para Servidor de Red es el 80386, 80386DX, u 80486. Utilizar procesadores 286 ó 386SX, en el servidor es desperdiciar las características que tienen los 80386 en adelante, porque, el Intel 80386SX, procesa la información a 32 bits, pero se comunican con el resto de los elementos de la computadora a 16 bits, tales como memoria, canales de disco, tarjetas de red. El 80386, 486 SX, y 486, lo hacen a 32 bits, e inclusive el 486 lo puede hacer a 64 bits.

Los Sistemas Operativos de Red como el Netware 3.11 o el LAN Manager (HPFS386), se han diseñado especialmente para los procesadores 386 y 486. Cuando Netware se utiliza en un 386SX, la comunicación entre el procesador y la memoria, en lugar de hacerse en un bus interno de 32 bits, se hace a 16 bits, con la consecuente pérdida de rendimiento en la velocidad del sistema. Esto no ocurre en Windows 3.0 ya que éste ambiente se diseñó para procesadores 286, y la comunicación de datos se hace siempre a 16 bits, nunca a 32 bits (el procesamiento interno en el procesador, si se hace a 32 bits).

### ***Multiprocesadores***

En el mundo de las redes locales, los servidores multiprocesador empiezan a ser una realidad. En la actualidad, Acer, Compaq, AST, Digital, y otras empresas cuentan ya con productos multiprocesador. Son en este caso los fabricantes de sistemas operativos de red (Novell, Microsoft, Banyan, etc) quienes deben seleccionar el enfoque de procesamiento múltiple, para sus respectivos productos.

Novell y Microsoft han optado por el enfoque asimétrico, que consiste en un procesador maestro que, cuando se encuentra saturado, entrega tareas al segundo procesador y así, sucesivamente. En el mundo Unix el enfoque ha sido el opuesto: procesamiento simétrico, el cual se basa en llevar tareas hacia el arreglo de procesadores en forma balanceada.

El primer enfoque puede concebirse como llenar primero un tinaco y después pasar al segundo y el simétrico como llenar los dos tinacos al mismo tiempo.

### ***Velocidad de Reloj***

La velocidad de reloj, medida en millones de ciclos por segundo (Mhz), indica el número de veces por segundo que el procesador ejecuta un ciclo de máquina, que no es el mismo que una instrucción. Esta es una de las grandes ventajas entre el procesador 80386 y el 80486.

Por ejemplo, para efectuar una suma, el procesador 80386 requiere de varios ciclos de máquina para arrojar el resultado. El primer ciclo puede ser tomar el primer dato, el segundo tomar el segundo dato, el tercer efectuar la operación y el cuarto arrojar el resultado.

El Procesador 486 maneja el tipo de instrucciones reducidas que se utilizan en los procesadores llamados RISC, esto es, en el primer ciclo toma ambos datos junto con la solicitud de operación (suma), y en el segundo ciclo se arroja el resultado. Esta es una de las grandes ventajas del *bus* interno de 64 bits. La diferencia entre el procesador 80386 y el 80486 es que este último, requiere mucho menos ciclos de máquina para la misma operación, con el consecuente beneficio en velocidad de respuesta del sistema.

## **Disco Duro y Controladora**

Existen en el mercado 5 tipos de discos duros y controladoras de disco:

- MFM: Utilizado en los primeros discos duros de baja capacidad que aparecieron en las microcomputadoras.
- RLL: El disco es idéntico, cambia la controladora, permite aumentar la capacidad de almacenamiento del disco y su velocidad de acceso.
- IDE: Interfase inteligente, es tendencia actual en discos de baja y mediana capacidad (150 Mb).
- ESDI: Interfase muy rápida, que está dejando el paso a la interfase SCSI
- SCSI: Interfase muy rápida, es la tendencia actual en discos de mediana y alta capacidad (200 Mb en adelante)

Tener un servidor de red, con discos de baja capacidad, tipo MFM, o de mediana o alta capacidad tipo IDE, es sacrificar otra vez, un servidor y un sistema operativo de red rápidos por un disco lento. El cuello de botella de la red será el disco duro del servidor, obteniendo una velocidad de respuesta global baja, en lo que a acceso a disco se refiere.

Las Interfases recomendables para servidores son: IDE en discos de baja capacidad y SCSI en discos de mediana y alta capacidad, por los siguientes motivos:

1. EL disco y la interfase IDE, resultan una alternativa mucho más rápida y económica que los antiguos discos MEM o RLL. Son la mejor opción en cuanto a velocidad de respuesta, para usos en DOS, Windows o redes de baja capacidad de disco. En instalaciones de 200 Mb en adelante, el disco duro puede empezar a ser un cuello de botella para los datos de entrada y salida.
2. Para instalaciones superiores a 200 Mb, la interfase SCSI es la mejor opción dada su alta velocidad de transferencia de datos, *bus* de 16 bits (ISA) o 32 (EISA), en redes donde se tiene una alta capacidad en disco, con discos y controladores SCSI el disco duro no se convierte en un cuello de botella.

Interfases de disco muy avanzadas son las manejadas por empresas como Compaq en el SystemPro o Acer en el AcerFrame 3000MP donde arreglos de disco (Disk Arrays) mantienen una alta velocidad de transferencia aun en capacidades cercanas o mayores al Gigabyte. En el caso del AcerFrame 3000MP, Acer utiliza el adac (Acer Disk Array Controller) que permite manejar los discos SCSI en *bus* de 64 bits, a través del *FrameBus* (*bus* de Acer de 64 bits)

## **Memoria**

Una de las características más importantes para que el servidor sea eficiente, es que cuente con una cantidad de memoria RAM suficiente, que permita al sistema operativo de la red hacer uso de intensivo de ella, para mejorar el rendimiento del sistema.

Netware es capaz de llevar a memoria RAM la tabla de directorios completa e inclusive archivos completos, lo que significa manejar una base de datos, con una gran cantidad de usuarios, en una especie de RAM *disk* multiusuario.

Esta característica incrementa en forma considerable la velocidad de respuesta del sistema. Netware es capaz de (gracias a que maneja el anillo 0 del procesador 386) de manipular las direcciones de memoria en forma dinámica, si un archivo es cerrado por un usuario, la memoria RAM que estaba siendo utilizada por ese archivo, es utilizada por otros recursos inmediatamente, esto permite tener una buena velocidad de respuesta sin necesidad de grandes cantidades de memoria.

LAN Manager, por estar basado en OS/2, utiliza direcciones de memoria definidas, que no son dinámicas, este enfoque tiene el mismo beneficio que Novell, con la desventaja que un servidor LAN Manager, suele requerir grandes cantidades de memoria, por lo que es importante considerar un servidor que permita un crecimiento en memoria en forma sencilla y económica (SIMMs de memoria)

### ***Ranuras de Expansión (slots)***

El servidor de archivos, puede llegar a requerir un crecimiento posterior, que se logrará a través de tarjetas de interfase, colocadas en las ranuras de expansión con que cuenta la computadora, por ejemplo tarjetas de red adicionales, tarjetas de expansión de memoria, controladoras de disco, tarjetas de puertos de serie y paralelo, módems, tarjetas de comunicaciones hacia otros ambientes (mini o mainframe).

## **2. ESTACIONES DE TRABAJO**

Las Estaciones de Trabajo son microcomputadoras interconectadas por una tarjeta de interfase, éstas compartirán recursos del Servidor y realizarán un proceso distribuido. Son esencialmente similares a las computadoras personales no conectadas en red, con la diferencia de que pueden lograr el acceso a archivos provenientes de otras unidades de disco, ubicados en el servidor, además de las unidades locales. Cada estación de trabajo procesa sus propios programas y archivos y utiliza una copia del sistema operativo MS-DOS. Es la computadora donde los usuarios van a realizar su trabajo.

El procesamiento de datos en una red es distribuido, por lo tanto el desempeño de la Estación de Trabajo se debe definir en función a la aplicación que se estará manejando en ella. Analizar el tipo de aplicaciones que se estarán manejando en la red es de suma importancia para lograr que la estación de trabajo cumpla con los requisitos necesarios.

Existen algunas reglas generales que hay que tomar en cuenta al seleccionar la estación de trabajo. Esta debe contar por lo menos con 640 KB de memoria, debe tener posibilidades de crecimiento tanto en ranuras de expansión como en capacidad para colocar un disco duro a una unidad de disco.

En el mercado existen estaciones de trabajo que no cuentan con disco duro o con unidades de disco flexible. En ellas el enlace al servidor se hace mediante la tarjeta de interfase de red, obteniendo seguridad de acceso y evitando lo más posible contaminación por "virus"

Este equipo es el más fácil de seleccionar, dado que en las instalaciones se cuenta normalmente con algún tipo de equipo PC-Compatible o Macintosh. Sólo será necesario agregar una tarjeta de interfase para que funcione dentro de la red. El equipo de la Estación de Trabajo deberá tener los requerimientos mínimos para la aplicación o aplicaciones que se estarán utilizando en la misma.

### 3. IMPRESORA

Una impresora adherida al Servidor para que todos los usuarios puedan mandar trabajos de impresión.

*Para ésto es necesario:*

Software de Conexión de Red: El software Netware de las Estaciones de Trabajo actúan como traductor entre el Netware y el DOS, éste reside en las estaciones e interpreta cada requerimiento proveniente del teclado o alguna aplicación. Entonces este direcciona el requerimiento al Netware o al DOS, según sea el apropiado, la impresora tiene un cable conectado directo al puerto paralelo del Servidor.

Cuando un usuario está listo para imprimir, la aplicación envía un archivo de impresión una a "cola" (un archivo conteniendo una lista de archivos para imprimirse en el servidor), entonces el Servidor envía los archivos en cola, a la impresora.

Si la impresora está ocupada, el Servidor guarda el archivo dentro de la cola hasta que la impresora esté disponible

### 4. TARJETAS DE INTERFASE

Las tarjetas de interfase nos permitirán el enlace entre microcomputadoras. Adapta a la PC para comunicarse a través de una red de área local. Para establecer comunicación hace uso de uno o más recursos del sistema en el cual están instalados.

Los recursos configurados se dedican en forma exclusiva a la tarjeta, no pueden ser compartidos con otras opciones de hardware esto significa que pueden ocurrir problemas si dos o más opciones tratan de usar en forma simultánea un mismo recurso.

Existen dentro del mercado una gran cantidad de tarjetas de interfase y no existe una cifra exacta de la base instalada (cantidad de tarjetas instaladas en el mundo) de cada una de ellas. La mayoría de los estudios muestran el predominio de las tarjetas Ethernet, Arcnet y Token Ring.

### 5. CABLEADO

Las redes utilizan diferentes tipos de cable para su conexión, éstos pueden ser:

- Cable Coaxial
- Par Torcido
- Fibra Optica

El cable que se utilice en las instalaciones será de suma importancia ya que cada uno de los diferentes tipos de cable nos indicará la distancia máxima que se pueda llegar a alcanzar entre nodos, nodo y repetidor pasivo o activo. Todo esto dependerá de la ubicación física de las máquinas que estarán conectadas dentro de la red.

También es importante tomar en cuenta el tipo de topología que se estará utilizando, ya que ésto también nos indicará el cable a ser utilizado.

Actualmente las instalaciones que más predominan son las de cable coaxial, básicamente por su costo y la facilidad de instalación. Este tipo de cable utiliza para las topologías Arcnet y Ethernet, aunque también se utiliza el cable telefónico para Ethernet.

El cable telefónico nos permite una distancia menor, es más barato y fácil de instalar ya que se pueden utilizar los ductos por los cuales están pasando las líneas del conmutador que tenemos instalado en el edificio.

El cable grueso (de color amarillo), al igual que la fibra óptica, se utiliza cuando las distancias son muy grandes o cuando el cable va a estar pasando por áreas de gran concentración magnética, se utiliza exclusivamente para Ethernet.

Es el software el que se encarga de administrar los recursos que se estarán compartiendo (Discos Duros, Impresoras, etc. ) y a los usuarios.

El software de conexión de entre Estaciones de Trabajo y Servidor es el software llamado Netware. El Sistema Operativo se selecciona según las necesidades de control de nuestra información.

Existen algunas consideraciones como son: el tipo de información que se estará compartiendo, los programas que se utilizarán, quién tendrá acceso a cierta información , etc. El Sistema Operativo seleccionado nos debe dar toda la seguridad que se requiera dentro de la red. Esta debe ir desde que máquina se pueda usar, a que hora se puede entrar a la red y que día se puede trabajar, hasta que clave de acceso tendremos, los archivos que se podrán compartir o los programas que se ejecutarán.

## 6. ELEMENTOS ADICIONALES DE SEGURIDAD

Los sistemas operativos de red, tienen elementos de seguridad por software. Es muy recomendable que el servidor, en su propio *hardware* tenga elementos de seguridad, tales como:

- **Password modo monousuario:** Obliga al usuario a dar un password al encender el equipo.
- **Password de servidor:** Obliga al sistema a arrancar desde disco duro, deshabilitando el teclado hasta que se de el password.
- **Password para deshabilitar el teclado:** permite al usuario usar el sistema hasta que haya dado un *password* (mientras está operando el sistema)
- **Control de Arranque por diskette:** Evita que el sistema operativo u otros programas sean copiados al *diskette* del servidor.

## 7. FUENTE ININTERRUMPIBLE DE PODER

Llamado normalmente *No-Break*, no es un elemento interno al servidor, sin embargo es uno de los dos elementos indispensables para garantizar la correcta operación de la red. Si se va la luz, y la información que está en la memoria RAM del servidor no es salvada a disco duro, la tabla de directorios puede corromperse y requerir correr procesos de regeneración, los *No-Break* llamados inteligentes, permiten al sistema, una vez que se va la luz, salvar todo a memoria, cerrar todos los archivos y apagarse automáticamente, son la mejor opción en lo que a *No-Break* para servidor refiere.

## 8. UNIDAD DE RESPALDO

Es el segundo elemento indispensable para garantizar la correcta operación de una red. La pérdida más cara que puede tener una empresa, es la de pérdida de información, que no puede recuperarse. Al igual que los *No-Break*, es importante que el elemento de respaldo sea rápido, confiable, y compatible con el sistema operativo de la red. Todos los servidores deben tener *No-Break* y unidad de respaldo.

## **EL MODELO CLIENTE-SERVIDOR**

Para definir este modelo, voy a tomar una analogía del mundo cotidiano; del mundo de oficinas.

En el modelo tradicional el jefe (cliente), solicita a la secretaria (servidor) el archivo de un proveedor (paso 1). Esta escucha la petición, se dirige al archivero (paso 2) y lleva a la oficina del jefe el archivo solicitado. El jefe abre el expediente analiza una serie de datos (paso 3), para tomar una decisión (paso 4). Hecho esto, vuelve a llamar a la secretaria, a quien le entrega el archivo (paso 5) que es puesto de nuevo en el archivero (paso 6).

Si se lee de nuevo el párrafo anterior, y se cambia la palabra jefe por cliente secretaria por servidor, se advertirá que, para un proceso de toma de decisiones relativamente sencillo, se intercambiaron una gran cantidad de información entre el jefe y la secretaria.

*En el modelo cliente-servidor, el caso del jefe-secretaria se daría de la siguiente forma:*

El jefe (cliente) solicita a la secretaria (servidor) que consulte en el archivero (paso 1) cierta información referente a un proveedor. La secretaria abre el archivero, consulta la información (paso 2) le da al jefe el dato preciso que él necesitaba (paso 3). Finalmente guarda la información en el archivero (paso 4). Además de que el flujo de información es más dinámico entre el jefe y la secretaria, dos intercambios en lugar de tres, en el modelo cliente-servidor, mientras la secretaria busca y selecciona la información que le fue requerida, el jefe trabaja en otra cosa, como puede ser atendiendo una llamada telefónica, o bien, trata otro asunto en su oficina.

