35

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

"C A M P U S A R A G O N"

IMPLEMENTACION DE UNA INTRANET EN EL CENTRO NACIONAL DE CONTROL DE ENERGIA

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

RUBEN SANCHEZ CLEMENTE
ALEJANDRO MAXIMILIANO PADILLA

ASESOR:
ING. ENRIQUE GARCIA GUZMAN

MEXICO 2000

Implementación de una Intranet en el Centro Nacional de Control de Energía

AGRADECIMIENTOS

Rubén Sánchez Clemente

Quiero dar gracias a:

Dios por haberme permitido llegar a esta fecha tan importante de mi vida en compañía de mis seres queridos.

A mi mamá que con sus sacrificios, apoyo y amor incondicional hicieron posible la terminación de mi carrera profesional y a quién debo todo lo que soy.

A mi hermano por su compañía, comprensión y apoyo.

A mi abuelita por todo su amor y su cariño que siempre fueron una motivación para lograr culminar esta etapa de mi vida.

A mi tíos, en especial a Eduardo, Arcelia, Cuca, Nabor por todo el apoyo incondicional que me brindaron a lo largo de mi carrera profesional.

A mi novia MHG por todo su amor y comprensión.

Agradezco a Nuestra Máxima Casa de Estudios, la UNAM, por haberme formado en esta hermosa profesión.

A mis amigos del CENACE por brindarme su apoyo, haciendo que la estancia en el trabajo fuese mas amena.

Al Ing. José Luis Pérez Mendoza por todo el apoyo recibido durante mi estancia en el CENACE.

Y a todas aquellas personas de una u otra forma influyeron para lograr culminar este proyecto.

Agradezco a mis Padres y mi Hermana, por estar siempre conmigo y ser parte de mi existencia.

Alejandro Maximiliano Padilla

INDICE

CAPITULO 3

TECNOLOGIAS DE CABLEADO EN REDES LAN.

CAPITULO 4

IMPLEMENTACION DE LA INTRANET

CAPITULO 5

ANÁLISIS DE COSTOS Y BENEFICIOS

INTRODUCCION

Nos encontramos en la era de la información en donde toda la sociedad gira alrededor de la transferencia, almacenamiento, creación y/o usos de los recursos para el procesamiento de información.

A medida que va progresando el desarrollo tecnológico y humano, empieza aumentar la necesidad de transmitir grandes cantidades de información a largas distancias, es por eso, que la transmisión de datos día con día desempeña un papel muy importante en nuestra sociedad, y a esto ha colaborado en gran medida la computadora que tiene capacidades de procesamiento cada vez más grandes y se espera sea mayor de acuerdo a la evolución de las computadoras.

El concepto de red de computadoras no es nuevo y nace de la necesidad de comunicar equipos de cómputo o computadoras independientes para formar un sistema integral. En los años 70's y 80's se inicia la combinación de los campos de la ciencia de computación y la comunicación de datos, por medio de las computadoras. Los adelantos de las comunicaciones de computadoras ha producido hechos importantes lográndose que no exista una diferencia fundamental entre procesamiento de datos (computadoras) y comunicaciones de datos (transmisión y equipo de conmutación).

Dicho resultado ha sido un traslape creciente de las industrias de computadoras y comunicaciones, empieza desde la fabricación de componentes hasta la integración de sistemas. El resultado es el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos e información. La tecnología y las organizaciones de estándares técnicos, se dirigen hacia un sistema público que integre todas las comunicaciones y haga que todas las fuentes de datos e información alrededor del mundo sean uniformes y accesibles de una manera más sencilla.

En la actualidad se han difundido mucho las redes de microcomputadoras llamadas Redes de Area Local (Local Area Networks), ya que por medio de estas redes se hace posible enlazar oficinas, equipos de producción, laboratorios, bibliotecas, etc. Dentro de un mismo edificio o conjunto de edificios, permitiendo a cualquier trabajador de la empresa almacenar, transmitir o recibir información.

Debido a que trabajadores de grandes habilidades deben cooperar rápidamente y comúnmente entre ellos para cumplir con sus metas críticas, teniendo sus computadoras personales infiltradas en lugares de trabajo; estos grupos productivos se dan cuenta que su productividad podía ser mejorada enlazando sus computadoras personales dentro de sus propias redes, compartiendo impresoras, ploters, escaners, manejadores de discos, archivos, permitiéndoles administrar y centralizar de forma optima la información con seguridad, que junto con la comunicación (comunicación remota, Internet, etc.), y servidor de Web forman lo que es una INTRANET.

Una Intranet es una red que existe exclusivamente dentro de una organización y que esta basada en la tecnología de Internet. Distribuye los recursos de información de la organización al escritorio de cada miembro de manera rápida y económica y, al mismo tiempo, protege la información frente accesos no autorizados.

Es importante hacer notar que existe una diferencia entre una red LAN y una Intranet, la red LAN permite compartir archivos, dispositivos de hardware como discos duros, impresoras, etc. en una red de área local, sin que necesariamente se tengan instalados servicios de Internet, como correo electrónico, o servidor de Web entre otros, que si son parte de una Intranet y que permiten el flujo de información de manera similar como ocurre en Internet, con la diferencia que este flujo de información es dentro de la red corporativa de una empresa. Puesto que una Intranet está basada en la tecnología de Internet, puede tener miles de usuarios ubicados en muchos lugares diferentes y seguir siendo privada.

De acuerdo al estudio realizado en el Centro Nacional de Control de Energía para la implantación de una Intranet en dicho lugar, nos encontramos con algunas deficiencias en el manejo de la información y procesos no adecuados de la información como son:

1. El estar sacando copias constantemente.
2. La búsqueda de información en los archivos particulares y generales del Centro Nacional de Control de Energía.
3. Ir a otros departamentos por información requerida.
4. Llamadas telefónicas o uso de faxes para obtener información.

Observando estos puntos, se decide que se deben reducir gastos y sobre todo el aprovechamiento del tiempo, ya que son dos de los puntos principales a resolver en la empresa y una de las mejores soluciones es la implementación de la Intranet con seguridad que nos permitió dar solución a dichos problemas.

El Centro Nacional de Control de Energía tuvo la necesidad de implementar una Intranet con seguridad y los beneficios que le proporcionaría la transmisión de datos para comunicar sus diversas áreas dentro de la empresa, con la finalidad de obtener la interconectividad total de computadoras personales a la Intranet

Sobre la base de las necesidades consideramos tres grupos de usuarios dentro de la empresa los cuales van a tener acceso a la Intranet y se mencionan a continuación:

Toma de decisiones: Gente involucrada en procesos de toma de decisiones para la organización del departamento, siendo estos los subdirectores.

Administrativo: Empleados que administran la información y los sistemas de flujo de información, que son gerentes y subgerentes.

Operativos: Personas que alimentan las aplicaciones y la información misma a los diferentes servidores que conforman el sistema.

En el presente trabajo se presenta un panorama general sobre redes de computadoras, se mencionan en el primer capítulo, los conceptos y antecedentes de las redes, así como los tipos de redes que existen y los elementos que las constituyen.

El segundo capítulo hace mención de la conectividad en las redes de área local y los protocolos de comunicación.

En el capítulo tercero se describen las diferentes topologías, así como las tecnologías de cableado en éstas redes.

El capítulo cuatro describe la implementación de la Intranet y todo lo que conlleva a constituirla, de tal forma que se detallará como configurar y administrar el servidor al igual que la instalación de los servicios que la integran.

Finalmente en el capítulo cinco, se mostrará de forma concreta el análisis costo beneficio como resultado de haber implementado la Intranet en el Centro Nacional de Control de Energía.