Como se puede observar, la ventaja del modelo cliente-servidor es que permite que las tareas se repartan en forma más eficiente entre los elementos involucrados (cliente-servidor) y que se minimice el intercambio innecesario de información entre ellos.

Dentro de los conceptos de sistemas de cómputo, y particularmente en el mundo de las redes de computadoras, el modelo cliente-servidor resulta útil en instalaciones donde se tiene un servidor de base de datos poderoso, que está dedicado exclusivamente a dar servicio de proceso de información en la base de datos, y una cantidad importante de estaciones de trabajo (clientes) que son procesadores menos poderosos.

Son precisamente las aplicaciones de base de datos las que mejor pueden aprovechar el modelo cliente-servidor, aunque no las únicas, tareas tales como servidores de impresión, de comunicaciones, de fax que son también instrumentaciones del modelo cliente-servidor, donde una computadora se encarga de llevar a cabo una tarea específica mientras que el cliente lleva a cabo otras.

## **ELEMENTOS DE LA ARQUITECTURA CLIENTE-SERVIDOR**

Además de los elementos tradicionales de computadoras, cableado, tarjetas de red, y sistema operativo de red, para tener aplicaciones cliente-servidor se requiere una serie de elemento *software*.

El primer elemento es la máquina de base de datos (Database engine), tales como el SQL Base de Grupta, el Netware SQL Server de Novell, el SQL Server de Microsoft, o el Oracle SQL, por mencionar algunos. Este tipo de productos no son un manejador de base de datos (como Dbase o Clipper). La maquinaria de base de datos dá la plataforma para que una computadora se convierta en un servidor de base de datos.

El segundo elemento es un manejador de base de datos que corre en dos computadoras al mismo tiempo, en el cliente y en el servidor.

La parte que corre en el servidor de base de datos se denomina *back-end* y la que corre en el cliente *front-end*. Algunos ejemplos de esto son Dbase 1.1, Clipper 5.0, Revelation 2.0, Informix, Paradox, XQL, SQL Windows.

En las aplicaciones tradicionales de bases de datos, es el archivo completo el que viaja desde el servidor de archivos a la estación de trabajo. Esta última procesa la información después de una serie de "preguntas y respuestas" que se llevan a cabo entre el servidor y la estación y, finalmente, devuelve el archivo.

El modelo cliente-servidor, la estación (cliente) pregunta al servidor de base de datos a través del *front end* y del *back end*. El servidor procesa la información y devuelve el resultado, el registro, no el archivo completo que el cliente demandó.

El proceso cliente-servidor, que se lleva a cabo en un *gateway* de comunicaciones es muy similar. La computadora *gateway* (servidor) que se encarga de las labores de comunicación entre el *host* y la estación de trabajo (cliente), le envía a este último solamente las pantallas necesarias y toma la información del teclado, pero el proceso de comunicaciones se lleva a cabo por completo en el *gateway* de comunicaciones.

Sin duda, el modelo cliente-servidor es el que le da a las redes locales la posibilidad de ir más allá de servicios de impresión o de archivos y el que permite que el proceso de información sea verdaderamente distribuido. Continuamente surgen aplicaciones en este modelo para todos los sistemas operativos de red. Esto con seguridad ayudará a desarrollar el verdadero proceso distribuido, que convierte a las redes de computadoras en piezas únicas del mundo de la computación.

## **MODELO OSI. OPEN SYSTEM INTERCONNECTION**

### **SISTEMA ABIERTO DE INTERCONECTIVIDAD**

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ha desarrollado una familia de estándares referentes a redes locales, conocido como el número 802. La diversidad de métodos de acceso, protocolos de línea, medios físicos, dispositivos conmutables, aplicaciones, etc. ha impuesto la necesidad de unificar criterios para encontrar una solución armónica y eficiente, que ahorre esfuerzos aislados y busque un nivel de compatibilidad a través del desarrollo de recomendaciones (estándares) de uso universal.

IEEE cuenta con un subcomité ISO (Organización Internacional de Estándares), que se dedica a los estándares relacionados con redes locales a través de su modelo OSI. Este modelo no está tan popularizado, ya que éste modelo surgió cuando ya existían en el mercado varios protocolos de comunicación muy populares y que actualmente no se ajustan a este modelo, por ejemplo el protocolo SNA de IBM. Lo que el modelo trata de lograr es una transparencia total para el usuario final que le permitirá tener una mayor interconectividad entre los diferentes tipos de computadoras que existen actualmente en el mercado.

El modelo OSI especifica 7 niveles. Cada uno de los cuales comprende una serie de funciones necesarias para la comunicación entre computadoras de diferentes marcas. Cada nivel usa a los niveles inferiores para comunicarse con su mismo nivel pero en otro equipo, y adicionalmente a cada nivel agrega o quita información dependiendo de que nivel se trate.

#### ***Nivel 1: Physical Layer (Capa Física)***

Este nivel está relacionado con el medio físico por medio del cual se transmite la información, es el que mantiene la conexión física activada o desactivada. Un ejemplo es el cable.

#### ***Nivel 2: Data Link Layer (Capa de Control de Enlace)***

Este nivel se refiere a las técnicas utilizadas para colocar la información en el medio físico, es aquí donde se definen los protocolos como pudieran ser CSMA/CD, Token Bus, etc.

#### ***Nivel 3: Network Layer (Capa de Red)***

Determina la forma de direccionamiento y entrega de la información.

#### ***Nivel 4: Transport Layer (Capa de Transporte)***

Este nivel provee la confiabilidad, transparencia del flujo de la información entre los usuarios, asegura que la información que se envió a cierto usuario haya llegado completo y con la veracidad que se merece.

#### ***Nivel 5: Session Layer (Capa de Sesión)***

Es en este nivel en donde se lleva a cabo toda la administración de las comunicaciones.

#### ***Nivel 6: Presentation Layer (Capa de Presentación)***

Este nivel nos provee con un formato común para la presentación de los datos y un lenguaje especial para mensajes, para lograr una total transparencia entre los usuarios, normalmente ANSI.

#### ***Nivel 7: Application Layer (Capa de Aplicaciones)***

Este nivel es el más completo ya que permitirá una total transparencia entre los usuarios de diferentes equipos de cómputo, a nivel de aplicaciones.

El éxito de éste modelo consistirá en que los fabricantes de los diferentes productos realmente se aseguren de que sus productos están apegados a éste modelo y que de ésta manera logren que el trabajo se haga con una total transparencia al estar inter-operando.

#### Ejemplo del modelo OSI en el Viaje Internacional de una Carta

El modelo OSI será analizado utilizando una analogía relativa al viaje de una carta desde que se escribe, hasta que el destinatario la recibe.

La carta se enviará desde Cuernavaca, México a Toronto, Canadá.

Pasos que seguirá la carta dentro del modelo desde su salida:

Capa 7.- El Lic. Pérez, Director en Cuernavaca, escribe a mano un memorándum al Sr. Smith, Director en Toronto.

Capa 6.- El memorándum es capturado y se imprime.

Capa 5.- El memorándum se coloca en un sobre y se pone en el correo.

Capa 4.- El correo de Cuernavaca recibe el sobre y lo envía al correo central en la ciudad de México.

Capa 3.- El correo central lo recibe y lo coloca en una bolsa con destino a Toronto.

Capa 2.- La bolsa se lleva al aeropuerto y es colocada en la salida adecuada para subirlo en el avión con destino a Toronto.

Capa 1.- El avión se lleva la carta a Toronto.

## Las Capas del OSI

La Capa de Aplicación proporciona la interfase entre los programas del usuario y la red.



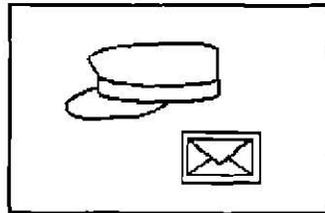
Capa 7  
El Sr. Smith lee el memorándum

La Capa de Presentación da el formato y el lenguaje comunes a los mensajes.



Capa 6  
La secretaria del Sr. Smith abre la carta y traduce el memorándum.

La Capa de Sesión maneja y sincroniza las conversaciones entre dos aplicaciones.



Capa 5  
El cartero entrega en la oficina del Sr. Smith la carta.

La Capa de Transporte provee un flujo de datos confiable y transparente entre usuarios finales.



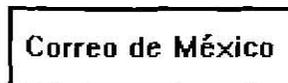
Capa 4  
La carta llega a la oficina postal para ser entregada.

La Capa de Red direcciona las comunicaciones.



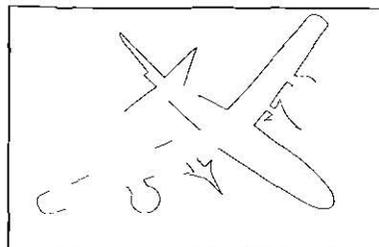
Capa 3  
La bolsa del correo es entregada a la oficina postal regional, donde se define si es local o se dirige a otra oficina.

La Capa de Control de Enlace proporciona control de errores y sincronización.



Capa 2  
El área de recepción del aeropuerto se asegura que la bolsa haya llegado.

La Capa Física activa, mantiene y desactiva la conexión física.



Capa 1  
El avión llega a Toronto.

## **TOPOLOGIAS**

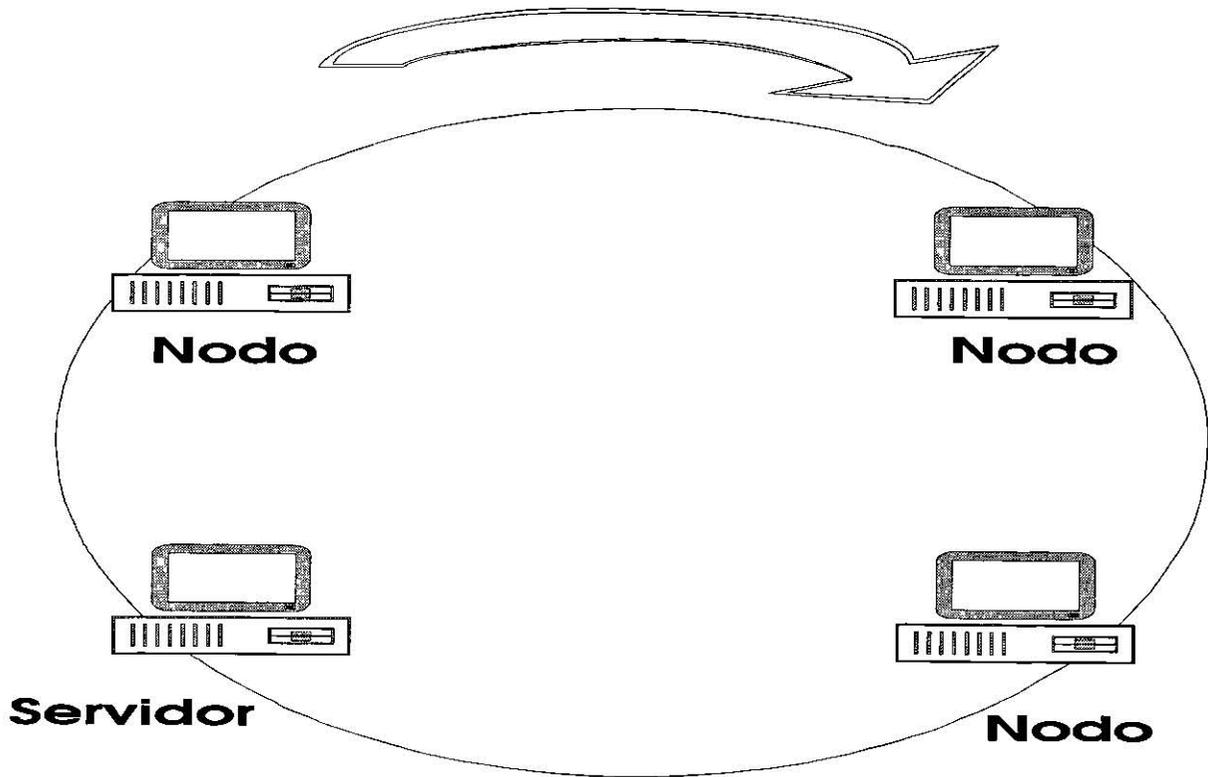
La Topología es la forma física o lógica como se conecta una red y la forma de la misma. Topología física es la forma o arreglo físico como está configurada la red, y topología lógica es la manera de como se distribuye la información dentro de la red, hay diversas topologías que pueden darle una determinada configuración a la red, pero todas éstas se derivan de las topologías básicas que son:

- Anillo
- Estrella
- Bus.

La Topología de la red se refiere a cómo se establece y se cablea la red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red

# TOPOLOGIA ANILLO

## Trayectoria de la Señal

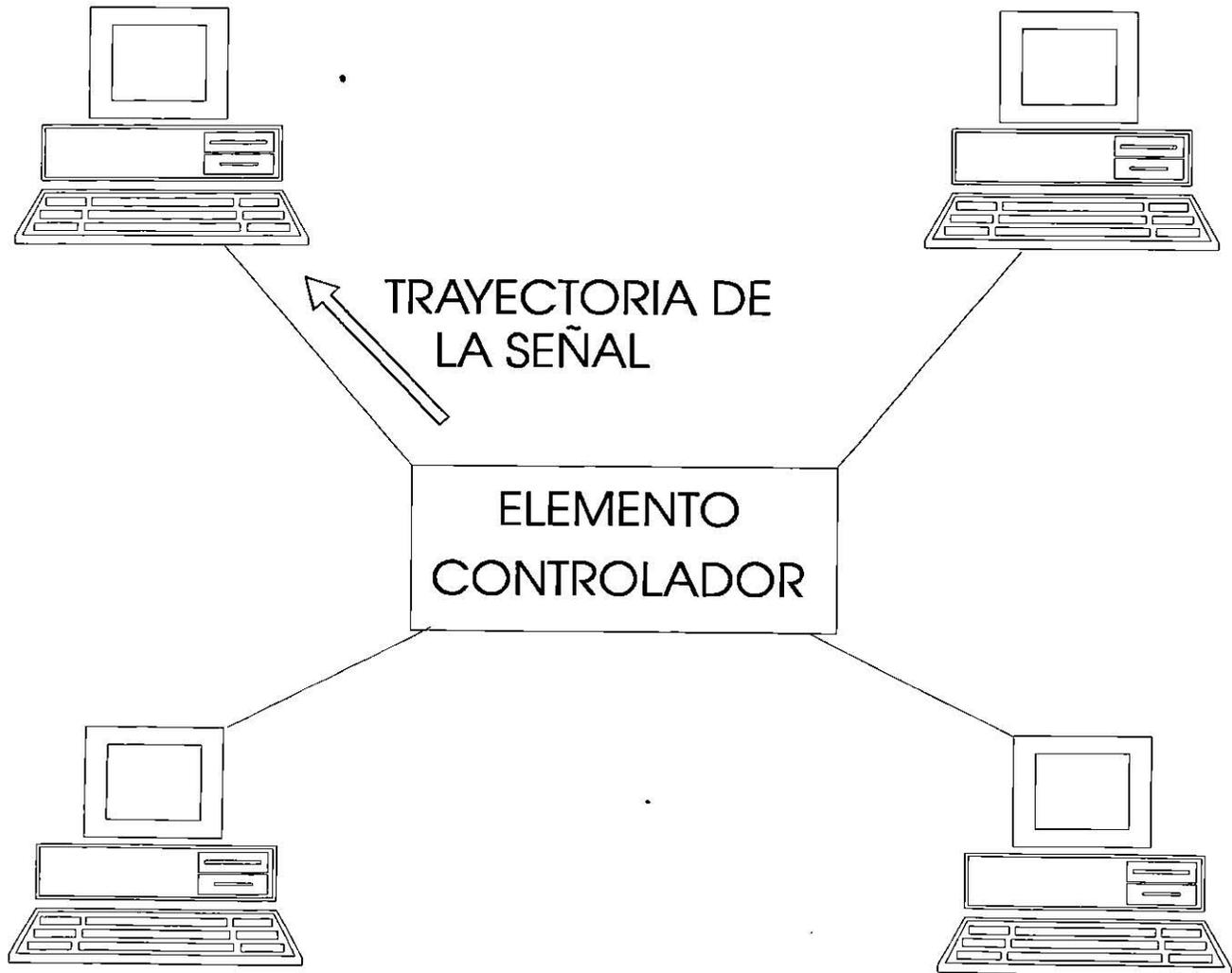


Esta Topología consiste en varios nodos (estaciones de trabajo) que están conectados en una serie circular cada uno conectado al siguiente nodo, un anillo no representa realmente un medio de difusión, sino una colección de enlaces punto a punto individuales que conforman un círculo, una desventaja de este tipo de enlaces es que en el momento en que un cable o nodo falle, el anillo también va a fallar. Corre a 2.5 Mbps y trabaja con repetidores activos a 600 m. de distancia, siendo la máxima en un repetidor, de 15m con respecto a un nodo. Este tipo de enlaces pueden funcionar en medios como par trenzado o fibra óptica.