Las especificaciones de hardware y de software del equipo de computo, en el presente trabajo, tanto del servidor, como de las estaciones de trabajo fueron tomados a mediados de 1997, por lo que el equipo y especificaciones seleccionadas y reseñadas en la tesis corresponden al estado del arte de la computación en esa época; que en ese momento, eran considerados como equipos actuales, por lo que al hacer la implementación de la intranet, se utilizó el equipo de computo existente en el mercado.

OBJETIVO GENERAL

Implementar una Intranet con seguridad en la red para el Centro Nacional de Control de Energía y de ésta manera facilitar el intercambio de información que contendrá dicha Intranet.

OBJETIVOS PARTICULARES

Dar la definición de una red de Area Local (LAN), así como mencionar aspectos básicos sobre la LAN.

Identificar los protocolos y métodos de comunicación que se usarán para transmitir y recibir información.

Contar con un servidor de Intranet; el cual tendrá la información necesaria para satisfacer las necesidades actuales de comunicación e información dentro del Centro Nacional de Control de Energía. Pero lo más importante que tenga la capacidad de acomodarse a nuevas necesidades a medida que estas surjan.

Implantar una Intranet para el Centro Nacional de Control de Energía, que identifique plenamente las necesidades de los clientes (agilizar información), para quien se va a diseñar y así mejorar los flujos de información.

Crear un sistema de seguridad que permita tener confiabilidad sobre los sistemas institucionales de base de datos, es decir sobre toda la estructura de la Intranet. Así como la organización de los servidores de la Intranet.

Capítulo I

CONCEPTOS GENERALES DE LAS REDES DE COMPUTADORAS

CONCEPTOS GENERALES DE LAS REDES DE COMPUTADORAS

1.1. ANTECEDENTES

En los años setenta la tecnología permite el desarrollo de equipos más pequeños con capacidad regular, entonces se diseña un MAINFRAME más pequeño conocido como "MINICOMPUTADORA", este evento causa una revolución importante en la industria de la informática y las comunicaciones. La "MINICOMPUTADORA" llevó el poder de la computación a las empresas medianas, a un costo más accesible, comparado con los "MAINFRAME" anteriores.

Tiempo después, la tecnología avanza y permite la integración en miniatura de componentes electrónicos, obteniendo mayor capacidad y menor tamaño consiguiendo con esto, máquinas más pequeñas que sustituirían a las "MINICOMPUTADORAS'", a estas nuevas máquinas se les llamó: "MICROCOMPUTADORAS" ó PC's "Personal Computer; Computadora Personal", con ellas se introdujo a las pequeñas empresas al mundo de la informática y las comunicaciones. Estas máquinas ayudaron a descongestionar a las grandes unidades de procesamiento central.

Con la aparición de los discos duros era posible almacenar grandes cantidades de información; el inconveniente era el alto costo de estos discos duros, ya que a mayor capacidad mayor precio.

Durante algunos años las PC´s permanecieron como "islas de información", procesando datos de manera independiente. Sin embargo, la necesidad de compartir información con otros usuarios y tener al mismo tiempo seguridad en la misma, además de compartir recursos de alta utilización y alto costo como impresoras láser, CD-ROM, entre otros, origina la idea de interconectar entre sí todas las computadoras. Así surgen las REDES DE COMPUTADORAS.

1.2. CONCEPTO DE RED

Una red es la interconexión entre dos o más computadoras a través de uno o más medios de comunicación, con el objetivo de comunicarse e intercambiar información y usar recursos comunes.

De la anterior definición podemos listar algunas ventajas de las redes de computadoras tales como:

a) Manejo confiable de toda la información a través, de la red.
b) Cuenta con niveles de seguridad para el acceso de los usuarios a la red.
c) Mejoran la comunicación.

d) Incrementan la productividad.
e) Permiten ahorrar dinero al aprovechar mejor los recursos comunes como impresoras, fax, CD-ROM, por citar algunos.

En general, existen tres tipos de redes que se clasifican principalmente por su cobertura geográfica. Estos tipos de redes son:

a) Red de Área Local (LAN: Local Área Network).
b) Red de Área Metropolitana (MAN Metropolitan Área Network).
c) Red de Área Amplia (WAN: Wide Área Network).

1.3. REDES DE ÁREA LOCAL (LAN Local Área Network)

En nuestro concepto, una LAN es un conjunto de computadoras interconectadas entre sí para intercambiar información y compartir recursos parece una tarea simple, hasta que se ve con detalle todo lo que implica un correcto intercambio de información.

El control de esta información puede estar centralizado, distribuido o ser una combinación de ambos. Una LAN generalmente, se encuentra dentro de un área física relativamente reducida (por ejemplo, un local comercial, un edificio o edificios cercanos entre sí). Por definición, las redes de área local tienen impuesta una restricción de alcance, limitando así su área de cobertura que por lo regular es de 1 km., pero no debe exceder más de 10 Km. siempre y cuando se utilicen los dispositivos de conectividad apropiados que las normas permitan para garantizar que la red funcione.

Se estima que las redes de área local manejan aproximadamente dos tercios del volumen total de las necesidades de comunicación de las grandes organizaciones. Según la práctica se afirma que en términos generales, el 80% de los requerimientos de procesamiento en las aplicaciones más comunes se resuelven en un entorno de 100 metros de la ubicación del usuario, y otro 10% dentro de los 800 metros siguientes. Si atendemos lo anterior, se puede decir que el 90% de los requerimientos de procesamiento de información se resuelven dentro de una LAN. Figura 1.1

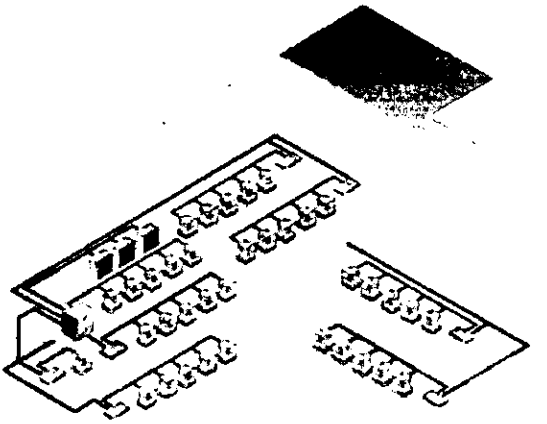


Fig. 1.1 Red LAN

1.4. ELEMENTOS DE LAS REDES DE ÁREA LOCAL

Las redes locales normalmente constan de un servidor de archivos o de varios servidores (computadoras o equipos que prestan un servicio), estaciones de trabajo (computadoras que son servidas), un software administrador de red, el medio de comunicación (cableado) y las tarjetas de red (interfaz entre la PC y el cableado). Fig. 1.2

A continuación presentamos una descripción resumida de los elementos básicos que componen a una red.

Servidor

Estación de Trabajo

Tarjeta de red

Fig. 1.2 Elementos Básicos de Red

1.4.1. EL SERVIDOR DE ARCHIVOS (File Server)

El servidor de archivos es una computadora con características particulares en una red, su función es dar a todos los usuarios acceso a la misma información, compartiendo su disco duro, archivos e impresoras; además cuenta con niveles de seguridad. El servidor debe contar con un procesador rápido, 128 MBytes de memoria RAM como mínimo y con gran capacidad de expansión, un disco duro de por lo menos 2.5 Gbytes para almacenar información. Debe contar con un software capaz de administrar todos los recursos (sistema operativo de red), con ello se obtiene una gran eficiencia e integridad en la mayoría de la información. En el servidor se cargan los programas de aplicación para el usuario, mas no interviene en el procesamiento de la aplicación.

El acceso a los archivos residentes en el servidor, se realiza guardando el orden de actualización por el procedimiento de bloqueo de registros, es decir, cuando un usuario se encuentra actualizando alguna información, el SERVIDOR bloquea el acceso a esta información para evitar que otro usuario la extraiga e intente actualizarla o trabajar sobre ella al mismo tiempo.

Existen dos tipos de servidores de archivos, que son:

1). Servidor de archivos dedicado.
2). Servidor de archivos no dedicado.

SERVIDOR DE ARCHIVOS DEDICADO

Un servidor de archivos dedicado se usa solamente para "administrar" a todas las pc's y periféricos de una red y, no puede utilizarse como una computadora normal en la que se ejecuten programas de aplicación. Es importante aclarar que el servidor de archivos no interviene en el procesamiento de la información, que es la tarea que más tiempo le quita a una computadora.

SERVIDOR DE ARCHIVOS NO DEDICADO

El Servidor de Archivos no dedicado, es una PC que además de trabajar como servidor de archivos administrando los recursos, puede funcionar como una estación de trabajo más en la red como cualquier otra, ejecutando programas de aplicación.

1.4.2. LAS ESTACIONES DE TRABAJO (PC's)

Las características de las computadoras destinadas a ser estación de trabajo de una red, pueden ir desde una modesta 486 con 8 MBytes de memoria RAM corriendo un sistema operativo DOS Versión 6.0 en adelante, hasta una PC 586 ó superior con 32 MBytes de RAM y Windows 95, Windows98 o Mc OS instalado. Estas pc's deben tener por lo menos una ranura ó slot libre para insertar una tarjeta de red.

En una red de tamaño mediano, con 50 usuarios, el servidor de archivos debe atender miles de solicitudes de lectura y escritura. Esta carga recae sobre las tarjetas de red y las unidades de disco duro.

Hay cinco tipos de bus en una PC y por supuesto en los servidores:

- ISA (Arquitectura Estándar de la Industria). La principal ventaja del bus ISA es que la mayoría de los vendedores de adaptadores diseñan para él, lo que hace que haya disponible un amplio rango de adaptadores para propósitos especiales.

- EISA (Arquitectura Estándar de la Industria Extendida). El bus EISA es una extensión del bus ISA. Puede instalar adaptadores de bus ISA estándar en estos sistemas, pero los adaptadores específicos para EISA proporcionan un rendimiento mejorado. Aunque EISA es un éxito técnico, no ha tenido un gran éxito comercial.

- VL-BUS (Arquitectura de Bus Local de Video). Bus de 32 bits de longitud de palabra de datos para PCs.

- MCA (Arquitectura de Microcanal). El bus MCA es un bus propietario desarrollado por IBM. El bus MCA, igual que el bus EISA ofrece un mejor rendimiento que el bus ISA más común. Como el bus MCA no ha tenido un gran éxito comercial, son limitadas las opciones para adaptadores MCA.

- PCI (Bus Local de Interconexión de Componentes Periféricos). El bus PCI es el de mas uso en la actualidad. Este es un nuevo estándar de bus que tiene compatibilidad con dispositivos de bus ISA, pero ofrece los beneficios de rendimiento de un bus local de 64 bits. Aunque el bus local PCI es relativamente nuevo, promete ser un éxito en sistemas de alto rendimiento.

Las estaciones de trabajo o nodos de red son pc´s encargadas de accesar y procesar en su CPU las aplicaciones que le solicitan al servidor.

Las Pc´s usan cinco tipos diferentes de disco duro. A continuación se proporcionan las características principales de cada tipo:

- MFM (Modified Frecuency Modulation, modificación de frecuencia modificada). Es un subsistema de disco MFM, el controlador reside en un adaptador y no en el disco. Los subsistemas MFM usan dos cables para conectar el controlador y el disco duro. Las unidades MFM representan la tecnología más antigua y el rendimiento más lento.

- RLL (Run Length Limited, longitud de ejecución limitada). Las unidades RLL son una modificación de los adaptadores de las unidades MFM, y empacan los datos en el disco duro con mayor capacidad que las unidades MFM.

- ESDI (Enhaced Small Disk Interface, Interfaz mejorada de disco pequeña). Las unidades de ESDI proporcionan mayor velocidad que las unidades anteriores, aunque en el aspecto técnico son mejores que las unidades MFM y RLL, las unidades ESDI nunca han tenido un gran éxito comercial.

- IDE (Interfaz Drive Electronic, Electrónica de interfaz integrada). La circuiteria del controlador de disco duro IDE reside en el ensamble de la unidad. El bus de la PC tiene instalado un adaptador anfitrión IDE para conectar el disco duro del sistema. Las unidades IDE proporcionan un excelente rendimiento y son con mucho el tipo de unidad más común instalado en las Pc´s actuales. Algunas PC´s tiene el adaptador anfitrión IDE integrado en la tarjeta del sistema, lo que elimina la necesidad de un adaptador anfitrión. El disco se conecta al anfitrión mediante un solo cable.

- SCSI (Small Computer System Interface, Interfaz de sistema de computadora pequeña). Como las unidades IDE, las SCSI tiene la circuitería del controlador integrada en el ensamble del disco y emplean un adaptador integrado para conectar dispositivos. El adaptador anfitrión es en realidad un subbus, en el que se pueden conectar hasta siete dispositivos.

ACTUALIZACIÓN DE LAS ESTACIONES DE TRABAJO

Cuando se ha instalado una red en una empresa, fábrica, corporativo, etc., lo ideal es que todas las estaciones de trabajo sean de la misma marca y modelo, esto con el fin de administrar mejor la red.

Pero en realidad una red esta compuesta por una gran variedad de estaciones de trabajo de diferentes fabricantes y por supuesto de características muy diferentes unas de otras. Actualmente el hardware de una estación de trabajo esta muy relacionado con el software que se esta empleando y la tendencia en cuanto a sistemas operativos de clientes es Windows, por lo cual los equipos viejos no podrán correr estas aplicaciones. Para solucionar este problema se tienen dos alternativas, la primera es cambiar todo el equipo viejo por uno más reciente y la otra solución que resulta más económica es actualizar las estaciones de trabajo. Una actualización se refiere al hecho de cambiar de procesador, disco duro y agregar más RAM.

Para ampliar la memoria RAM de una estación de trabajo se tiene que tomar en cuenta las características del SIMM o DIMM, esto con el fin de no tener conflictos con la memoria. En el manual de usuario de cada máquina se especifican las características de los SIMM´s (por ejemplo en el caso de la máquina DELL modelo Optiplez Gs se recomienda colocar SIMM de 72 pines con paridad con una velocidad de 70 ns).

Para los equipos viejos en donde ocupan SIMM de 30 pines es mejor cambiar la mother board, ya que esto también nos indica que el procesador que emplea no es tan poderoso como los actuales. La implementación de los SIMM en las estaciones de trabajo no requiere de ninguna configuración especial, dado que la máquina al encenderse hace un

test de la RAM que tiene. Cuando un SIMM no es compatible con la mother board esta se manifiesta de varias formas, entre ellas la ausencia de vídeo, conflictos con aplicaciones, el no-reconocimiento de toda la RAM, etc. Para el caso de los servidores, la RAM es más sofisticada, en algunos casos los SIMM (Con paridad) ya cuentan con autocorreción de errores y una velocidad mayor comparada con la que se emplea en las estaciones de trabajo.

Para instalar un disco duro IDE en las estaciones de trabajo, se tiene que consultar nuevamente el manual del usuario de la PC en el que nos indicará la capacidad máxima que puede soportar un disco duro, sin la necesidad de usar un software especial como el Disk Manager. En máquinas 386 y 486 por lo regular la máxima capacidad que se podía soportar era de 500 Mb y se tenía que instalar un drive para utilizar un disco de mayor capacidad. Con las mother board para Pentium MMX y Pentium II las capacidades de los discos son mayores llegando arriba de 4 Gb.