En ésta topología la información viaja de manera lógica y cíclica por lo que el tiempo de respuesta no es muy atractivo y el tráfico es común además de que cada estación ó nodo debe esperar su turno para poder ejecutar algún proceso pues se encuentran conectadas físicamente en orden y la conexión inicia en la misma dirección donde termina. Por ello, cuando una estación deja de funcionar el total de la red se paraliza.

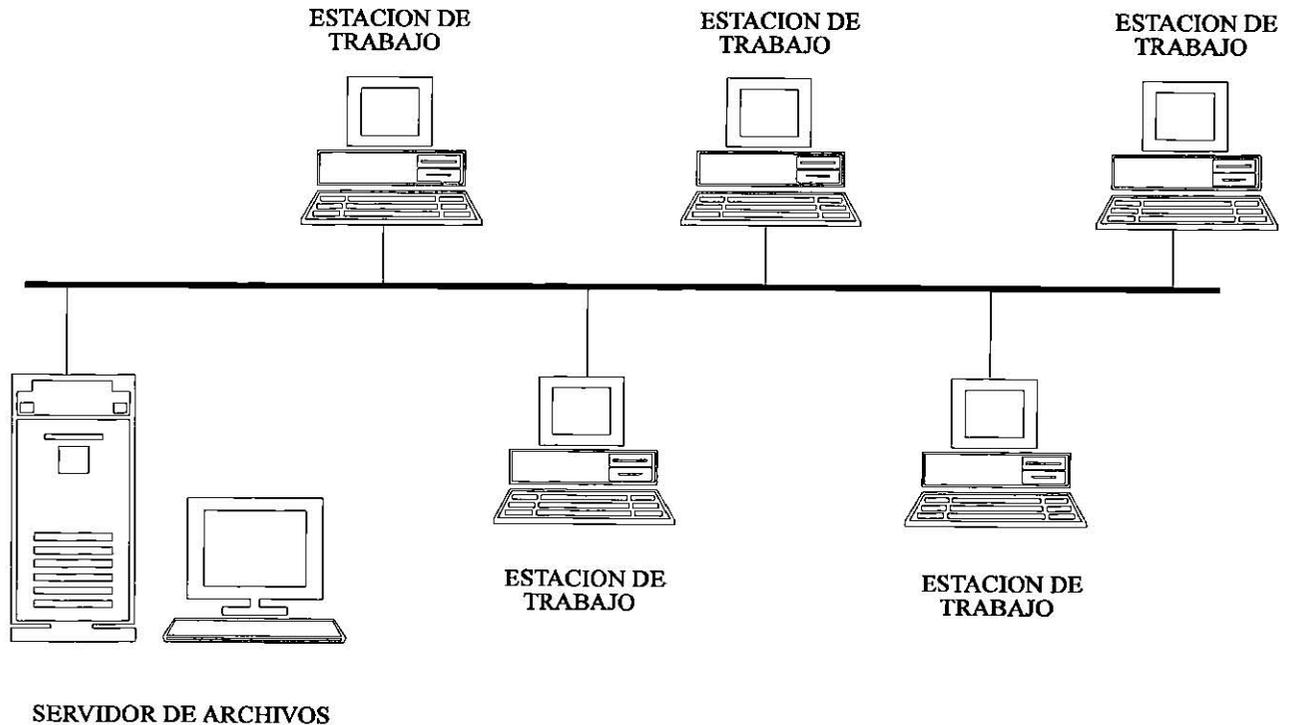
Trabaja en armonía en ambientes de oficina donde la carga de información no es muy grande o donde el procesamiento es similar para los 25 ó 40 usuarios que pueden acceder esta topología. Es una buena opción para aplicaciones que no requieren un tiempo de respuesta inmediato y por su diseño, es ideal para aquellas estructuras donde se dificulta la instalación de cableado.

# TOPOLOGIA ESTRELLA



Esta topología utiliza un dispositivo central, ya sea un servidor, un repetidor ó un alambrado central que está conectado directamente a las estaciones de trabajo. En este tipo de configuración se puede tener conectadas varias estrellas creando una cadena de estrellas. En este tipo de enlaces se utiliza principalmente par trenzado como medio físico de transmisión.

# TOPOLOGIA BUS



Esta topología consiste en varios nodos conectados que comparten el mismo cable (bus) conocido como línea troncal ó backbone. En este tipo de enlace el backbone puede ser un cable coaxial grueso, cable coaxial delgado, fibra óptica.

## **PROTOSCOLOS Y ESTANDARES**

### **ESTANDARES DE REDES LOCALES**

Los Estándares son un conjunto de lineamientos que todos están dispuestos a cumplir, en el mundo de la computación cuando se establece un estándar y un fabricante lo cumple se dice que es compatible. De ésta manera, los fabricantes pueden desarrollar productos de red que puedan desempeñarse con otros productos que a su vez también lo sean, con ésto no importa la marca de un producto. Mientras se apegue al estándar podrá comunicarse perfectamente con todos los que lo sigan.

Para las redes locales organizaciones tales como la Asociación de Ingenieros Electrónicos y Eléctricos (IEEE), principalmente, cuyo proyecto es el 802, desarrollan estándares de comunicación.

Este proyecto, en particular, tiene como finalidad establecer el procedimiento para lograr la comunicación entre los nodos de una red.

La Asociación, que tiene gran reconocimiento en esta industria, elabora documentos con los detalles del estándar a fin de lograr la conexión a través de la tarjeta de interfase.

Entre los más destacados se encuentran los siguientes:

- 802.1 Describe un modelo de referencia y proporciona un glosario.
- 802.3 Estándar de contención de bus (CSMA) para las redes Ethernet.
- 802.4 Estándar de *token bus* (token passing) para las redes Arcnet.
- 802.5 Estándar de Ethernet 10 Mb por cableado telefónico.

Gran parte de las redes existentes en el mercado utilizan alguno de éstos estandares para lograr la intercomunicación entre sus nodos.

## **PROCOLOS DE COMUNICACION**

En una empresa se requiere del trabajo en equipo, ésto no sólo se refiere a las herramientas de trabajo sino a una óptima comunicación entre los colaboradores. De tal manera, se requiere una solución que permita ese objetivo, y ésta es una red.

Las redes de computadoras necesitan del empleo de un protocolo que controle y administre la forma o "lenguaje" en que éstas se comunican.

Dado que existen diversos tipos de protocolos, las computadoras pueden establecer comunicación hacia otras con protocolo diferente a través de un puente o *bridge*.

Para lograr la comunicación entre los equipos se utilizan tarjetas de interfase que normalmente son las que manejan el protocolo, lo cual da como resultado una gran eficiencia en el funcionamiento de la red.

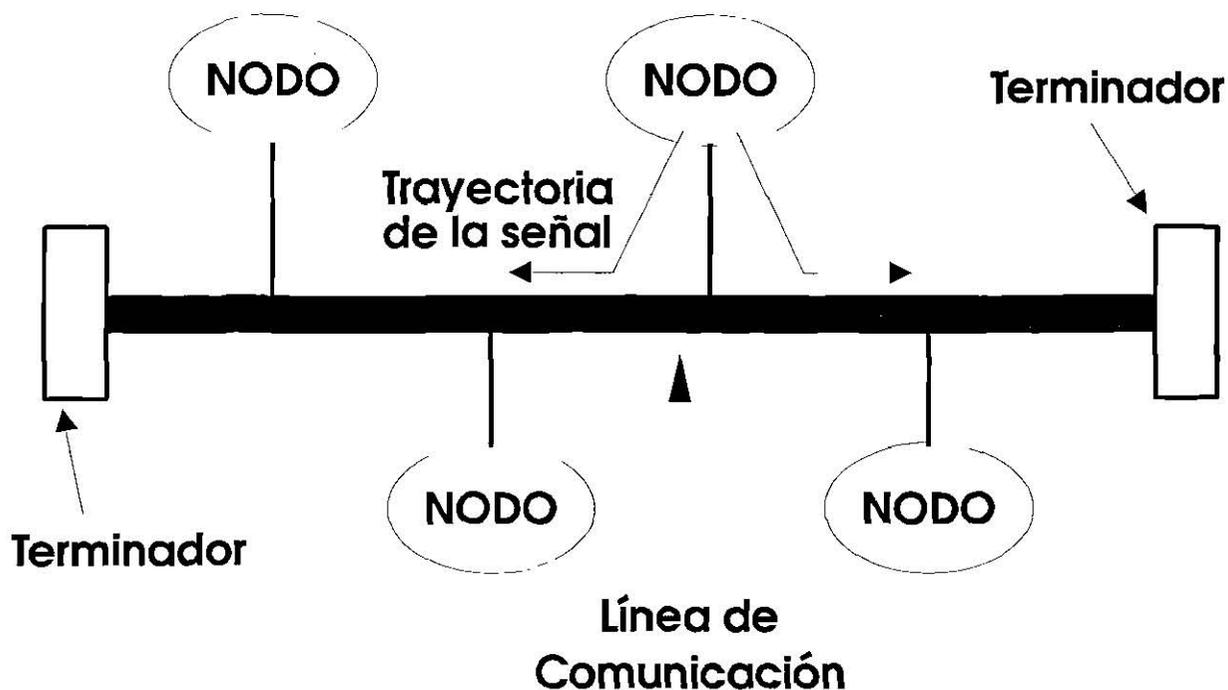
### ***Existen tres tipos de protocolos básicos para redes locales, a saber:***

- ***ETHERNET***

Que utiliza el detector de colisiones, que es el más comúnmente utilizado en topologías de bus, CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) Acceso múltiple del sentido del transporte/Detección de colisiones).

Funciona de la siguiente manera:

Cada nodo monitorea la línea común constantemente, entonces cuando una estación desea transmitir, escucha la información que fluye a través del cable, si el cable se encuentra ocupado la estación se espera hasta que esté en estado inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones en forma simultánea comienzan a transmitir a través del cable inactivo generan una colisión (detector de colisión) entonces terminarán su transmisión. Se basa en el principio de que cada estación tiene la misma oportunidad de utilizar la red. La especificación incluye un algoritmo de justicia que impide que cualquier estación o grupos de estaciones monopolice la red.



Para comprender mejor el proceso, es necesario aclarar que Ethernet es un sistema de red que utiliza un protocolo de contención, donde cada estación envía su propio paquete de información a través de un cable donde se encuentran conectadas las demás estaciones.

Ethernet se puede utilizar con distintas opciones de cableado, no requiere de aditamentos especiales y brinda entre otras ventajas la posibilidad de administrar recursos de hardware más fácilmente. El procesamiento y transmisión de datos es más rápido y atractivo.

Físicamente las estaciones de trabajo se conectan a través de un centro de cableado ó concentradores y estos podrán enlazarse a un bus de cable coaxial, fibra óptica o par trenzado,

Ethernet utiliza cable coaxial delgado para distancias cortas y coaxial grueso para distancias largas. Una ventaja de éste tipo de cable con respecto al de par trenzado es que soporta velocidades de transmisión de datos mucho más altos y puede utilizarse para conectar estaciones más lejanas, además de que resiste la interferencia electromagnética.

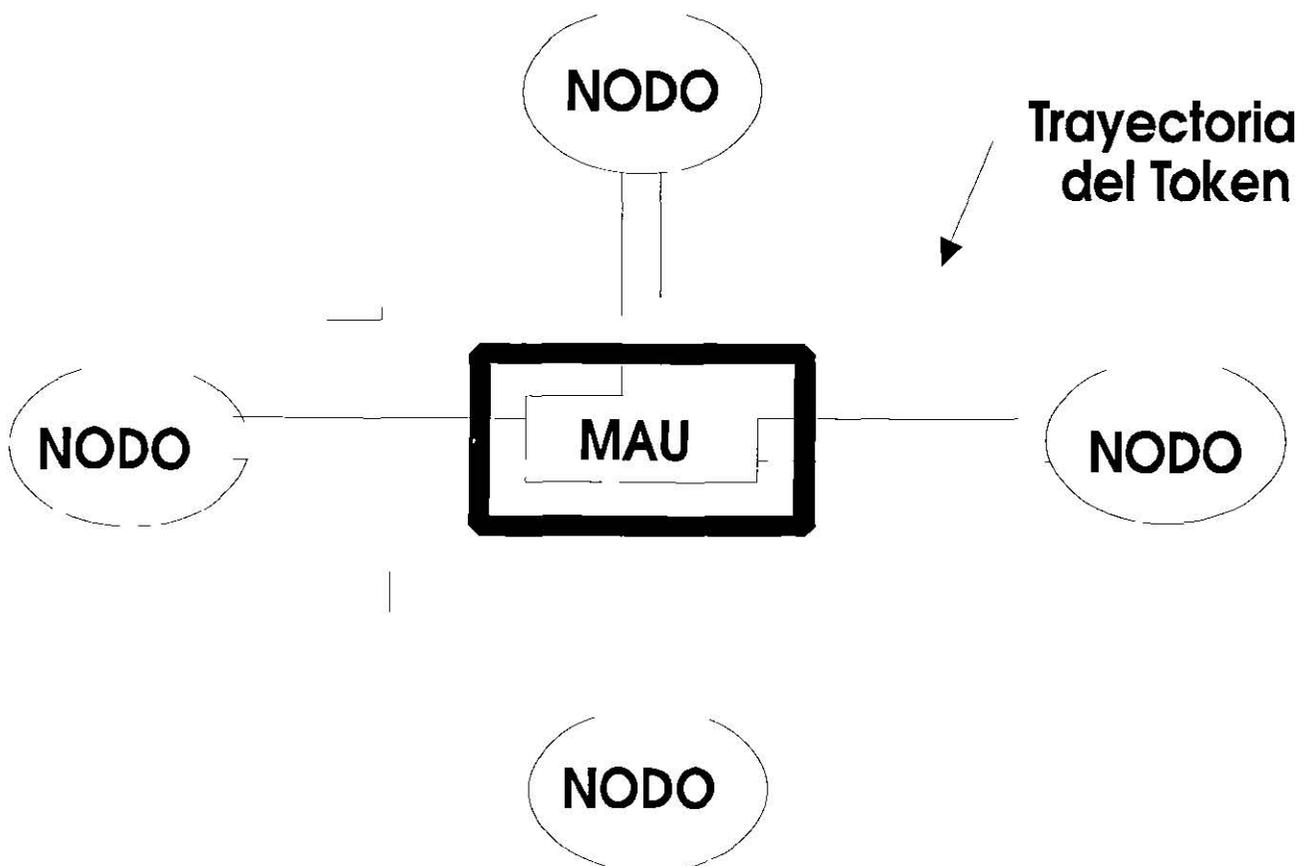
En resumen Ethernet, es atractivo por su precio, estandarización, sencillez en la instalación de cableado cuenta con el respaldo de diversos fabricantes, lo que permite a los usuarios con instalaciones de equipo distinto implantarlo sin el menor problema.