El instalar un disco duro de mayor capacidad de la que puede soportar la PC, se utiliza el Disk Manager o cualquier otra aplicación similar, y en el mejor de los casos al comprar el disco duro este ya viene con el software de instalación y solo hay que seguir las instrucciones para su instalación. Pero antes de eso el disco duro tuvo que ser configurado. La configuración en los discos duros se refiere al valor jerárquico que tendrá el disco, ya sea maestro o esclavo, si solo se cuenta con un solo disco este tendrá que estar configurado como maestro. La configuración se hace por medio de jumpers.

Para cambiar el procesador de la PC no es tan fácil, ya que no se puede cambiar un procesador 386X por un Pentium dado que la mother board no soporta el nuevo procesador.

El cambio de un procesador esta limitado a la capacidad de la mother board, si la mother board puede soportar el procesador que se pretende instalar, hay que hacer algunas configuraciones en la mother board. Estas configuraciones se hacen por medio de jumpers y los parámetros que se tocan son: la velocidad del procesador y el voltaje del mismo. Si los parámetros no coinciden con las especificaciones del procesador, este no trabajará y se verá reflejado en la Pc por la ausencia de vídeo.

Para las mother board viejas es recomendable también reemplazarlas, dado que estas se limitan a soportar procesadores 386 ó 486 de 33 a 60 Mhz.

1.4.3. EL SISTEMA OPERATIVO DE RED

Un sistema operativo de red es un programa (software) que se instala en el SERVIDOR DE ARCHIVOS y una pequeña parte se encarga de manera residente en las estaciones de trabajo, para que, estas puedan conectarse al servidor. Este Software es quien rige y administra todos los recursos y periféricos,ricos de la red, y además, lleva todo el control de la seguridad y acceso de toda la información.

El sistema operativo de red se engloba en dos componentes básicos:

a) El sistema operativo del servidor de la red.
b) El sistema que reside en las estaciones de trabajo.

El sistema operativo del servidor se ejecuta dentro de la máquina del servidor y soporta todos los servicios solicitados. El sistema operativo de red es proporcionado por el fabricante.

Los componentes del sistema operativo que residen en las estaciones de trabajo se ejecutan en estas, y establecen la conexión con la red y el servidor, y además controlan el flujo de las comunicaciones.

Las siguientes son algunas de las características propias de un sistema operativo de red:

- Ofrecen Seguridad de Acceso a la red.
- Verifican el Estado de Funcionamiento de cada uno de los dispositivos conectados a la red.
- Administran los Recursos de la red tales como impresoras, unidades de cintas, CD ROM, sistemas de archivos, bases de datos, entre otros.
- Efectúan el monitoreo de todos los elementos de la red.
- Basan su funcionamiento en el Sistema Operativo DOS. OS/2 y Windows NT.

COMPARACIÓN ENTRE LOS DIFERENTES SISTEMAS OPERATIVOS DE RED

Actualmente existen varios sistemas operativos de red, algunos proporcionan mayor rendimiento y seguridad que otros, por lo cual, cada uno tiene una participación diferente en el mercado. En México, son dos los sistemas operativos más vendidos, aunque no son los únicos, estos sistemas son: NetWare de Novell y Windows NT de Microsoft. Sin embargo, existen otros sistemas operativos y en constante desarrollo por sus fabricantes, entre los que destacan:

1. NetWare de Novell Inc.
2. LAN Server de IBM Corporation.
3. LAN Manager de Microsoft.
4. Windows NT Advanced Server de Microsoft.
5. VINES de Banyan Systems.

Enseguida se presenta una comparación entre algunos Sistemas Operativos de Red, tomando como base su rendimiento en redes LAN pequeñas, medianas, medianas/grandes y grandes. También se hace referencia a los requerimientos de Hardware para el servidor.

Requerimientos de Hardware en el servidor para Novell NetWare:

- PC Compatible con procesador 386, 486 o superior. 8 MBytes de Memoria RAM como mínimo (12 MB recomendados).
- Mínimo 90 MB de espacio libre en disco duro. (15 MB para una partición para el sistema operativo 75MB para la partición Novell).
- Sistema Operativo (Versión 5.0 o superior).

Además de los servicios de archivo y de impresión, este sistema operativo de red ofrece un completo rango de características, entre las que se encuentra el sistema de correo electrónico, los servicios de nombre y directorios y un método que permite a los desarrolladores de otras firmas comerciales la creación de servicios adicionales, llamados módulos cargables de NetWare (NLM). Mediante este método, los usuarios pueden tener acceso a servicios de fax, copias de seguridad, protección de antivirus y muchos otros.

Requerimientos de Hardware en el servidor para OS/2 LAN Server de IBM:

- PC Compatible con procesador 386 o superior. 8 MBytes de Memoria RAM (16 MB recomendados). 60 MB de espacio libre en disco duro.

Este sistema operativo de red de 32 bits funciona sobre IBM OS/2 2.x como sistema igualitario y como sistema cliente-servidor. Proporciona a los usuarios una tecnología de objetos distribuida, similar a la incrustación y vinculación de objetos (OLE) de la familia Microsoft. La estrategia de objetos de IBM, llamada Open Doc, no solo permite que los objetos se compartan entre aplicaciones y redes, también los incluye en tareas. Con Open Doc los usuarios serán capaces de leer aplicaciones no monolíticas, como son Microsoft Word o cualquier otra aplicación. LAN Server también rivaliza con la estabilidad y la potencia de Novell NetWare gracias a su nuevo multiproceso simétrico. Sin embargo, no es capaz de utilizar dinámicamente servicios de red como lo hace NetWare con su arquitectura NLM.

Se denomina sistema igualitario, cuando ambos equipos pueden trabajar uno sobre el otro de forma idéntica. Las redes Macintosh, hasta la última aparición de los archivos de trabajo en grupo y los servidores de impresión son un ejemplo excelente de red igualitaria.

Requerimientos de Hardware en el servidor para Microsoft LAN Manager

- PC Compatible con procesador 386 o superior, 5 MB de Memoria RAM (8 MB recomendados), 30 MB de espacio libre en disco duro.

Requerimientos de Hardware en el servidor para Microsoft Windows NT Advanced Server

- PC Compatible con procesador 386, 486, PENTIUM o superior. También puede operar con procesadores RISC. 32 MB de Memoria RAM (64 MB recomendados). 92 MB de espacio libre en disco duro.

Este sistema operativo de 32 bits amenaza la competencia y estabilidad de Novell NetWare mediante su multitarea con derecho preferente, su multiproceso simétrico (la posibilidad de utilizar procesadores para realizar tareas simultáneamente) y la capacidad de direccionamiento de memoria en Gigabytes. Este entorno operativo se utilizará como pieza central en muchas redes basadas en Windows 95.

Requerimientos de Hardware en el servidor para Vines de Banyan Systems:

- PC Compatible con procesador 386 (486 recomendable) 6 superior. 4 MB de Memoria RAM (8 MB recomendados).
- 40 MB de espacio libre en disco duro.

Gracias a su servicio y a StreetTalk, Banyan VINES es un excelente sistema operativo de red para los modelos cliente servidor basados en WAN. Los usuarios, independientes de su ubicación, pueden obtener acceso fácil y rápido a los servicios de archivos, impresión y correo electrónico entre otros.

De acuerdo con la aplicación es el requerimiento de memoria. Generalmente este dato se encuentra en una guía o catalogo de productos, también se puede localizar en los manuales de instalación de Hardware y Software de los fabricantes. Normalmente la memoria RAM de un servidor se puede establecer empíricamente por un número múltiplo de 4, (ya que 4 MBytes es la memoria base o estándar de casi todos los equipos de cómputo), pudiendo ser 8, 12, 16, 20, 24, 28, 32 Mbytes, etc. Una razón más es que los "SIMM´s" de memoria son fabricados para estas capacidades.

1.4.4 EL CABLEADO DE RED

El cableado es la columna vertebral de cualquier estructura de red, ya que es el medio de comunicación responsable de llevar la información de un nodo a otro. Este punto se verá con mas detalle en el Capítulo 3.

1.4.5. LAS TARJETAS DE RED

Las tarjetas de red permiten empaquetar la información y transmitirla a una velocidad de acuerdo a la configuración determinada para el envío. Las tarjetas de red

varían según la topología y el protocolo de red que vayan a utilizar, como pueden ser: Ethernet y Token Ring, que son las redes locales más comunes en el mercado.

1.5. PROCESAMIENTO CENTRALIZADO Y DISTRIBUIDO

En un sistema Mainframe, el sistema central tiene conectadas terminales tontas (estas terminales son generalmente equipos de captura de datos e impresoras), de manera que el procesamiento de información ocurre en un mismo punto (el sistema central), a esto se le llama PROCESAMIENTO CENTRALIZADO ya que el Mainframe es quien procesa la información de todas las terminales. En otras palabras, el procesamiento centralizado es aquel donde todos los usuarios comparten la capacidad de un procesador central con una sola copia del Software de aplicación que corre en este mismo. Las terminales tontas enlazadas que requieren usar la aplicación deben compartir la copia de dicho procesador.

En contraste a lo anterior, el PROCESAMIENTO DISTRIBUIDO es mucho más flexible, ya que el procesamiento de la información se lleva a cabo en cada estación de trabajo instalada a la red; es decir, se realiza en forma descentralizada. De esta manera, una red completa puede ser vista como un solo dispositivo de cómputo. En este tipo de procesamiento cada PC corre su propia copia del programa y el sistema operativo de red sincroniza el uso de los recursos compartidos para las múltiples aplicaciones.

Los beneficios, rendimiento, flexibilidad y ahorro en costos que ofrece la tecnología del procesamiento distribuido, son mayores que los que otorga el procesamiento centralizado en la mayor parte de las redes actuales, por ello es el más utilizado.

1.6. SERVICIOS DISTRIBUIDOS

El procesamiento distribuido, especialmente en redes de computadoras donde el número de máquinas interconectadas es grande, hace que este procesamiento se lleve al punto llamado: SERVICIOS DISTRIBUIDOS. Los servicios o procesos distribuidos se llevan a cabo cuando existen varios servidores en la red y cada uno de ellos realiza tareas especificas. No se trata de varios servidores de archivos, ya que el servidor de archivos donde reside el sistema operativo de red es uno solo. Algunos ejemplos de servicios distribuidos son los servidores de archivos, de comunicaciones y de impresión (aunque los tres tipos de servidores se pueden hallar concentrados en una sola PC).

En muchas ocasiones se conjuntan varios de estos servicios mencionados, en una sola de las computadoras de la red. Es decir, si en una misma computadora se instala el sistema operativo de la red (servidor de archivos), el software de comunicaciones (servidor de comunicaciones) el manejador de las bases de datos (servidor de base de datos) y muchas impresoras compartidas (servidor de impresión), se estarán integrando demasiadas tareas en un solo procesador y se caerá en parte en un procesamiento centralizado, a pesar de que el procesamiento de la información sigue siendo distribuido.

1.7. VENTAJAS DE LAS REDES DE AREA LOCAL

1.- Es indudable que poder compartir recursos, trae como consecuencia mayores posibilidades desde el punto de vista de las aplicaciones; así como también, disminuyen los costos por usuario conectado.

2.- Compatibilidad de equipos. Esto quiere decir, que en una red se puede tener flexibilidad a nivel de interconexiones, proporcionando la posibilidad de poder conectar equipos de diferente tecnología, proveedor, aplicación. etc.

3.- Procesamiento distribuido. Es la posibilidad de tener unidades redundantes, para no depender de un único elemento central, permite disponer de cierto grado de independencia a nivel de usuario para poder procesar los datos en el lugar donde se origina, se toman las decisiones finales. Estos beneficios trae consigo el uso de las redes de área local.

4.- Aplicaciones complementarias. Las comunicaciones entre estaciones de trabajo, el acceso a base de datos y documentación útil, el soporte de correo electrónico, etc., son otros beneficios relacionados al uso de las redes locales.

5.- Distribución física Hardware. Las redes permiten optimizar la disposición de los equipos, mejorando la interrelación entre el hombre y la máquina; los requerimientos ambientales, reduciendo los costos de instalación, volviendo estéticos los lugares de trabajo.

6.- Las redes locales también presentan simplicidad y flexibilidad de configuración. Las altas y bajas de elementos en la red no afectan al resto de los usuarios ni implican cambios en el software de control.

1.8. TIPOS DE REDES DE ÁREA LOCAL

Hoy día, se pueden encontrar dos tipos de redes locales: el modelo punto-a-punto y el modelo de servidor residente (tradicional). Sin embargo, el modelo tradicional es el más desarrollado y que mejor soporte tiene por parte de los fabricantes de Software.

En esencia todas las redes se parecen, ya que están formadas por los cinco componentes que ya mencionamos (servidor, estaciones de trabajo, software de red, tarjetas y cableado) y la finalidad que persiguen sigue siendo la misma: intercambiar información y recursos A continuación describiremos muy brevemente los tres tipos de redes de área local.

1.8.1. RED PUNTO A PUNTO

Por punto a punto (peer-to-peer) nos referimos a una estructura de red donde todas las máquinas pueden intercambiar entre sí sus recursos; no hay un punto central en la red,

aquí todas las máquinas son iguales. Así, una estación cualquiera de la red puede leer los archivos de cualquier otra (siempre y cuando esté encendida y conectada a la red) como si fueran propios y existentes en algún disco duro interno.

Las redes ***Punto a Punto*** son tan simples, que pueden crecer hasta 500 máquinas sin necesidad de requerir de un servidor dedicado. Una ventaja fundamental de este tipo de red, es que no requieren de mucho hardware para su buen funcionamiento.

1.8.2. RED CON SERVIDOR RESIDENTE (Modelo Tradicional)

El modelo de red con "servidor residente" es el esquema tradicional, y permite concentrar en una o varias máquinas dedicadas los recursos más importantes, de modo que puedan ser utilizados por cualquier máquina de la red (siempre y cuando se le otorguen los derechos al usuario). Dicha concentración permite una administración muy eficiente de todos los recursos. Este es el modelo del que más instalaciones se han hecho, y por consiguiente, el que mayor número de productos tiene en el mercado

Este modelo es recomendable para los medianos y grandes negocios, donde la contabilidad y la seguridad de la red es prioritaria, aunada a una gran capacidad de procesamiento y manejo de información entre varios sistemas operativos o diferentes versiones del mismo.

Las redes con servidor residente usualmente requieren de un administrador para instalar y dar mantenimiento mediante Software a la red. Sin embargo, este modelo facilita el manejo de programas sofisticados, bases de datos y además brinda mucha solidez en el control de la información debido a que ésta se encuentra concentrada en un sólo punto, el Servidor de Archivos.

1.8.3. EL MODELO DE RED CLIENTE/SERVIDOR

Se califica como cliente/servidor ***a una red basada en servidor, con lo que indica que el servidor dedicado comparte sus recursos con otros mientras el cliente se sirve de esos recursos.***
Una red basada en cliente/servidor debe estar compuesta por lo general por servidores dedicados muy poderosos, con unidades de disco grande, que deben tener capacidad de soportar cientos de nodos. El software cliente se instala en cada estación de trabajo y reside con el software del sistema operativo, lo cual permite que el nodo tenga acceso a los recursos compartidos de cada servidor. Debido a que las redes basadas en servidor suelen estar conectadas a una WAN, ***La seguridad es un requisito vital: se requiere proteger la información contra acceso no autorizado y contra pérdidas accidentales.***

En otras palabras, el cliente puede efectuar otras tareas y solo recibe resultados ya procesadas por el servidor.