- **TOKEN RING**

Este estándar de comunicación consiste en una topología lógica de anillo. En éste estándar se tiene un patrón de bits especial el cual se le conoce como Token, el cual circula alrededor del anillo.

Cuando una estación quiere transmitir es necesario capturar el token que circula a través del anillo y quitarlo antes de efectuar la transmisión. Entonces se inserta un bit en el token para indicar que el token está ocupado y de ésta manera convertir el token en un frame (estructura de información), después se introduce la información detrás del bit insertado y posteriormente la información de control, después se envía a circular el frame alrededor del anillo hasta el nodo destino.

El nodo destino copia el frame y lo devuelve de nueva cuenta al anillo. A medida que regresan los bits que se han propagado alrededor del anillo, el transmisor los retira directamente del token. Este puede optar por almacenarlos con el objeto de compararlos con los datos originales para controlar la confiabilidad del anillo, o bien, desecharlos. Después de que la estación ha terminado de transmitir deberá generar un nuevo token.



El sistema de cableado o topología Token Ring se define como un anillo lógico con cableado tipo estrella, que obedece a la tecnología de Token Passing

Cada estación contiene una tarjeta de interfase de red que funciona como transmisor y receptor conectado a una unidad de acceso multiestaciones (MAU) ó a un concentrador de grupo que forma una configuración de estrella físicamente, internamente el cable forma dos pares, uno de entrada (recepción) y otro de salida (transmisión)

El MAU o el concentrador de grupo, convierte a esta estrella física en un anillo lógico al conectar cada estación con sus vecinas y proveer un círculo cerrado entre la primera y la última. Es de ésta manera que los datos se transfieren secuencialmente de una estación a otra obedeciendo a la tecnología de Token Passing.

Un MAU o un concentrador de grupo puede presentar 4, 8, 16 ó más puertos de conexión a estaciones y tiene además dos puertos de anillo, Anillo de Entrada (Ring In, RI) y Anillo de Salida (Ring Out, RO) que permiten la expansión de la red.

Cuando un dispositivo de éstos se utiliza standalone (solo), los puertos de RI, RO se cierran para formar un anillo interno con una ruta de respaldo. En los puertos de conexión a estaciones, un relevador cierra las conexiones para formar parte del anillo y en el caso de que un puerto no sea utilizado ó esté conectado a una estación inactiva, el relevador crea un bypass para evitar las pérdidas del anillo.

Expandiendo el anillo:

Generalmente las redes utilizan más de un dispositivo de conexión y éstos se entrelazan en cascada a los MAU's del puerto RO de uno al RI del siguiente. En este momento se crea una conexión redundante que forma dos anillos típicamente. La ruta principal en "X" y la de respaldo en "Y"

La combinación de anillos y rutas proveen un buen nivel de tolerancia a fallas para la red. Es importante mencionar que está comprobado que el 85% de las fallas y tiempos muertos que se presentan en una red local, se deben al cableado por lo que hablar de niveles tolerantes a fallas es una necesidad. Si existe una ruptura o un falso contacto en alguno de los segmentos entre MAU's, el mecanismo de respaldo se activa para rutear los datos por la ruta de respaldo evitando el punto de falla. La nueva ruta formada "Z" aún cuando es más larga que la original sigue formando un anillo completo.

Es muy común que una red con topología Token Ring tenga más de cien nodos. Sin embargo, los nodos raramente forman parte de un sólo anillo ya que esto acrecenta por mucho la probabilidad de fallas importantes dentro del sistema.

La solución que encontramos normalmente en el mercado es formar muchos anillos pequeños, unidos entre sí por dispositivos de puenteo y ruteo. Estos subanillos son mucho más sencillos de administrar y reparar, cuando al mismo tiempo ofrecen a la red un mejor rendimiento. Cabe mencionar que en gran medida el rendimiento de una red está íntimamente relacionado con el manejo de tráfico dentro de la misma.

Las redes corporativas generalmente se encuentran divididas en líneas departamentales, especialmente cuando todos los nodos de cada departamento se concentran en la misma área.

Entonces por ejemplo puede existir un anillo de mercadotecnia, otro para ventas, un tercero para compras, en fin todo irá de acuerdo a las necesidades. Al limitar el tamaño de un anillo se puede asegurar que los datos serán transferidos de una manera confiable y segura.

La diferencia principal entre estas dos maneras de enviar datos a través de la red es que en las redes del tipo Token Passing, como lo son Arcnet y Token Ring, un mensaje, o ficha (Token) se encuentra siempre circulando a una cierta velocidad, cada que ésta ficha pasa por una estación, se le encarga el envío de un paquete de datos al servidor o a otra estación. En las redes que utilizan protocolos de contención, como por ejemplo Ethernet, cada estación se encarga de enviar su propio paquete a través del cable, para lo cual debe checar previamente si el canal no es utilizado ya por otro paquete, en cuyo caso deberá contenerse y tratar de nuevo. En caso de que dos o más paquetes se envíen al mismo tiempo, el protocolo detecta colisión y pide a las estaciones que envíen nuevamente.

La norma para las redes basadas en el protocolo de contención de la asociación de ingenieros IEEE 802.3, a la que con frecuencia se denomina Ethernet, se basa en el principio de que cada estación tiene la misma oportunidad de usar la red. De hecho, la especificación incluye un algoritmo de justicia que impide que cualquier estación o grupo de estaciones monopolice la red. Mientras que por otro lado, Token Ring del IEEE 802.5 y el Token Bus Arcnet IEEE 802.4 incluyen una capacidad de prioridad, la cual permite que algunas estaciones tengan más acceso que otras.

El Token Passing ofrece la seguridad de que en el momento de paso de la ficha la estación enviará sus datos, sin embargo esto por lo general se compensa por la mayor velocidad de transferencia de las de contención.

Las colisiones son una parte normal de la operación en las redes de contención. Ethernet tiene colisiones al enviar mensajes, pero éstas son una parte integral del método de acceso de contención. Estas contenciones son típicamente infrecuentes, y duran millonésimas de segundo. La lógica para manejar las colisiones se integra en los chips del controlador. Como una salvaguarda, si una estación experimenta un nivel anormalmente alto de colisiones, reporta un error y lo remueve de la red.

Aunque es verdad que bajo condiciones normales el funcionamiento de una red Token Passing es muy determinístico y predecible, Que sucede cuando se pierde una ficha (o token); Aquí tiene lugar una rutina de recuperación de la red, empezando con un proceso llamado "beaconing", durante el cual identifica un maestro del sistema; entonces el maestro genera una nueva ficha.

Mientras esto está sucediendo, toda la red está parada y desaparece la naturaleza predecible de las redes Token Passing. Adicionalmente éste proceso puede durar varios segundos.

El protocolo de contención por otro lado, utiliza una forma de control distribuido en el cual no está presente ni se requiere de ningún maestro del sistema. Si por alguna razón un mensaje o paquete de CSMA/CD se pierde, no se requiere de ningún control superior para reparar la red.

Los algoritmos de contención del CSMA/CD son mucho más simples, dando como resultado chips del controlador mucho menos complejos y más confiables que son menos susceptibles a fallas. Además, las redes Ethernet utilizan conexiones de red pasivas, de modo que las estaciones que no están involucradas en una transmisión no afectan el flujo de la información transmitida de manera alguna. Este enfoque se agrega a la confiabilidad global de la red. Las redes Token Passing como la 802.4 y la 802.5, hacen un uso extenso de los componentes activos tales como repetidores.

En general, el protocolo Token Passing requiere una relación diferencial entre señal y ruido de 23 db, mientras que el de contención Ethernet requiere de 13 db, Por esa razón es más fácil ejecutar en Ethernet 10 Mbps en un par telefónico sin protección, mientras que IBM recomienda fuertemente el cable protegido aún para la Token Ring de 4Mbps.

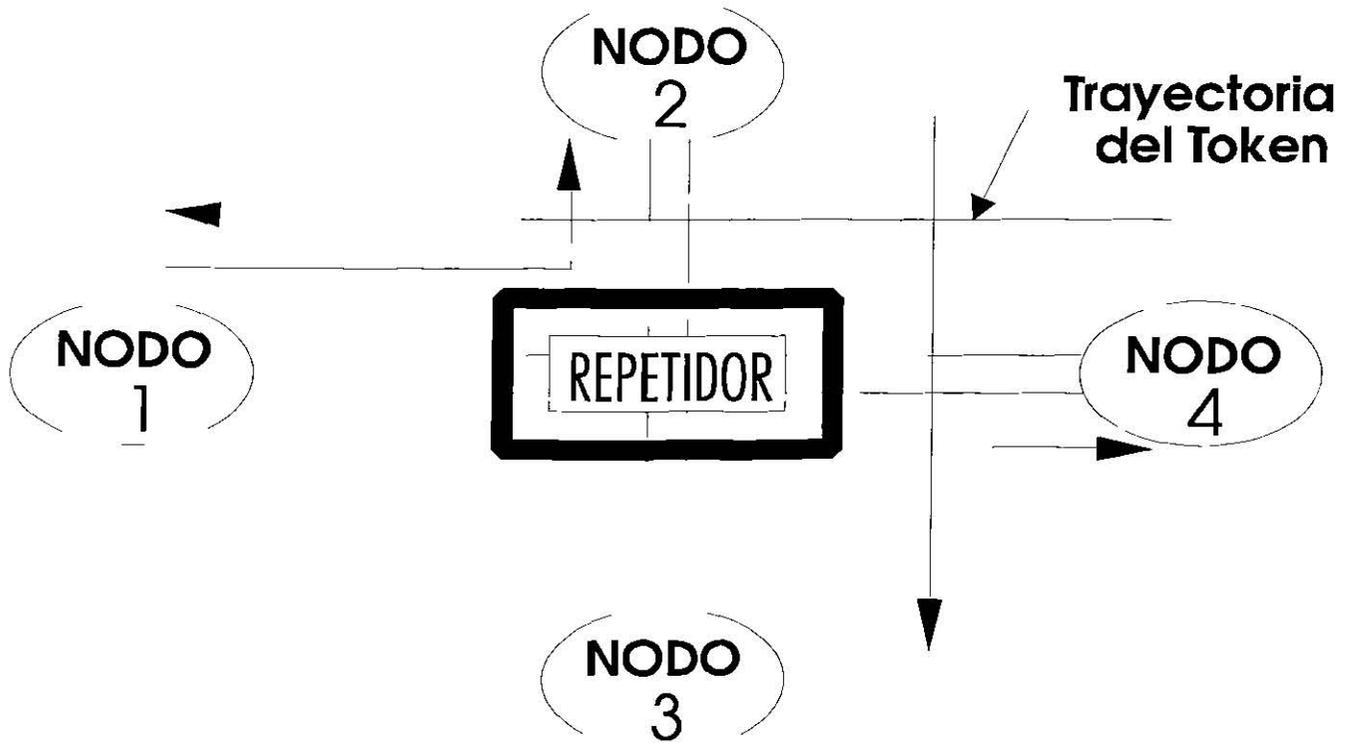
Esta característica de diferencial necesario entre señal y ruido habla de un factor confiabilidad de las redes Ethernet en condiciones similares de cableado.

En los casos que crece el número de estaciones, ambos protocolos sufren un cierto degradamiento en su transferencia real (throughput). No es posible presentar una fórmula que represente el degradamiento de uno u otro protocolo ya que en ambos casos, se comporta irregularmente conforme crece una red.

- **ARCNET**

Por lo común, la red Arcnet utiliza el protocolo de acceso *Token Passing* y la topología de anillo, con cableado en forma de estrella.

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



Para explicar esto imagínese un tren que tiene que llegar a diferentes destinos. En cada uno, entregará o recogerá algún paquete el cual ostenta una etiqueta de quién lo envía y para quién es.

El tren (*token*) viajará a través de esa vía (cableado) primero hacia el destino (nodo) marcado como primer número (nodo uno); a continuación se dirigirá al siguiente destino que tendrá un número superior ascendente al cual ya visitó. Después de haber recorrido todos los destinos (nodos), regresará al primero para reanudar con ese mismo viaje. Si se le agregase un nuevo destino (nodo), el operador del tren (sistema operativo) revisará en qué número de importancia está ese destino adicional para atenderlo conforme a su nueva ruta. En Arcnet todo esto se realiza a una velocidad de 2.5 Mbps dentro del cableado. Es posible afirmar que Arcnet es una topología de anillo modificado, ya que en verdad recorrerá los nodos en forma de anillo por ser un ciclo de atención cada uno de ellos. Pero esto lo hará no en la posición física en que se encuentran, sino en el orden lógico que se le dé a cada uno. Por tal razón, cada tarjeta lleva un número asignado de nodo (*node address*) se direcciona físicamente a cada tarjeta.

Si existiesen dos nodos con número iguales en la red, como consecuencia, habría fuertes conflictos en la comunicación de ésta, inclusive puede no existir respuesta en nodo alguno. Es decir, como se dice comúnmente *la red no levanta*.

Cada mensaje incluye una identificación del nodo fuente y del nodo destino y sólo el destino puede leer el mensaje completo. En este tipo de red no es necesario que cada estación regenere el mensaje antes de transmitirlo al siguiente. Todas las estaciones tienen la capacidad de indicar inmediatamente si pueden o no aceptar el mensaje y, además, reconocen cuándo ya se recibió.

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

Físicamente sería conflictivo tener una red de éste tipo ya que se tendría que cerrar ese anillo y agregar o eliminar un nodo sería muy complicado. En la actualidad, éste tipo de red se maneja por centro de alambrado o repetidores (hubs), los que se encargan de hacer ese anillo. Existen dos tipos de repetidores: activo y pasivo. Los activos llevan toda una electrónica que direcciona la información y la amplifica. Los pasivos constituyen bifurcadores de la señal hacia cada nodo conectado. Los repetidores activos pueden estar conectados entre sí, o directamente a un nodo o a un repetidor pasivo. Sin embargo, los repetidores pasivos sólo se podrán conectar a partir de un sólo activo y de nodos.

Arcnet es una red que corre a 2.5 Mbps. La distancia máxima que puede tener un repetidor activo a otro activo, o a otro nodo, es de 600m. La distancia máxima de un repetidor pasivo a un nodo o repetidor activo es de 15m. La máxima distancia que puede alcanzar este tipo de red a través de repetidores es de 6000m.

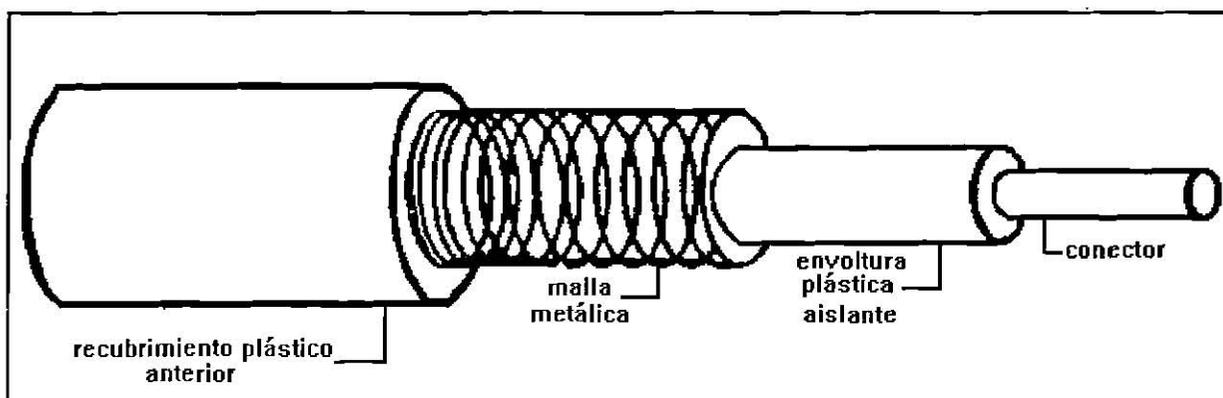
Este tipo de redes se recomienda ampliamente cuando el trabajo o el procesamiento en la misma no es muy fuerte. El tráfico de la red no es tan importante como podría ser el caso de que se utilizaran procesadores de palabras y/u hojas de cálculo.