Por una parte el modelo contempla a nivel aplicaciones dos partes, una llamada **Front-End,** y la otra **Back-End.**

El Front-End es la parte de la aplicación que interactúa con el usuario, está ubicada en la estación de trabajo (equipo terminal) y potencialmente orientada a la interpretación y presentación de la información procedente del servidor, generalmente está conformada por un ambiente gráfico.

El Back-End es la parte que reside en el servidor, básicamente orientada a recibir las solicitudes del cliente teniendo la capacidad de procesarlas, y de regresar la información solicitada al cliente.

El modelo Cliente/Servidor puede emplearse donde se desee el equipo de cómputo y procesamiento distribuidos más que el empleo de grandes equipos de procesamiento Centralizado De ninguna manera esto quiere decir que es más económico o sencillo, simplemente es otra tecnología que presenta ventajas operativas exclusivas y el desahogo del canal de comunicaciones.

1.9. REDES DE ÁREA METROPOLITANA (Metropolitan Area Network).

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbits/s hasta 155 Mbits/s.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

El objetivo de las redes de área metropolitana es ofrecer sobre el área urbana el nivel de ancho de banda requerido para tareas tales como: aplicaciones cliente-servidor, intercambio de documentos, transferencia de mensajes, acceso a base de datos y transferencia de imágenes.

Las redes de área metropolitana tienen muchas aplicaciones, las principales son:

- Interconexión de redes de área local
- Interconexión de pequeñas centrales telefónicas digitales
- Interconexión ordenador a ordenador
- Transmisión de vídeo e imágenes
- Transmisión CAD/CAM
- Pasarelas para redes de área extensa (WANs)

Una red MAN será recomendada cuando haya una necesidad para transportar simultáneamente diferentes tipos de tráfico tales como datos, voz y vídeo sobre un área no mayor de 150 kms de diámetro para entornos públicos o privados.

1.10. REDES DE ÁREA AMPLIA (Wide Área Network).

La necesidad de comunicación no sólo dentro de una área geográfica pequeña sino en distancias mucho mayores, como por ejemplo, oficinas del Distrito Federal con la Ciudad de Monterrey o Guadalajara, traen como consecuencia que se desarrollen formas de integración de protocolos, topología y sistemas operativos para la comunicación entre éstas diferentes oficinas que posiblemente cuentan con estructura en comunicaciones diferente. Este es el inicio del concepto de interoperabilidad que permite precisamente esta interacción.

Una Red de Área amplia traspasa los límites geográficos de lo que inicialmente comprendía una red local, esta red puede estar distribuida a lo largo de una ciudad o de un país o de un continente.

Por lo tanto, una red local se convierte en parte de una WAN o red de área amplia usando el enlace se establece entre sistemas centrales y como medio de comunicación se usa una red pública de datos e inclusive con otra red a través de la red telefónica pudiendo ser privada o rentada, microondas y satélites entre otros.

Capítulo II

CONECTIVIDAD EN REDES DE AREA LOCAL

CONECTIVIDAD EN REDES DE AREA LOCAL

2.1. ANTECEDENTES

En este capítulo se habla sobre el Modelo OSI, los Estándares del Comité de la IEEE 802 que hacen referencia a los dos niveles más bajos del Modelo OSI, el Nivel Físico y el Nivel de Enlace de Datos, estos estándares proporcionan una vía libre de errores para llegar al Nivel de Red del Modelo OSI.

Los protocolos de comunicación juegan un papel muy importante ya que son los responsables de la secuencia y la integridad de todos los datos transmitidos entre las estaciones de trabajo, esto lo realizan mediante caracteres de control bien definidos que aseguran que los datos lleguen correctamente a cada estación de trabajo, entre los protocolos más conocidos se encuentran CSMA/CD que significa Acceso Múltiple con Sensor de Portadora/Detección de Colisiones, es un método de acceso de LAN en la cual la contienda entre dos o más estaciones es resuelta mediante la detección de colisiones. Antes de empezar a transmitir verifica que nadie más utilice el canal de comunicación, cuando dos estaciones transmiten al mismo tiempo, ambas se detienen e informan que ha ocurrido una colisión, luego cada una intenta nuevamente transmitir después de esperar un tiempo aleatorio, generalmente es de varios microsegundos. En el protocolo Token Passing ó Paso de Testigo las estaciones de trabajo sólo pueden transmitir información cuando reciben un "Token" (señal de control) el cual está circulando por toda la red.

Los tipos de redes más conocidas y usadas en la actualidad son Ethernet, Token Ring y FDDI. La red Ethernet utiliza un protocolo de Acceso al Medio CSMA/CD con topología lineal. La Red Token Ring utiliza un "Token" para la transmisión de la información en una topología de anillo. La red FDDI especifica una LAN con anillo con protocolo "Token Passing" de Alta Velocidad y como medio físico de transmisión Fibra Optica, básicamente se usa en Redes "Backbone" ó Redes de Columna, en los Centros de Cómputo y en Redes de Alta Velocidad.

La interconectividad entre los equipos y protocolos es muy variada e importante, existen básicamente 4 tipos de equipos para este fin.

1. Los repetidores permiten extender la longitud de la red, amplificar y retransmitir la señal de la red, enlazan redes iguales y trabajan solo en el Nivel Físico del Modelo OSI. Fig. 2.1

Fig. 2.1 Repetidor.

2. Los Puentes conectan dos LAN separadas para crear lo que aparenta ser una sola LAN. Los puentes revisan la dirección asociada con cada paquete de información. Luego, si la dirección es la correspondiente al otro segmento de red, el puente pasará el paquete al segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento de red actual, no pasará el paquete al otro lado. Aíslan el tráfico de red o una sección de la misma y trabajan en el Nivel Físico y de Enlace. Fig. 2.2

Fig. 2.2 Puente.

3. Los Ruteadores son similares a los puentes, solo que operan a un nivel diferente. Los ruteadores requieren por lo general que cada red tenga el mismo Net Operating System (Sistema operativo de Red). Con un Sistema operativo de red común, el ruteador puede ejecutar diferentes funciones más avanzadas que las que podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring. Los ruteadores también suelen ser lo suficientemente inteligentes para determinar la ruta más eficiente para el envío de datos, en caso de haber más de una ruta. Aprovechan la existencia de vías alternas en la red ó redes para el envío de información y trabajan en el Nivel Físico, de Enlace y en el de Red. Fig. 2.3.

Fig. 2.3 Ruteador.

4. Las compuertas permiten la comunicación entre redes de diferente protocolo y operan en los niveles superiores, de Transporte, Sesión, Presentación y Aplicación.

2.2. EL MODELO DE INTERCONEXION DE SISTEMAS ABIERTOS OSI

La Organización Internacional de Normalización conocida como ISO (International Standards Organization), es una Federación de organismos que se ocupa de la elaboración de Recomendaciones Internacionales, a partir de propuestas de los países miembros y otros organismos profesionales, así como comerciales.

El objetivo de la ISO es definir una serie de mecanismos que hagan posible la interconexión de Sistemas Informáticos Heterogéneos, utilizando los medios públicos de

Transmisión de Datos, como las líneas telefónicas. Se proporcionan o fijan bases lo suficientemente amplias y bien definidas, que faciliten el desarrollo de sistemas de interconexión.

ISO como organismo, propone el modelo denominado OSI (Open Systems Interconetion, Interconexión de Sistemas Abiertos), como un estándar a nivel mundial del que parten los fabricantes para lograr que sus productos se comuniquen.

Este modelo define la estructura de una red como una jerarquía de 7 capas o niveles. Cada capa o nivel comprende una serie de funciones bien definidas para la comunicación entre computadoras. Adicionalmente a cada capa se le agrega o quita señales de control dependiendo de su función.

El objetivo principal del modelo OSI, es definir en una red como debe ver una estación de trabajo a otra. Esto permite la interconexión de redes que difieren en los aspectos de aplicación, organización interna y operación.

A continuación se da una breve descripción de los siete niveles del modelo OSI (Ver figura 2.4).

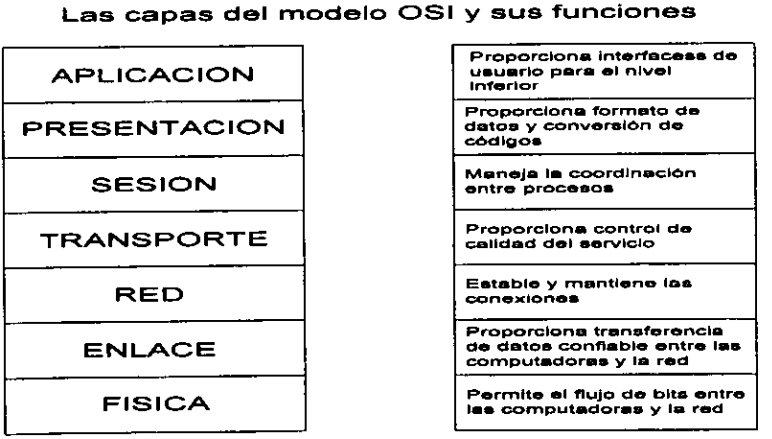


Fig.2.4 Modelo OSI.

NIVEL 1 CAPA FISICA

En este nivel se lleva a cabo el intercambio de señales eléctricas (bits) que representan a los datos y a la información de control. Este nivel incluye la especificación de las características mecánicas de la conexión física (cable y conectores) y eléctricas (como el nivel de voltaje y duración de la señal o bits). También se definen los procedimientos para establecer, mantener y liberar las conexiones entre los circuitos eléctricos que están enlazados físicamente por el medio de comunicación.

En este nivel se realiza el conocimiento de la recepción de datos a partir de los bits que le proporciona el nivel físico y le agrega información de control. Es aquí donde se definen los protocolos de comunicaciones o de enlace de datos.

Existen actualmente, diferentes tipos de protocolos de enlace de datos utilizados en el intercambio de información, los más conocidos son el CSMA/CD y Token Passing, los cuales se describen más adelante. En esta categoría de protocolos se define la forma en que los datos se manejarán, por ejemplo: Formatos de Mensajes, Señales de Control, Sincronización, Velocidades de transmisión y otras funciones adicionales que optimicen a la red.

NIVEL 2 CAPA DE ENLACE

El nivel 2 también se encarga de asegurar la Confiabilidad de la transferencia de datos, por medio de la técnica del control de errores, con la posibilidad de Retransmisión si es necesario. También está presente en este nivel, el Control de Flujo para evitar que los dispositivos más rápidos saturen a los más lentos.

El nivel de enlace de datos, proporciona los elementos necesarios para establecer, mantener y terminar interconexiones de enlace de datos, entre elementos del nivel de red correspondiente al nivel 3.

CAPA 3 NIVEL DE RED

El nivel de red es el responsable del enrutamiento de los paquetes de datos a través de la red, para ello toma los paquetes que provienen del nivel superior (nivel de transporte) y les añade la información de la dirección de destino. Es decir, determina la forma de direccionamiento y entrega de los paquetes de información en una red de transmisión de datos.

Cada vez que un paquete llega a una estación de trabajo, el nivel tres de esta estación deberá seleccionar el mejor enlace de datos por el que enviará la información. El enrutamiento se puede limitar a una sola red o extenderse a la transferencia de paquetes entre redes interconectadas.

NIVEL 4 CAPA DE TRANSPORTE

El nivel 4 es el encargado de proporcionar un Servicio de Transmisión y Recepción confiable de la información a través del sistema. Es quien asegura la entrega puntual e intercambio de datos, ya que conoce las direcciones de origen y destino que le proporcionó la capa de red. Para asegurar la entrega de los datos le añade a la información señales de protección que tienen que ver con el control del circuito como la prevención de errores y colisiones.

CAPA 5 NIVEL DE SESION

El Nivel de Transporte es responsable de transmitir de la manera más eficiente y con la velocidad que corresponda para las necesidades del Nivel de Sesión.

La distinción entre los niveles 3 y 4 del modelo OSI no es del todo clara, y de hecho, el punto de división lógico se encuentra entre los niveles 4 y 5. Los niveles del 1 al 4 están encargados de la transmisión de los datos de acuerdo a la técnica elegida, mientras que los niveles del 5 al 7 se involucran en el uso de estos datos, estos últimos son los concernientes al utilizar los datos que los niveles inferiores han comunicado o transportado.

El nivel de sesión establece, mantiene y termina la conexión en combinación con un proceso entre terminales de una red, es decir, involucra el diálogo de comunicación entre las redes o elementos de una red. Es decir, si se va a enviar un archivo a la impresora o un mensaje a otra.

La capa sesión también maneja problemas en las capas más altas del modelo OSI, como el inadecuado espacio en disco duro y la falta de papel en la impresora.

NIVEL 6 CAPA DE PRESENTACION

El Nivel de Presentación proporciona un conjunto de servicios de conversión y descifrado que la capa de aplicación (nivel 7) puede seleccionar (de un formato a otro) para poder interpretar el significado de los datos intercambiados; es decir, transforma los datos en un formato que puede ser entendido por cada aplicación y por las computadoras que en ellas corren. La capa de presentación puede también comprimir, expandir, encriptar y desencriptar datos.

NIVEL 7 CAPA DE APLICACION

El Nivel de Aplicación es el nivel superior del Modelo OSI y el más alto en la jerarquía de la red. Éste es el nivel que interactúa directamente con el software de aplicación y el usuario que quiere transferir datos a través de la red; es decir, es la interfaz de comunicación entre el usuario y las aplicaciones de la computadora. Ejemplos de las aplicaciones de red incluyen el acceso a archivos, transferencia de información, manejo de la red, servicios de directorio y servicios de correo electrónico, por citar algunos. Los programas y las aplicaciones se comunican unos con otros a través de esta capa.

Los demás niveles del modelo existen con el único propósito de satisfacer las necesidades de este nivel y ocultan las características físicas de la red subyacente.

En la mayoría de las redes locales el nivel uno se aplica en el hardware y el nivel dos se aplica parcialmente en el hardware, uniendo los cables sueltos con el software. El nivel tres y siguientes normalmente se aplican en el software. Por lo general, el nivel tres es el último nivel que tiene en cuenta las propiedades particulares de la red en la cual opera. Los niveles superiores son normalmente independientes de la red.

Se observa el resultado final del Nivel de Aplicación en su interacción con los niveles inferiores del modelo OSI, este nivel es el que visualiza el usuario final.

2.3. EL ESTANDAR "IEEE 802"

A principios de la década de los ochentas , el IEEE (con sede en los Estados Unidos y de naturaleza multinacional) se dedicó a la tarea de desarrollar un estándar para redes locales. Hasta la fecha , el comité 802 de la IEEE ha desarrollado una familia de estándares con la finalidad de unificar criterios, tratando de encontrar una solución armónica y eficiente que ahorre esfuerzos aislados, buscando un nivel de compatibilidad a través del desarrollo de recomendaciones de uso "universal" para beneficio de los fabricantes y del usuario final.

Las especificaciones del comité IEEE 802 tratan lo concerniente a los dos niveles más bajos del modelo OSI. Los estándares de la IEEE 802 para redes locales se definen a continuación:

El estándar IEEE 802.1 proporciona una introducción a los estándares 802 y está proyectado con el fin de integrar otros estándares. También especifica la relación de los estándares IEEE y su interacción con el modelo OSI. En términos específicos, 802.1 ofrece los servicios de interconectividad y se ubica en el nivel de red del modelo de OSI.