## TIPOS DE CABLEADO

Existen varios tipos de cables para la interconectividad de las redes locales y entre ellos destacan:

- **COAXIAL:**

El cable coaxial se emplea bajo diferentes arquitecturas siendo uno de los más utilizados en las redes locales. Está compuesto de un alambre que funciona como conductor cubierto de una malla que actúa como tierra. El conductor y la tierra están separados por un aislante.



Existen dos servicios de transmisión en cable coaxial; banda base y banda ancha.

La Banda Base, utilizada principalmente en redes, usa una sola frecuencia de transmisión. La banda ancha es un servicio de transmisión simultánea de múltiples señales (datos, video y audio) que trabaja gracias a esquemas de multiplexión de la información (por ejemplo Cablevisión).

La Red Digital de Servicios Integrados (RDSI), es un sistema de banda ancha que opera con una línea de 2 MBPS multiplexada por división de frecuencia (a cada canal se le asigna una frecuencia de operación) en 30 canales de 64 KBPS, con fibra óptica.

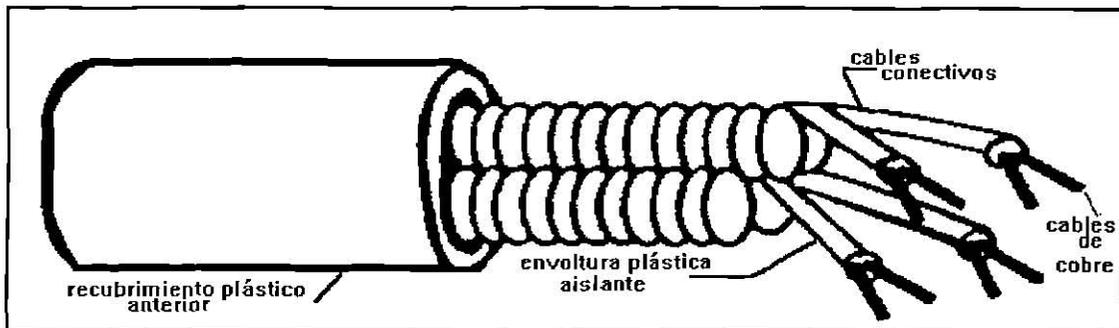
*Este cable puede ser de varios tipos:*

- *Coaxial Grueso (RG-11):* el cual transporta señales a distancias hasta de 500 mts. máximo, es más caro y menos flexible. Tiene buena tolerancia a interferencias debidas a factores ambientales, se utiliza en Bus Lineal (10Base2).
- *Coaxial Delgado (RG-58):* más flexible por lo mismo puede ser usado en lugares donde ya existen canales para cableado o se cuenta con espacio limitado. Transporta señales a distancias hasta 185mts. y es muy fácil de instalar. Se utiliza en Bus Lineal (10Base5).
- *Coaxial Arcnet (RG-62):* Transporta señales hasta de 600 mts. del repetidor activo y 30 mts. si la conexión va a uno pasivo.

- **PAR TORCIDO**

Para éstos cables se manejan dos tipos.-

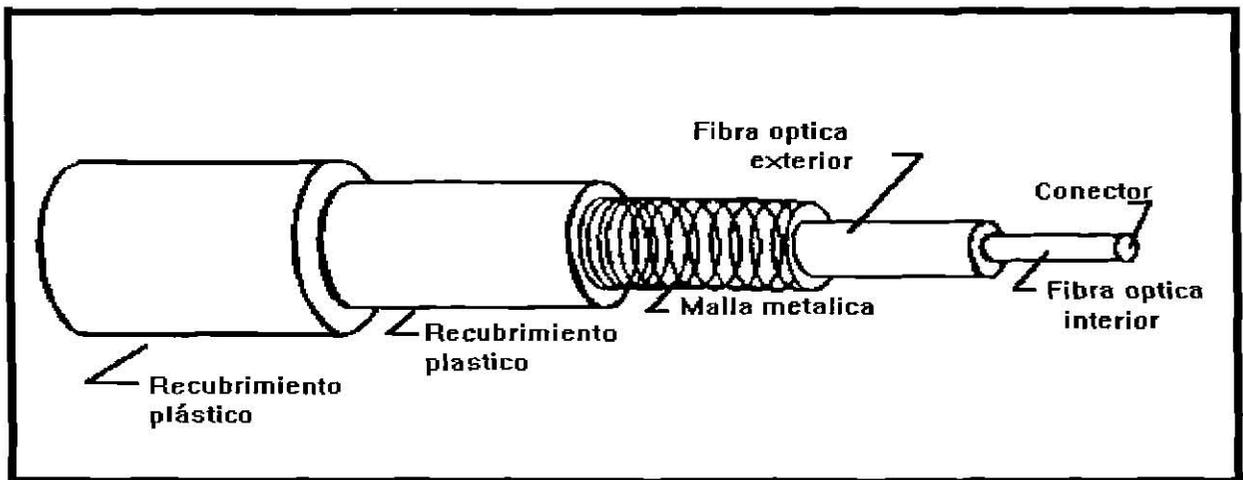
- *Cable Telefónico sin blindaje UTP(Unshielded Twisted Pair)*: el cual está formado por dos cables que están separados y a su vez torcidos. Es muy flexible, fácil de instalar y de bajo costo es usado con Ethernet (10BaseT) y Token Ring.
- *Par Torcido con blindaje STP (Shielded Twisted Pair)*: el cual está formado por un par de cables torcidos protegidos por una capa exterior aislada llamada "jacket", es menos flexible que el cable telefónico, muy confiable y usado con Token Ring.



- **FIBRA OPTICA:**

Es la tecnología más nueva de transmisión, está compuesto de una fibra muy delgada hecha de dos tipos de vidrio, uno interior y otro exterior, ambos tienen diferentes índices de refracción siendo el exterior el más elevado.

La señal eléctrica generada por la computadora es convertida en una señal de luz, la cual es llevada por la fibra de vidrio.



Este cable es utilizado para grandes distancias y alta capacidad de aplicaciones de comunicación y cuando el ruido y la interferencia electromagnética son un factor ineludible.

Aunque el precio de este cable ha bajado considerablemente sigue siendo uno de los más costosos.

Es un cable muy delgado y flexible, ofrece la mayor capacidad de adaptación a nuevas normas de rendimiento utilizado con Ethernet, Token Ring, y FDDI.

**TABLA DE ASOCIACIÓN DE TOPOLOGÍAS, PROTOCOLOS Y CABLEADO.**

TARJETA (NIC)	TOPOLOGÍAS	PROTOCOLO	CABLEADO
ETHERNET	BUS LINEAL	CSMA/CD	COAXIAL, UTP, FIBRA OPTICA
ARCNET (RX-NET)	BUS-ESTRELLA	TOKEN BUS	COAXIAL RG-62
TOKEN RING (IBM)	ANILLO	TOKEN PASSING	UTP, STP, FIBRA OPTICA

## COMUNICACION ENTRE REDES

### *Definición de Dispositivos:*

Gracias al veloz avance de la tecnología, en la actualidad se cuenta con una gran variedad de herramientas para crear la solución de interconectividad e interoperabilidad que se busca. Las herramientas más importantes con las que contamos incluyen repetidores, *bridges* (puentes), ruteadores y *gateways* (compuerta de salida). Desgraciadamente el funcionamiento de cada una de éstas, es un poco confuso. Para que entendamos mejor cuales son las diferencias principales entre una y otra vamos a utilizar una analogía de la vida real.

- **Repetidores**

Los repetidores ofrecen la conexión más económica y más "tonta" entre las redes locales. En la analogía a utilizar el repetidor funciona como Sergio, uno de los cuatro empleados en la oficina de correspondencia corporativa. Sergio controla todos los fax que llegan, pero como la calidad de impresión de las transmisiones a veces no es muy legible, tiene que leer cada uno y hacer un duplicado exacto del mismo para asegurarse que el mensaje que se entregó sea legible y después colocar la copia en la charola. Sergio es un repetidor.

Este dispositivo ofrece servicios sencillos de regeneración de señales. A medida que una señal eléctrica pasa a través de los medios de transmisión, (por ejemplo a través del cable coaxial), se genera en proporción directa a la distancia recorrida. La pérdida de la señal se llama atenuación.

Un repetidor enlaza dos redes locales idénticas, por ejemplo dos Ethernet's, y las protege de la atenuación. Un repetidor simplemente amplifica la señal que recibe en un segmento del cable y después la retransmite (repite) a otro segmento del mismo.

Los repetidores son un medio sencillo para ampliar la distancia máxima de transmisión entre los dispositivos sin afectar la calidad de ésta; proporcionan una conexión básica y simple entre redes locales adyacentes. La sencillez, sin embargo, se alcanza a costa de un mayor congestionamiento en la red.

Debido a su importancia en la red, los repetidores presentan una dicotomía interesante: todos los nodos se comunican a través del repetidor, de tal forma que éste se convierte en el punto único de falla. Al mismo tiempo, ofrece un punto central ideal desde el cual se puede observar y controlar la red. La desventaja que tiene el repetidor es que repite indiscriminadamente todas las señales que recibe y esto puede congestionar la red.

- **Puentes**

Los puentes proporcionan un servicio de conexión más inteligente. Un puente puede considerarse como un empleado de la oficina de correspondencia, muy cuidadoso pero muy poco imaginativo.

Puesto que éste empleado, Diego es en extremo muy rápido y lleva registros muy meticulosos, todo el correo que se genera en un lugar tiene que pasar por su escritorio. Tal devoción al deber, sin embargo, tiene su precio; él es genéticamente incapaz de procesar información a la vez.

Supóngase que varios artículos de correspondencia, entre éstos artículos está un memorándum interno que tiene como destinatario un colega que se encuentra dos pisos abajo y una carta a un cliente en Guadalajara. Ambos artículos están en sobre cerrado con la dirección del destinatario y su remitente.

Al final, los dos sobres llegan al escritorio de Diego para que se les procese, éste lee la dirección del cliente de Guadalajara y coloca ese sobre en la charola de "salida". De la misma manera lee la dirección del destinatario interno y pone el sobre en una charola "local". Diego funciona como un puente.

Se aseguró que los sobres "locales" se queden dentro del edificio, mientras que los que se destinan a lugares lejanos se pongan en camino. Pero, ¿Cómo distingue una dirección local de una lejana?

En realidad, la respuesta es relativamente sencilla, ya que Diego lleva registros meticulosos y puede manejar dos piezas de información a la vez, es éste caso, la dirección del destinatario y la del remitente.

Cada vez que Diego procesa un sobre lee primero la dirección de origen y después consulta una tabla de direcciones locales. Si el destinatario no está dentro de ella, le añade esa información. Así, después de un tiempo, tiene una tabla que contiene la mayoría de las direcciones locales, si no es que todas.

Después de leer la dirección de origen, actualizar la tabla mencionada, Diego lee la dirección destino. Si la encuentra en la tabla, coloca el sobre en la charola "local", conserva así el tráfico "local" como local, y evita una transmisión innecesaria de mensajes. De lo contrario, coloca el sobre en la charola de "salida".

## • **Ruteador**

Un ruteador es un nodo de la red (el servidor o una estación de trabajo) en el que se coloca más de una tarjeta de red, de modo que ésta máquina se vuelve un nodo común entre dos ( o más) redes. Maneja el intercambio de la información (en forma de paquetes de datos) entre el cableado de la red.

Los ruteadores de Netware son "inteligentes", éstos no pasan solamente los paquetes de datos entre los diferentes cables, sino que éstos direccionan el paquete por un camino más eficiente. Cada ruteador constantemente chequea su status actual, actualiza la distancia de otros ruteadores, y su localización en las tablas de direccionamiento (ruteo) y selecciona el camino más eficiente al momento de ocurrir un cambio repentino en su ruta; tal como dar de baja un servidor.

El ruteador permite:

Comunicar redes con diferentes topologías colocando en el una tarjeta de cada topología que se desee conectar, por ejemplo:

- Conectar una red utilizando la estructura Ethernet y cable coaxial RG/58 a otra red usando la estructura ARCNET con cable coaxial RG/62.
- Desahogar tráfico en un bus Ethernet, vía colocar dos tarjetas Ethernet en el servidor y partir, por lo tanto el bus en dos.
- Exceder los límites de distancia de cada topología puede soportar porque en un ruteador la señal que transita vuelve a ser regenerada.

De acuerdo a en que máquina se defina el ruteador, éste puede ser de dos tipos:

**Ruteador Interno:** en el servidor de archivos de la red, se genera al momento de instalar el sistema operativo en el servidor y basta con definir todas las tarjetas de red que se deseen colocar. Por ejemplo, si colocamos tres tarjetas estaríamos creando un ruteador capaz de comunicar tres redes. Netware 2.2 soporta hasta cuatro tarjetas de red en el servidor. Un Ruteador Interno corre como parte del servidor de archivos, cuando se utilizan varios servidores crea un "backbone", éste cable controla todo el tráfico de la red mientras que incrementa la velocidad de transmisión y decrementa el tráfico de la red. Cuando se tienen más de tres servidores ésta es una manera eficiente de implementar un ruteador

**Ruteador Externo:** Es una estación de trabajo. Se genera a través de la utilería que se llama *ROUTGEN*. De igual forma tenemos que declarar los diferentes tipos de tarjetas que se colocan en la estación de trabajo. Esta máquina, que soporta también hasta cuatro tarjetas de red, puede ser definida como un ruteador dedicado o no dedicado.

Los ruteadores, al igual que los puentes, pueden aumentar el tamaño de una red. Sin embargo, ofrecen un servicio de conexión todavía más inteligente. Si se vuelve a la analogía utilizada anteriormente, un ruteador se puede caracterizar como un empleado más calificado en la oficina de correspondencia, Alejandro, que puede manejar direcciones de origen y destino, además de tomar decisiones sobre cuál es la "mejor" manera de llegar de un lado a otro. Esta mayor capacidad, sin embargo, también tiene su precio: Alejandro es más lento que Diego.

Dos paquetes de correspondencia pasaron de su escritorio y se dejaron a la oficina de correspondencia. Uno es una propuesta para la que el tiempo es crítico, ya que se debe enviar de un día para otro a un cliente potencial en un estado lejano. Para indicar la naturaleza urgente de este material, se le pone una nota que dice: "Alejandro: URGENTE, se debe entregar mañana".

El otro es una caja grande llena de material promocional para entregar en la próxima exposición comercial. Para indicar la naturaleza menos sensible de este material, se le pone a la caja otra nota que dice: "Alejandro: ENVIO DE RUTINA, entrega en tres días".

Al recibir el envío urgente, Alejandro elige un servicio de entrega de entre los diferentes con que cuenta en las instalaciones. Al tomar ésta decisión, tal vez considere diversos aspectos, como: la velocidad con la que el servicio puede entregar el envío, el costo de la entrega, la prioridad del material a entregar, la posibilidad de dar acuse de recibo, y otras garantías.

Al recibir el envío de rutina, Alejandro vuelve a escoger un servicio de entrega. En ésta ocasión, sin embargo, puede decidir que la caja de gran tamaño puede enviarse en forma más eficiente como dos paquetes más chicos. De ser así, tal vez la abra y vuelva a acomodar el material en paquetes más pequeños.

En ambos casos, Alejandro ha funcionado como un ruteador.

Con la entrega urgente, tomó una decisión de ruteo que se basó en múltiples fuentes de información, incluyendo el sobre de la propuesta que tenía la dirección de origen destino y la nota que especificaba prioridad en la entrega. La información sobre las alternativas de entrega se derivó de fuentes totalmente diferentes al envío mismo. Con la entrega de rutina, Alejandro abrió y volvió a empacar el contenido del envío.

## Comparación de Ruteadores Vs. Puentes

A continuación se presentan algunas de las principales diferencias entre ruteadores y puentes:

1. **Instrucciones** Los ruteadores llevan una instrucción explícita (las notas que piden prioridad a la información se dirigen al ruteador). Los puentes no reciben instrucciones (los dispositivos no tienen conocimiento de su existencia)
2. **Información** Los ruteadores pueden tener acceso y usar múltiples fuentes de información. Los puentes sólo usan las direcciones de origen y destino (la tabla de direcciones es sólo una recopilación de direcciones de origen)
3. **Sobre** Los ruteadores pueden abrir sobres y manipular (fragmentar) su contenido, pueden dividir mensajes largos en dos o más de menor tamaño y así ofrecer los servicios de conexión entre redes locales que usan diferente extensión de mensaje. Los puentes no tienen acceso al sobre.
4. **Retroalimentación** Los ruteadores pueden proporcionar retroalimentación acerca de la situación de la red a los usuarios finales. Los puentes no.
5. **Envío** Los ruteadores pueden enviar un sobre a un destino específico. Los puentes sólo envían el sobre a una "charola de salida".
6. **Prioridad** Los ruteadores ofrecen diferentes "tipos" de servicio. Los puentes manejan todos los paquetes de la misma manera.
7. **Seguridad** Tanto los puentes como los ruteadores tienen la capacidad de ofrecer muros de seguridad alrededor de dispositivos específicos (por ejemplo, una minicomputadora de administración que procesa información delicada de nómina y de personal). Por lo general, los ruteadores ofrecen mayor seguridad que los puentes porque pueden recibir instrucciones de forma directa y usan información adicional.

Los beneficios que proporcionan los ruteadores son más evidentes a medida que las redes crecen en tamaño y complejidad. En resumen, ofrecen una mejor segmentación de la red, mayor seguridad y confiabilidad, puesto que pueden usarse trayectorias alternativas, y mejor uso del ancho de banda, porque eligen la mejor trayectoria entre origen y destino.

- **Gateways:**

Los gateways ofrecen el servicio de conexión más inteligente pero más lento. De vuelta a la oficina de correspondencia, el gateway, Pedro, es bilingüe. Si tiene correspondencia de un colega que hable ruso, se prepara el material en inglés y se le envía a Pedro. El traduce el material al ruso y después lo entrega a su destino, de la misma manera que lo hace Alejandro, el empleado de ruteo. Las computadoras, al igual que las personas, hablan diferentes idiomas o protocolos.

Los gateways ofrecen servicios de traducción entre diferentes protocolos de computadora, y también permiten que los dispositivos de una red se comuniquen con los de una red diferente y no sólo se conecten a ella.

## **INSTALACION DEL NETWARE**

*Requerimientos para la instalación del sistema operativo de red:*

- Discos del sistema operativo MS-DOS
- Discos del sistema operativo NOVELL NETWARE 3.11

Un servidor de archivos es una computadora que hace uso del sistema operativo de red a fin de administrar los procesos de la red. Coordina el funcionamiento armónico de las diversas estaciones de trabajo y regula la manera en que éstas comparten los recursos de la red. Al mismo tiempo determina quien tiene acceso a qué archivo, quien puede introducir cambios en los datos y quien utiliza la impresora primero. Todos los archivos de la red se almacenan en un disco duro ubicado o conectado al servidor de archivos en lugar de almacenarse en discos flexibles o en los propios discos duros de las estaciones de trabajo.

El servidor de archivos de Novell Netware 3.11 necesita para su instalación una máquina cuyo procesador sea 386 o mayor a éste y un mínimo de 4 Mb en memoria RAM. Este sistema operativo no tiene la capacidad de inicializarse por sí sólo, ya que no cuenta con un archivo de arranque, por éste motivo debe inicializarse desde un "boot disk" o desde una pequeña partición del DOS ubicada en el disco duro.

Ventajas de cada forma:

- Desde un disco de inicio
  1. Creando discos de inicio es más rápido que crear particiones de DOS en el disco duro
  2. Los discos de inicio pueden ser guardados aparte para prevenir el mal uso
- Desde el disco duro
  1. Después de la instalación, inicializar desde el disco duro es más rápido
  2. Las fallas serían mucho menores
  3. Si se desea espacio para la detección de errores (tal como INSTALL y VREPAIR) en adición a un largo número de drivers y el operador del sistema (SERVER.EXE), la partición del DOS puede tener espacio para todo esto (5Mb)

Lo más conveniente es la inicialización desde el disco duro, por lo que es necesario particionarlo.

En éste caso se deberá crear una partición para el DOS y otra para el sistema operativo (NETWARE 3.11). Un sistema operativo se pone en uso activando su partición, al hacer la partición de un disco duro se especifican las secciones del disco que podrá utilizar DOS u otro sistema operativo. Al dar formato al disco, DOS preparará la partición existente para recibir archivos. Es decir, que después de haber hecho la partición del disco duro, es necesario dar formato a cada partición antes de poder usarla.

Para crear una o más particiones de DOS en un disco duro, se utiliza el comando FDISK. Esta utilidad suministra información sobre las particiones, sirve para crear o eliminar particiones y unidades lógicas y definir la partición activa. FDISK destruye todos los archivos existentes en cualquier partición que se modifique. Si se utiliza para modificar las particiones de un disco que tenga archivos, asegúrese de hacer copias de seguridad de los que desee guardar antes de comenzar el proceso.

Ya que se tiene creada una partición para el DOS el siguiente paso es la instalación del sistema operativo Novell Netware. Recuerda que tu computadora debe tener como mínimo 8 Mb en memoria RAM para que este sistema operativo pueda correr. Antes de proceder a la instalación de Novell Netware y dar de alta el servidor es necesario conocer que clase de disco duro se tiene (ISA, ESDI, MFM, etc. ) y que clase de adaptador de red se va a instalar en dicho servidor con sus respectivos datos de configuración. Ya que se tienen bien definidos estos parámetros, se debe copiar el disco el cual contiene los comandos para inicializar la instalación.

Prácticamente la instalación la vamos a realizar en dos partes:

### 1) **Fase 1: Partición del disco duro del servidor de archivos**

*Para esta fase debes tener un diskette con el comando del DOS FDISK.COM, los comandos necesarios para arrancar la máquina (IO.SYS, COMMAND.COM, MS-DOS.COM, éstos se copian tecleando C:> SYS A: ), y el FORMAT.COM*

- Insertar el disco donde tiene la utilería FDISK
- Borrar las particiones existentes (si las tiene, primero debe borrar las particiones No-DOS y después las particiones de DOS)
- Crear la partición primaria para el DOS (5 Mb)
- Dar de alta dicha partición
- Salir de la utilería FDISK
- Dar formato al sistema al disco duro (*FORMAT C: /S*)

### 2) **Fase 2: Instalación del sistema operativo de red Novell Netware**

*Antes de proceder la instalación, tenga a la mano los siguientes datos: el tipo de arquitectura, el tipo de controlador del disco duro y el tipo de tarjeta con su respectiva configuración.*

- Crear un directorio en el disco duro llamado INSTALAR (en éste directorio se instalaran los archivos de Netware)
- Copiar el disco NETWARE V3.11 OPERATING SYSTEM-1 y NETWARE V3.11 OPERATING SYSTEM-2, en la unidad de disco duro C (en el directorio INSTALAR), éste disco contiene los comandos de Netware para inicializar la instalación y los drivers de algunos tipos de controladores de discos duros.
- Correr en C el archivo SERVER.EXE
- Cargar el driver correspondiente del disco duro dependiendo del tipo de controlador que posee.

TIPO DE ARQUITECTURA	TIPO DE CONTROLADORA DEL DISCO DURO	DRIVER DEL DEL DISCO DURO
INDUSTRY STANDARD ARCHITECTURE (ISA)	AT	ISADISK
EXTENDED INDUSTRY STANDARD ARCHITECTURE (EISA)	AT	ISADISK
MICROCHANNEL	ESDI	PS2ESDI
MICROCHANNEL	MFM	PS2MFM
MICROCHANNEL	IBM SCSI	PS2SCSI

- Cargue el programa INSTALL (*LOAD INSTALL*)
  - 1) Crear una partición para Netware
  - 2) Dar de alta el volúmen para Netware (Netware necesita un volúmen para su instalación [SYS])
  - 3) Salvar los archivos AUTOEXEC.NCF y STARTUP.NCF y anexar en el AUTOEXEC.NCF el bind de la tarjeta (el bind realiza el enlace del IPX y la tarjeta). Cada vez que se de alta el servidor se ejecutará el AUTOEXEC.NCF
- Copiar los archivos de Netware al servidor
- Dar de baja al servidor (teclea DOWN y después EXIT)
- Dar de alta el servidor y verificar que este operando

## **GENERACION DEL SOFTWARE DE RED DE LA ESTACION**

Antes de iniciar el proceso de generación del software de red de la estación, asegúrese de tener lo siguiente:

- a) Los datos de configuración del adaptador de red de la estación
- b) Una copia del disco *WSGEN Workstation Services* y del disco *DOS ODI Workstation Services*
- c) Si su adaptador de red no está soportado por Netware, una copia del disco que contiene el driver del adaptador
- d) Un disco de DOS *bootable*

Una vez que las estaciones de trabajo están conectadas físicamente, usando cualquier topología, necesitan correr el software que las integrará a la red como clientes de la misma.

El software de red permitirá a las estaciones aprovechar los recursos que el servidor ofrece, estableciendo la comunicación lógica entre el servidor y la estación.

*El software de red de la estación consiste en dos programas. Estos son:*

- **IPX.COM**
- **NETX.COM**

El programa **IPX.COM** es el protocolo de Novell que produce, mantiene y finaliza las conexiones entre los dispositivos de la red (servidores, estaciones de trabajo, routers, etc.). Este protocolo se llama precisamente, IPX (Internetwork Packet eXchange), éste se puede adaptar a diferentes tarjetas de red, ya que éste se genera en base a:

- a) El tipo de adaptador de red de la estación de trabajo
- b) La configuración del adaptador

EL **NETX.COM** se conoce como el shell de Netware, es el interpretador de los comandos de red que el usuario teclea en la estación, a diferencia del IPX.COM no se genera. Se utiliza tal como viene en el disco de instalación. En algunos casos el nombre del programa NETX.COM varía; donde la X indica el número de versión del DOS. Esto indica que el programa sólo puede ser utilizado con el número de la versión de DOS.

El shell de Netware tiene tres variantes que nos indican en que región de memoria va a trabajar dicho archivo:

- **NETx.COM**: Shell en Memoria Convencional
- **XMSNETx.EXE**: Shell en Memoria Extendida
- **EMSNETx.EXE**: Shell en Memoria Expandida

El archivo IPX.COM se genera a través de la utilería *WSGEN*. Esta utilería viene en el disco *WSGENDOS Workstation Services*, que forma parte de los discos de instalación de Netware.

El archivo NETX.COM se obtiene del mismo disco, haciendo una copia del mismo. Dentro de la generación del software de red existe una variante para mejorar el desempeño del mismo. Esto se logra trabajando bajo el ambiente de **DOS/ODI** y son un grupo de archivos que permiten los siguientes beneficios:

- Pueden expandir la red utilizando múltiples protocolos (tal como IPX/SPX, Apple Talk o TCP/IP) sin agregar tarjetas de red en la estación de trabajo
- Pueden comunicarse con una gran variedad de estaciones de trabajo, servidores, etc., vía diferentes protocolos sin tener que inicializar la máquina.
- El protocolo ODI puede comunicarse a través de cualquier adaptador de LAN escrito a la especificación ODI.

- Se ahorra tiempo con un driver LAN que dé apoyo a los múltiples protocolos.

El DOS/ODI cuenta con tres sets de archivos que permiten a las estaciones de trabajo comunicarse entre ellas, con otros servidores o un tercer host.

<b>LSL.COM</b>	Link Support Layer File, permite la comunicación sobre varios protocolos.
<b>LAN drivers</b>	Comunica directamente a las tarjetas LAN.
<b>Protocol Stacks</b>	Archivos como el IPXODI.COM y el TCPIP.EXE que permiten las comunicación entre estaciones de la red.

### ***Para ejecutar la utileria WSGEN:***

1. Introduzca en el drive A: una copia del disco *WSGEN DOS Workstaion Services*
2. Teclee A:WSGEN
3. Recibirá una serie de mensajes, Presione <ENTER> para continuar
4. La utilería mostrará una lista de los drivers soportados actualmente por Netware
  - Si el driver de su adaptador de red se encuentra en la lista, teclee <ENTER>.
  - Si el driver de su adaptador de red no se encuentra en la lista, presione <INSERT> e introduzca en la unidad A el disco que contiene el driver. El driver aparecerá ahora, selecciónelo y presione <ENTER>. Quite el disco del driver y coloque nuevamente el disco WSGEN.
5. La utilería mostrará una lista de las configuraciones más usuales para su adaptador de red. Seleccione la configuración que corresponda a la configuración actual de su adaptador.
6. La utilería le pedirá confirmar la creación del software de la estación. Responda afirmativamente.
7. Salga de la utilería (Presione <ENTER>)
8. Copie los archivos IPX.COM y NETX.COM del disco *WSGEN DOS Workstation Services* al disco bootable donde residirán permanentemente.

## ***Ejecución del software de red de la estación:***

- 1) De boot al sistema desde el disco booteable
- 2) Ejecute el software de red de la estación, en el siguiente orden:
  - a) A:>IPX
  - b) A:>NETX
- 3) Posicione en el drive F:
- 4) El sistema responderá con  
F:\LOGIN>
- 5) En éste punto ya está trabajando en un directorio del servidor de archivos que se llama LOGIN. Para completar el proceso de conexión al servidor, necesita darse de alta en una cuenta, por ejemplo:  

Login usuario	(alta en la cuenta)
Enter Password:	(clave de acceso)

## **EJEMPLOS DE ARCHIVOS AUTOEXEC.BAT PARA ACCESAR A LA RED:**

1. mode co80  
ipxmca  
net4  
f:  
Login Enterprise/

Este archivo se utiliza para estaciones de trabajo con microchannel, utilizando la version 4.x del DOS (net4). El archivo ipx ha sido renombrado para representar la tarjeta adaptadora de la estación (ipxmca). El archivo configura el modo para monitor a color/gráficos con un ancho de despliegue de 80 caracteres (mode co80) y despliega el login Enterprise, para acceder a ese servidor (Enterprise)

2. @echo off  
cls  
prompt \$p\$g  
type screen.asc  
ipx>nul  
net3>nul  
f:  
login eliot/jean

Este ejemplo es escrito para una estación con arquitectura ISA, despliega el contenido de un archivo tipo ASCII (type screen.asc) que podría ser un mensaje para los usuarios, carga los drivers ipx y net3 evitando el despliegue de éstos (>nul), entra al drive default (f:) y accesa al servidor eliot con la cuenta de usuario eliot.

3. ipx  
net3  
c:  
prompt \$p\$g

Este ejemplo es para una arquitectura ISA (XT o AT) utilizando la version 3.x del DOS, carga los drivers de la red (ipx, net3), y accesa al drive c:, antes de ejecutar el login.

En este ejemplo es necesario que el usuario teclee f:login , para poder acceder a los drives de la red.

## **CLASIFICACION DE LOS USUARIOS DE LA RED**

La red puede ser operada por cualquiera de los siguientes usuarios:

- **usuario:** es toda aquella persona que ha sido dada de alta como autorizada para operar la red. Cada usuario tiene una cuenta con un nombre específico el cual sirve como llave de entrada, además tiene asignados privilegios que están en función del papel que desempeña en la red.
- **supervisor:** es aquella persona que coordina a los usuarios y tiene absolutamente toda la responsabilidad en la organización y buen funcionamiento de la red. Debido a sus funciones, el supervisor requiere de todos los privilegios de operación y no puede ser borrado de la red.
- **superusuario:** dado el volúmen de trabajo que implica administrar la red y como medida de seguridad es recomendable que exista en la red al menos un usuario con "equivalencia de supervisor"
- **grupos:** los grupos son una forma de organizar a los usuarios que pertenecen a una misma área o perfil de operación, cada grupo al igual que los usuarios tendrá sus privilegios asignados.

## **ESTRUCTURA DE LA RED**

El concepto de red se basa en el principio de compartir recursos entre los usuarios. La principal característica de este tipo de red es el contar con un lugar común de almacenamiento de los datos para compartir la información, entre los distintos usuarios que están dados de alta en la red. Esto es a lo que se le llama "*Multiusuario*".

Cada usuario tiene una microcomputadora que funciona como una Estación de Trabajo. Puede tener acceso a la información de un lugar común de almacenamiento, este lugar es el File Server (Servidor) donde se administra la operación de las estaciones de trabajo. El lugar común de almacenamiento es el disco duro "hard disk". Dentro del disco duro del servidor existe una estructura de directorios semejante a la que podemos crear en un disco controlado por sistema operativo DOS.

Netware crea cuatro directorios en el volúmen, que no se deben modificar:

**Login:** Es el directorio de acceso a la red porque en el se encuentran las ordenes de entrada para los usuarios que deseen hacer uso de los recursos.

**Mail:** Es un directorio en el que está definido un buzón (box) para cada usuario de la red. Dentro de este se guarda su Login Script (secuencia de órdenes específicas para dicho usuario, que se ejecuta al entrar éste a la red).

**Public:** Es el lugar donde se encuentran todas las órdenes de Netware que puede utilizar el usuario, es decir aquellas que son de dominio público.

**System:** En el se encuentran las órdenes exclusivas para el supervisor de la red. A ellas no tiene acceso el usuario normal de la red.

## SEGURIDAD

En un sistema de redes es absolutamente necesario controlar el acceso a la información, para asegurar que el trabajo de un usuario no ocasione problemas a otros.

### Niveles de Seguridad:

- 1) **Login y password:** Es indispensable para que una persona pueda acceder a la red que exista como un usuario de la misma. El supervisor es la persona facultada para definir usuarios en la red.

Cada usuario puede tener una clave secreta (password) de acceso a la red que sólo él conoce. Dicha clave evita la posibilidad de que otra persona entre a la red con nuestro nombre.

Además cuenta con una serie de restricciones que pueden ser asignadas a las cuentas y a los passwords.

- 2) **Derechos:** Cuando un usuario es definido en la red por el supervisor, éste establece los derechos del usuario, las áreas de la red a las que tiene acceso el usuario y con que privilegios trabaja. De esto depende, en gran parte, el buen funcionamiento y la seguridad de la red.

### Existen ocho derechos:

DERECHO	FUNCION A NIVEL DIRECTORIO	A NIVEL ARCHIVO
<i>Read(R)</i>	Permite al usuario abrir y leer o ejecutar cualquier archivo del directorio	Permite al usuario abrir y leer o ejecutar el archivo
<i>Write(W)</i>	Permite al usuario abrir y escribir sobre los archivos del directorio	Permite al usuario abrir y escribir sobre el archivo
<i>Create(C)</i>	Permite al usuario crear archivos y subdirectorios	Permite al usuario rescatar el archivo después de ser borrado.
<i>Erase(E)</i>	Permite al usuario borrar un directorio, subdirectorio o archivo	Permite al usuario borrar el archivo.
<i>Modify(M)</i>	Permite al usuario cambiar los atributos de cualquier archivo, subdirectorio o el directorio, así como renombrarlos.	Permite al usuario renombrar y cambiar los atributos del archivo.
<i>File Scan (F)</i>	Permite al usuario ver con la orden DIR de D.O.S., los archivos y subdirectorios.	Permite al usuario ver el archivo con la orden DIR de D.O.S.

DERECHO	FUNCION A NIVEL DIRECTORIO	A NIVEL ARCHIVO
<i>Acces Control(A)</i>	Permite al usuario modificar sus asignaciones de derechos y la máscara de derechos heredados (IRM) en el directorio o archivo. El usuario puede asignar cualquier derecho menos el derecho Supervisor y a otro usuario.	Permite al usuario modificar sus asignaciones de derechos y la máscara de derechos heredados (IRM) del archivo. El usuario puede asignar cualquier derecho menos el derecho Supervisor y a otro usuario sobre el archivo.
<i>Supervisor</i>	Garantiza todos los derechos. Este derecho se sobrepone a cualquier restricción asignada anteriormente. Cualquier usuario con este derecho puede asignar a su vez cualquier otro derecho a otro usuario. Una vez que este derecho ha sido asignado no se puede revocar a menos que se elimine la asignación. Nos permite modificar las restricciones de espacio en disco.	Garantiza todos los derechos. Este derecho puede ser asignado a otro usuario y éste puede modificar todos los derechos del archivo.

3. **Atributos:** asignan propiedades especiales a directorios o archivos individuales. Los atributos se sobrepone a los derechos efectivos impidiendo tareas que los derechos de usuario, de grupo y de área permitieran.

Los atributos son:

*ARCHIVE NEEDED(A).*- Sólo puede ser asignado a archivos. Netware automáticamente asigna éste atributo a cualquier archivo al momento de crearlo, o bien, luego que ha sido modificado desde el último respaldo de información. El usuario puede asignar o quitar este atributo.

*COPY INHIBIT(CI).*-Sólo puede ser asignado a archivos. Este atributo restringe los derechos de copiado en estaciones de trabajo Macintosh atados a la red.

*DELETE INHIBIT(DI).*-Este atributo puede ser asignado a directorios, archivos e impide a los usuarios (en primera instancia inclusive al supervisor) borrar los directorios o archivos aún cuando tengan el derecho erase.

*HIDDEN(H).*- Este atributo puede ser asignado a directorios o archivos. Su función es ocultarle al usuario un archivo o directorio al ejecutar la orden de DOS, *DIR*. Además impide que el archivo o directorio sea borrado o copiado. Si se posee el derecho File Scan, los archivos o directorios aparecerán al ejecutar la orden en Netware, *NDIR*. Los archivos con este atributo siguen siendo ejecutables.

*PURGE(P).*- Puede ser asignado a directorios o archivos. Cuando es asignado a un archivo, éste es purgado en el instante que es borrado. Cuando es asignado a un directorio, éste atributo purga todos los archivos existentes en el directorio cuando son borrados, los archivos con éste atributo no pueden ser recuperados con la utilería *SALVAGE*.

*READ AUDIT(Ra)*.- Sólo puede ser asignado a archivos.

*READ ONLY/READ WRITE(Ro/Rw)*.- Sólo puede ser asignado a archivos. Cuando el atributo Read Only es asignado, Netware otorga automáticamente los atributos: Rename Inhibit y Delete Inhibit, impidiendo así que el archivo sea borrado, modificado o renombrado aún cuando se posean los derechos efectivos Right y Erase en el directorio que lo contiene. Si no existe el atributo Read Only automáticamente el atributo es Read Write.

*RENAME INHIBIT(R)*.- Puede ser asignado a directorios o archivos e impide en primera instancia que el usuario (inclusive el supervisor) los renombre aún cuando tenga el derecho *modify*.

*SHAREABLE(S)*.--Sólo puede ser asignado a archivos y permite que el archivo pueda ser usado por más de un usuario al mismo tiempo.

*SYSTEM(Sy)*.- Este atributo puede ser asignado a directorios o archivos. Su función es ocultar al usuario un archivo o directorio al ejecutar la orden de DOS, *DIR*. Además impide que el archivo o directorio sea borrado, copiado o ejecutado. Si se posee el derecho File Scan los archivos o directorios aparecerán al ejecutar la orden de Netware *NDIR*.

*TRANSACTIONAL(T)*.- Sólo puede ser asignado a archivos. Este atributo indica que los archivos están protegidos por el transaccional Tracking System (TTS).

*WRITE AUDIT(Wa)*.- Solo puede ser asignado a archivos.

## COMANDOS UTILIZADOS PARA EL MANEJO DE ATRIBUTOS

- **FLAG**: Es utilizado para asignar atributos sobre archivos  
*sintaxis: flag [path [opción | [+ | ] attribute ] [sub]]*  
*opciones.-*  
RO Read Only  
RW Read Write  
S Shareable  
H Hidden  
SY System  
T Transactional  
I Indexed  
A Archive Needed  
RA Read Audit  
WA Write Audit
- **FLAGDIR**: Es utilizado para asignar atributos a directorios  
*sintaxis: flagdir [path [opción...]]*  
*opciones.-*  
Normal  
System  
Hidden  
Private

- GRANT:** Este comando es para asignar derechos a grupos o usuarios sobre directorios determinados  
*sintaxis: grant rightslist\* [for path] to [user|group] name [opciones]*  
*opciones.-*  
*/Subdirectorios| /Files*  
*ALL=all*  
*N=Sin derechos*  
*R=Lectura (Read)*  
*W=Escritura (Write)*  
*C=Crear*  
*E=Borrar (Erase)*  
*M=Modificar*  
*F=Busqueda de Archivo*  
*A=Control de Acceso*
- REMOVE:** Borra una lista de derechos de un directorio a un usuario o grupo de usuarios *sintaxis:*  
*remove [user | group ] name [from path] [option]*  
*opciones.-*  
*/subdirectorios*
- REVOKE:** Utilizado para quitar derechos de directorio a usuarios o grupos de usuarios  
*sintaxis: revoke rightslist [for path] from [user | group] name [opciones]*  
*opciones.-*  
*/subdirectorios*
- RIGHTS:** Visualiza los derechos efectivos sobre un directorio.  
*sintaxis: rights [path]*
- TLIST:** Despliega en pantalla la lista de derechos efectivos de usuarios y grupos sobre un directorio específico  
*sintaxis: tlist [path [users | groups]*

## COMANDOS UTILIZADOS PARA ACCESAR EL SISTEMA

- LOGIN: Utilízelo para dar acceso a un usuario a un servidor en una red. El sistema de seguridad de Netware no permite el acceso al sistema, si el supervisor no ha dado de alta al usuario. Este procedimiento es conocido como "firmarse" y se realiza mediante esta orden.  
*sintaxis: login [/opciones] [server/] [username] [scriptparameters]*  
*opciones.-*  
*Clear Screen*  
*No Attach*  
*Script <path esp.>*  
  
Si existe más de un servidor es necesario especificar a cual de ellos deseamos entrar.
- ATTACH: Use éste comando para conectar su estación de trabajo a un servidor adicional en la red o interred  
*sintaxis: attach [fileserver [/name] [/private | /global]]*
- CASTOFF: Este comando es utilizado para bloquear los mensajes enviados por send y broadcast  
*sintaxis: castoff [All]*
- CASTON: Desactiva el bloqueo realizado por castoff  
*sintaxis: caston*
- LOGOUT: Utilízelo para dar de baja un usuario de un servidor en una red, por lo que el servidor cierra todos los archivos relacionados con él.  
*sintaxis: logout / logout [server]*
- SEND: Envía mensajes a un usuario o un grupo de usuarios en la red  
*sintaxis: send "message" [to] [[user | group] [server/] name [, server/ ] name...]*
- USERLIST: Muestra una lista de usuarios que están trabajando en el servidor de red.  
*sintaxis: userlist [fileserver/] [name] [address | object] [/continuos]*
- WHOAMI: Despliega el nombre del usuario que está trabajando y en que servidor está conectado  
*sintaxis: whoami*

## COMANDOS PARA MANEJO DE IMPRESIONES

- **CAPTURE:** Para acceder un direccionamiento de alguna cola de impresión de la red  
*sintaxis: capture /SHow /Job=Jobname /Server=Fileserver /Queue=queuename /local=N /Form=form or n /Create=path /Copies=n(1-99) /Timeout=n /Keep /Tabs=n (1-18) /Notabs/Banner=bannername /name=name /No banner/Formfeed /No formfeed /Autoendcap /No autoend /notify /No notify*
- **PSC:** Puede usar éste comando para un rápido control del servidor de impresiones y de las impresoras remotas, los usuarios de la red pueden usar psc para ver el estado del servidor y las impresoras remotas.  
*sintaxis: psc ps[=]print\_server p[=]printer\_number flaglist*
- **PSTAT:** Despliega el estado actual del servidor de impresiones o impresoras remotas de la red.  
*sintaxis: pstat [[/server]=server name] [[/printer]=printer\_number*
- **NPRINT:** Es utilizado para mandar a impresión un determinado archivo.  
*sintaxis: nprint path options*  
*opciones:*  
*/banner= banner name /name=name /no banner*  
*/[no] formfeed /[no] notify /tabs=n (1-18) / no tabs*

## COMANDOS UTILIZADOS PARA MANEJO DE ARCHIVOS

- **NCOPY:** Copia uno o más archivos de un directorio a otro  
*sintaxis: ncopy [path] [to] path [option..]*  
*opciones.-*  
*/s copia subdirectorios*  
*/s/e copia subdirectorios aún estando vacíos*  
*/f copia archivos esparcidos o vacíos*  
*/l información de archivos de formatos DOS*  
*/c copia archivos sin respetar los atributos que tenga*  
*/v verifica la lectura después de la escritura*  
*/h/? despliega los comandos de ayuda*
- **NDIR:** Despliega el contenido de un directorio o subdirectorio obteniendo información como: tamaño de archivos, fecha y hora de creación.  
*sintaxis: ndir [path] [/option]*
- **PURGE:** Borra permanentemente los archivos borrados anteriormente (no hay manera de recuperarlos al dar purge)  
*sintaxis:*  
*en Novell 2.x purge*  
*en Novell 3.x purge [filename |wildcard] [all | /a]*

## COMANDOS UTILIZADOS PARA MANEJO DEL SERVIDOR

- ATOTAL: Despliega el sumario del día y semana del administrador.  
*sintaxis: atotal*
- BINDFIX: Corrige o actualiza los bindery de la red  
*sintaxis: f:\system\bindfix*
- BINDREST: Restaura una versión anterior de archivos de bindery de red actualizada por bindfix  
*sintaxis: f:\system\bindrest*
- NVER: Informa sobre las versiones de software que se están usando en el servidor de archivos y en las estaciones  
*sintaxis: nver*
- SECURITY: Encuentra posibles violaciones de seguridad  
*sintaxis: f:\system\security*
- SETPASS: Crea o cambia una clave de acceso (password) en uno o más servidores de archivos.  
*sintaxis: setpass [fileserver] [/username]*
- SLIST: Despliega lista de servidores en la red y la información de cada uno  
*sintaxis: slist [fileserver] [/continue]*
- SYSTIME: Despliega la fecha y el día actual de la red  
*sintaxis: systime [fileserver]*
- VERSION: Despliega la versión de Netware de archivos ejecutables  
*sintaxis: version [path] filename*
- WSUPDATE: Se utiliza para actualizar los archivos de una estación de trabajo, puede ser usado para actualizar los shell de netware [ipx, netx] para el acceso de la red.  
*sintaxis: wsupdate /f=<infile>| [<sourcepath> <destdrive:destfile>[/option]*

## COMANDOS UTILIZADOS PARA MANEJO DE DIRECTORIOS Y VOLUMENES

- CHKDIR: Se utiliza para revisar el total del espacio ocupado por un directorio  
*sintaxis: chkdir [path]* (éste comando es de la versión 3.x solamente)
- CHKVOL: Revisa el volúmen del disco (sys, vol1, vol2, etc,) dando el total del espacio en disco duro, bytes utilizados, bytes libres.  
*sintaxis: chkvol [path]*
- LISTDIR: Es utilizado para ver la información de los directorios, incluyendo derechos máximos, fechas de creación, etc.  
*sintaxis: listdir [path] [option]*  
*opciones:-*  
*/R rights*  
*/E effective rights*  
*/D date*  
*/T time*  
*/S subdirectories*  
*/A all*
- MAP: Es utilizado para ver o cambiar las direcciones de búsqueda de drive  
*sintaxis: map [option] [drive:= drive /path]*
- RENDIR: Se utiliza para renombrar un directorio o subdirectorío  
*sintaxis: rendir path new\_directory\_name*

## COMANDOS UTILIZADOS PARA EL MANEJO DE LA CONSOLA

- BROADCAST: Utilizado para enviar mensajes a todos los usuarios de la red
- CLEAR MESSAGE: Borra los mensajes enviados por broadcast
- CLEAR STATION: Cierra los archivos de una estación determinada y la dá de baja del servidor
- CONFIG: Muestra por pantalla la configuración de las tarjetas de red instaladas en el servidor
- CONSOLE: Esta función es para servidores no dedicados, usada para pasar al modo de servidor

- DISABLE LOGIN: Deshabilita la entrada de cualquier usuario a la red
- DISK: Es usado para monitorear el estado del disco
- DISMOUNT: Sirve para dar de baja un volumen del disco que no es usado
- DISPLAY SERVERS: Use ésta instrucción para ver la lista de todos los servidores y ruteadores que están conectados entre sí.
- DISPLAY NETWORKS: Muestra por pantalla la lista de los números de los nodos de los servidores o ruteadores que están conectados entre sí.
- DOS: Es usado para servidores no dedicados, para pasar al modo de estación de trabajo
- DOWN: Instrucción usada para dar de baja el servidor
- ENABLE LOGIN: Usado para habilitar los logins de los usuarios (pueden acceder a la red)
- MOUNT: Para montar los volúmenes que desmontamos anteriormente con `dismount`
- MONITOR: Usado para ver las actividades de los usuarios conectados a la red
- NAME: Nos despliega por pantalla el nombre del servidor en que estamos trabajando
- OFF: Para borrar la pantalla del servidor
- PRINTER: Es usado para crear, borrar, y configurar colas de impresión, controlar las formas de papel, controla las impresiones y las prioridades.
- QUEUE: Lista, mueve y borra los trabajos de impresión.
- REMIRROR: Usado para restaurar el espejo de los discos cuando no se ha actualizado alguno de ellos
- RESET ROUTER: Utilizado para restaurar los ruteadores instalados que hayan sido afectados por algún problema

- SET TIME: Utilizado para configurar la fecha y la hora del servidor
- SPOOL: Es usado para listar y cambiar las asignaciones de spool
- TIME: Sirve para ver fecha y hora del servidor
- UNMIRROR: Desactiva la función de espejo entre dos discos en un servidor de archivos con espejo
- UPS: Nos da la información del tiempo de respaldo que tenemos en nuestra unidad de respaldo.
- VER: Muestra la versión del Netware con la que estamos trabajando en nuestro servidor
- WATCHDOG: Para monitorear los usuarios del servidor

## MENUS DE UTILERIAS

- COLORPAL: Menú utilizado para configurar los colores de los menús de netware y menús creados por la utilería menú  
*sintaxis: colorpal*
- DSPACE: Menú utilizado para limitar a un usuario en los diferentes volúmenes el espacio utilizado en disco  
*sintaxis: dspace*
- FCONSOLE: Utilizado para analizar la operación del servidor de archivos, los programadores experimentados de novell utilizan ésta utilería para obtener información de lectura, escritura, y búsqueda de los programas
- FILER: Sirve para ver y controlar la información y la seguridad de los directorios de la red  
*sintaxis: filer*
- HELP: Use éste menú para ver información en línea de las utilerías de Netware, mensajes de error de advertencia y conceptos

- **MAKEUSER**: Para crear y borrar usuarios temporales, es frecuente para usuarios temporales  
*sintaxis: makeuser*
- **MENU**: Sirve para acceder los menús que son creados por medio de algún editor de texto ASCII, usando algún editor se especifican las aplicaciones y programas que se usan  
*sintaxis: menu [path] filename*
- **PRINTCON**: Es usado para crear job's de configuración para impresión (un job describe la configuración de como se va a imprimir un trabajo)  
*sintaxis: printcon*
- **PRINTDEF**: Usado para definir los manejadores de impresión, para cada tipo de impresora en particular, definir formas (tipo de papel), ver las formas definidas (ancho, largo, nombre y número)  
*sintaxis: printdef*
- **SALVAGE**: Use ésta opción para recuperar archivos borrados en ese momento (sin haber dado purge)  
*sintaxis: salvage*
- **SESSION**: Menú utilizado para ver o cambiar temporalmente los drives de búsqueda, seleccionar el drive por default, ver lista de usuarios y grupos y enviar mensajes a los mismos.  
*sintaxis: session*
- **SYSCON**: Menú utilizado para administrar y controlar las actividades del servidor de archivos tanto de los grupos como de los usuarios, crear usuarios, grupos, asignar derechos de directorio  
*sintaxis: syscon*

*Esta utilería accesa los siguientes menús con sus respectivas opciones.*

#### **1) AVAILABLE TOPICS**

**accounting**: opción que muestra los recursos utilizados por la contabilidad de la red.

**change current server**: permite al usuario atarse, cambiarse o salirse de un servidor.

**file server information**: muestra información sobre las características del servidor seleccionado.

**group information**: lista todos los grupos definidos en la red.

**supervisor options**: ésta opción sólo está disponible para el supervisor.

**user information**: muestra el login\_name de todos los usuarios.

### 1.1) ACCOUNTING

**accounting servers:** permite ver los servidores que manejan la contabilidad de la red.

**blocks read charge rates:** muestra las tarifas empleadas en la lectura decada bloque de información (Kb).

**blocks write charge rates:** muestra las tarifas empleadas por la escritura de cada bloque de información (4 Kb).

**connect time charge rates:** muestra la tarifa empleada por cada minuto de conexión en la red.

**disk storage charge rate:** muestra la tarifa empleada por cada bloque de información (4Kb) escrito en el disco.

**service requests charge rate:** muestra la tarifa empleada por el uso de dispositivos periféricos.

- 2) **GROUP NAMES:** Lista todos los grupos definidos en la red y sólo si selecciona aquellos a los que pertenece, tendrá acceso a la siguiente ventana:

#### 2.1) GROUP INFORMATION

**full name:** muestra el nombre completo del grupo

**manager user and groups:** lista todos los usuarios y grupos que administra este grupo

**managers:** lista los usuarios que administran éste grupo

**member lista:** lista todos los usuarios que pertenecen a éste grupo

**other information:** especifica el número de identificación de éste grupo.

**trustee directory assignments:** lista los derechos de grupo por directorio

**trustee file assignments:** lista los derechos del grupo por archivo.

- 3) **USER NAMES:** Lista el login\_name de todos los usuarios definidos en la red y sólo si selecciona su login\_name correspondiente, tendrá acceso a la siguiente ventana.

#### 3.1) USER INFORMATION ACCOUNT BALANCE:

Muestra una cantidad que representa la disponibilidad de los recursos de la red para el usuario.

**account restriction:** muestra las restricciones a las que está sujeto el usuario.

**change password:** permite modificar la clave de acceso del usuario

**full name:** muestra el nombre completo del usuario

**groups belonged to:** Lista los grupos a los que pertenece el usuario

**login script:** programa de entrada del usuario en la red

**managed user and groups:** lista todos los usuarios y grupos que administra éste usuario.

**managers:** lista los usuarios que administran a éste usuario

**other information:** muestra algunas especificaciones del usuario como: fecha y hora de entrada, espacio ocupado en el disco y su número de identificación.

**security equivalences:** muestra las equivalencias de derechos a otros usuarios o grupos

**station restrictions:** en ésta opción el usuario puede conocer en que máquina(s) y con que servidor(es) puede trabajar

**time restriction:** indica el horario de trabajo del usuario dentro de la red

**trustee directory assignments:** muestra los derechos individuales por directorio para el usuario.

**trustee file assignments:** muestra los derechos por archivo para el usuario

**volumen/disk restrictions:** muestra las restricciones de espacio por volúmen para el usuario

#### 4) **ACCOUNT RESTRICTIONS:**

**disable:** indica si la cuenta está habilitada para trabajar en la red. La cuenta no puede acceder a la red si ésta opción tiene el valor YES.

**account has expiration date:** especifica si la entrada del usuario tiene fecha de expiración

**date account expires:** muestra la fecha de expiración para la entrada de usuario a la red

**limit concurrent connections:** indica si el usuario está limitado en el número de entradas a la red éste número especifica el número de entradas a realizar simultáneamente

**allow user to change password:** advierte la posibilidad que el usuario modifique su password y login script

**required password:** indica si el usuario tiene restricciones en la definición de su password

**minimun password lenght:** la longitud mínima especificada para el password

**force periodic password changes:** si ésta opción es afirmativa, el usuario debe modificar su password periódicamente

**days between forced changes:** señala la cantidad de días que deben pasar entre los cambios forzosos de password

**date password expires:** muestra la fecha en la que el password expira

**limit grace logins:** advierte si el usuario puede entrar a la red después de la fecha de expiración del password

**grace logins allowed:** indica el máximo número de oportunidades que tiene el usuario para entrar a la red, al no haber modificado su password

**remaining grace logins:** informa el total de que dispone el usuario para entrar a la red, al no haber modificado su password.

**require unique password:** indica si el password del usuario es único. Si es así, debe especificar un password diferente a los ocho últimos, cada vez que lo modifique.

- **PCONSOLE:** Usado para controlar las impresiones de la red, se pueden crear, borrar, o renombrar colas de impresión, crear servidores de impresión, asignar o modificar operadores y usuarios de impresión, cambiar el orden de las impresiones, borrar impresiones.  
*sintaxis: pconsole*

*Esta utilidad accesa los siguientes menús con sus respectivas opciones:*

### 1) **AVAILABLE OPTIONS**

**change current file server:** permite al usuario atarse, salirse o cambiarse del servidor

**print queue information:** opción para mandar archivos a impresión

**print server information:** información sobre los servidores de impresión

#### 1.1) **PRINT QUEUE INFORMATION:**

**current print job entries:** muestra los trabajos formados en la cola de impresión y permite al usuario anexar sus archivos y modificar características

**current queue status:** indica el estado de la cola seleccionada

**currently attached server:** indica el nombre de los servidores de archivos atados a la cola de impresión

**print queue id:** número de identificación de la cola

**queue operators:** nombre de los usuarios que son operadores de ésta cola.

**queue servers:** nombre de los servidores que atienden la cola seleccionada.

**queue users:** usuarios y grupos que están autorizados para utilizar la cola de impresión.

**new print job:** permite definir las características de impresión del archivo.

#### 1.2) **PRINT SERVER INFORMATION:**

**full name:** escribe el nombre completo del servidor de impresión.

**print server id:** identificador del servidor de impresión.

**print server operators:** indica quienes son los operadores del servidor de impresión.

**print server status/control:** muestra la información referente a ese servidor de impresión.

**print server users:** nombra los usuarios que utilizan el servidor de impresión seleccionado.

#### 1.2.1) **PRINT SERVER STATUS AND CONTROL:**

**file server serviced:** señala a que servidores de archivo atiende ese servidor de impresión.

**notify list for printer:** lista los usuarios a los que tiene que informar en casos de falla.

**printer status:** muestra y permite cambiar la información relacionada con la impresora

**queues serviced by printer:** colas de impresión que son atendidas por la impresora

**server info:** información acerca del servidor.

- USERDEF: Nos permite crear usuarios, login scripts, signar directorios base, dar restricciones de espacio en disco.  
*sintaxis: userdef*
- VOLINFO: Menú utilizado para ver la información de cada volumen del servidor de archivos  
*sintaxis: volinfo*

## **UTILERIAS PARA LA CREACION DE CUENTAS DE USUARIOS**

Puedes crear usuarios de la red con:

1. *SYSCON*
2. *MAKEUSER*
3. *USERDEF*

Sin embargo, los grupos solamente pueden ser creados solamente con SYSCON, para modificar cuentas de usuario también solamente se utiliza el SYSCON.

*SYSCON*: Puedes crear usuarios individualmente con la opción "User Information". Al configurar el System Default Restrictions, puedes asignar automáticamente todas las restricciones de acceso excepto restricciones de estación a nuevos usuarios. Cualquier función de cuentas de usuario no son creadas automáticamente por default, deben ser creadas ó asignadas individualmente.

Para dar de alta un usuario utilizando SYSCON:

- a) *SYSCON (Enter)*
- b) *Seleccionamos User Information*
- c) *Despliega un listado de los usuarios dados de alta actualmente en la red, nos posicionamos en cualquiera de éstos, presionamos la Tecla <INSERT>*
- d) *Nos aparecerá en el inferior de la pantalla un recuadro, donde nos pide el nombre que se le asignara a la cuenta con la que trabajará el usuario, lo tecleamos (Enter)*
- e) *Observarás que el nombre de la cuenta se agregó al listado (del inciso c)*
- f) *Nos posicionamos en el nombre de la nueva cuenta y presionamos <Enter>, aparecerán varias opciones (password, límite de espacio en disco, login script), las cuales se llenarán de acuerdo a las especificaciones del administrador de la red.*

*Para salir de cada opción <Esc>, al salir de la utileria te pregunta si deseas guardar todos los cambios realizados.*

MAKEUSER: Puedes crear múltiples cuentas de usuarios creando y procesando un script (equivalente a un archivo por lotes en DOS) .USR con ésta utilidad. Un .USR es una lista de comandos en un archivo de texto que especifica como crear usuarios y las funciones de cada cuenta del usuario (tales como grupo, miembros, passwords y restricciones del tiempo de uso de la red). Sin embargo MAKEUSER no soporta asignar derechos a archivos, sólo a directorios. Puedes crear múltiples usuarios.

USERDEF: También asigna a los nuevos usuarios un password inicial, y configuraciones de trabajos de impresión, para que nuevos usuarios puedan trabajar en la red.

Cuando los usuarios son creados con los defaults proporcionados por el USERDEF, cada nuevo usuario es automáticamente provisto de un login script básico con el mapeo (path) de drives esenciales. La primer búsqueda del drive mapeado es SYS:PUBLIC y el segundo al directorio default del usuario.

Aunque los nuevos usuarios pueden empezar a trabajar inmediatamente con su cuenta, se recomienda utilizar USERDEF cuando:

- *Se tiene que dar de alta un gran número de usuarios*
- *Se tienen que crear cuentas de usuario en serie, pero no es posible realizar scripts con MAKEUSER, se crea una plantilla personalizada para los usuarios.*

## BIBLIOGRAFIA

RECOPIACION DE PUBLICACIONES DE LA REVISTA RED PUBLICADA POR EL GRUPO INTERSYS

TRADUCCION DE LA AYUDA (HELP) DE NOVELL INSTALADO EN AGENCIAS VOLKSWAGEN

CURSO DE REDES LOCALES ORGANIZADO POR EL CLUB DE INFORMATICA DE LA U.A.N.L.

ASESORIA DE EL ING. PORFIRIO RODRIGUEZ RESPONSABLE DEL MANTENIMIENTO DE LAS REDES DEL GRUPO VOLKSWAGEN

MANUAL DE CURSO DE ADMINISTRADOR CERTIFICADO POR NOVELL

CURSO DE ADMINISTRACION DE NOVELL NETWARE 3.11