El IEEE subdivide las funciones del nivel de enlace de datos del modelo OSI en dos partes. Una parte define el Control de Acceso al Medio (llamado subnivel MAC), mientras que la otra parte es llamada Control de Enlace Lógico (subnivel LLC), abarca los siguientes puntos:

- Administración de los sistemas
- Manejo de red
- Aplicaciones de alto nivel
- Topología, arquitectura, direccionamiento y redes de área metropolitana (MAN)
- Prueba de conformidad
- Protocolos de trabajo y de red

El estándar IEEE 802.2. Control de enlace lógico (LLC). Es el responsable de proporcionar una vía de transmisión libre de errores al nivel de red en el modelo OSI. Además, estas funciones son transparentes a los niveles superiores. Los servicios que proporciona la 802.2 (subnivel LLC) son compatibles con varios estándares de Control de Acceso al Medio (MAC). El estándar IEEE 802.2 fué modelado para implementar la parte superior del nivel de enlace del modelo OSI, abarca los siguientes puntos:

- Protocolo de control de enlace lógico
- Control de flujo de enlace lógico
- Administración de la subcapa de enlace lógico
- Interface de control de enlace al medio
- Interface a la capa de red
- Opción de seguridad para enlace

El estándar IEEE 802.3. Red de Area Local. Está basado para una red con topología de "bus" lineal y método de acceso al medio CSMA/CD para Ethernet. Sin embargo, proporciona múltiples opciones para el nivel físico, incluyendo diferentes modos de señalamiento, tipos de medios, topologías y velocidades de transmisión. Algunos estándares para el nivel físico que puede manejar 802.3 son: 10Base5, 10Base2,10BaseT, 10BROAD36, abarca los siguientes puntos:

- Capa física y control de acceso al medio (MAC) para redes CSMA/CD tipo bus
- Topología de sistemas
- Administración de capas
- Mantenimiento 802.3
- Prueba de conformidad

La IEEE publicó un suplemento de estándares, el cual presenta las especificaciones para cuatro nuevos apartados que son:

- IEEE 802.3a. Especificaciones para la unidad de conexión al medio(tranceptor), así como el medio de transmisión de redes LAN tipo 10Base2 (10 megabits/segundo, transmisión banda base, segmentos de cable coaxial de 200 metros).
- IEEE 802.3b. Especificaciones de conexión al medio, para una red local de 10Broad36 (10 megabits/segundo, transmisión en banda amplia en segmentos de 3600 metros).
- IEEE 802.3c. Nuevas especificaciones para dispositivos repetidores que son utilizados en redes 10Base5 y para redes 10Base2.
- IEEE 802.3d. Especificaciones para unidades de enlace al medio y especificaciones para enlace al medio utilizado en redes de área local CSMA/CD 10Base5 con cable par trenzado (Red Estrella).

El estándar IEEE 802.4 Método de acceso Token Bus. Define una red usando el método de acceso al medio Token Passing (paso de señal ó paso de testigo lineal), que físicamente es un cable lineal, o en forma de árbol, al cuál se conectan las estaciones; pero su funcionamiento en realidad es el de un anillo lógico.

Para la capa física, el paso de testigo lineal utiliza un cable coaxial y puede tener una velocidad de 2.5 Mbps. La capa física en su totalidad, es completamente incompatible con el 802.3 y además, tiene un grado de complejidad mayor. Los puntos que trata son:

- Capa física y control de acceso al medio para redes de token bus passing.
- Topología de sistemas
- Administración de capa
- Mantenimiento
- Prueba de conformidad
- Banda base y banda amplia
- Fibra óptica

El estándar IEEE 802.5 Método de Acceso Token Ring. Es el único Control de Acceso al Medio (MAC) especificado por el IEEE para una Red de Area Local con topología en anillo. IEEE 802.5 es también análogo a los estándares 802.3 y 802.4 por lo que ocupa la parte baja del nivel de enlace del modelo de OSI.

Aunque IEEE 802.5 no especifica muchas limitaciones en el nivel físico, este estándar describe un anillo simple de hasta 250 estaciones conectadas en serie por enlaces punto a punto de cable STP con una velocidad de 4 a 16 Mbps. De esta especificación, se desarrolló el IBM Token Ring que actualmente se usa. Las redes Token Ring de IBM así como de otros fabricantes se ofrecen en velocidades de 4 ó 16 Mbps., abarca:

- Topología de sistemas
- Administración de capa
- Mantenimiento
- Pruebas de conformidad
- Velocidad de transmisión de 16 Mb.

En resumen, el IEEE 802.2 proporcionó el control lógico del enlace (LLC), IEEE 802.3 definió una red CSMA/CD, IEEE 802.4 definió una red lineal utilizando un acceso de paso de testigo lineal y el IEEE 802.5 definió una red en anillo utilizando acceso de paso de testigo en anillo.

El estándar IEEE 802.6 Anilo Ranurado (Slotted Ring). Se enfoca a las redes de área metropolitana (MAN). Se basa en una topología propuesta por la "University of Western Australia", conocida como DQDB (Distribuited Queue Dual Bus: Canal Dual de Cola Distribuida). DQDB utiliza un "bus" dual de fibra óptica como medio de transmisión. Ambos "buses" son unidireccionales, y en contra-sentido. Con esta tecnología el ancho de banda es distribuido entre los usuarios, de acuerdo a la demanda que exista. Puesto que puede llevar transmisión de datos síncronos y asíncronos, soporta aplicaciones de vídeo,

voz y datos. IEEE 802.6 con DQDB, es la alternativa que ofrece la IEEE para la Red Digital de Servicios Integrados (ISDN). Menciona los puntos siguientes:

- Capa física y control de acceso al medio.
- Fibra óptica
- Velocidad de Transmisión 43 Mb para anillos de 50 Km. en adelante
- Velocidad de 15 Mb en anillo de 2 Km.
- Anillo y bus dobles
- Conmutador multipuerto

Los estándares IEEE 802.7 y 802.8 son comités creados para apoyar y supervisar los desarrollos de tecnologías existentes, que puedan emigrar hacia fibra óptica o tecnologías en banda ancha (broadband), que utilizan señales analógicas y no digitales como los especificados anteriormente .

El estándar IEEE 802.9 Voz y datos integrados en una red LAN. Se enfoca en arquitecturas e interfaces estándares que permitan aplicaciones de escritorio con servicios integrados de voz, vídeo y datos. También se ha anunciado que este estándar sería compatible con la ISDN (Se tiene entendido que su ratificación se hará en fecha próxima).

El estándar IEEE 802.10 desarrolla otros estándares concernientes a seguridad en una red de área local, que incluyen mecanismos de seguridad en la transferencia de datos, administración de redes, administración de procesos de encriptación y procesos de seguridad compatibles con el modelo OSI.

El estándar IEEE 802.11 toca a las redes inalámbricas (Wireless LAN's) y especifica un sistema de red local por medio de radiofrecuencias. Debido a que su análisis y comprensión requiere de un estudio minucioso de la problemática que concierne al uso de frecuencias.

El estándar IEEE 802.12 prevé la posibilidad de que el estándar IEEE 802.3, se convierta en IEEE 802.12 para referirse al Fast Ethernet (Ethernet de alta velocidad: 100 Mbps usando el protocolo CSMA/CD).

El estándar IEEE 802.14 es una propuesta no ratificada para Fast Ethernet pero que no utiliza CSMA/CD para la capa de MAC. Por ahora este proyecto sigue denominado como 100 Base-VG y es la primera ocasión en que se pretende ratificar dos estándares oficiales e

internacionales, para una misma solución: Ethernet de alta velocidad (100 Mbps sobre cable de cobre de par trenzado)

2.4. PROTOCOLOS DE COMUNICACIONES EN REDES DE AREA LOCAL

Para que pueda existir una verdadera comunicación entre computadoras se requiere de un protocolo. El protocolo de comunicaciones se refiere a la manera de como los datos viajan de una estación a otra en una red; este es un procedimiento que se utiliza para controlar y administrar cuando una estación de trabajo se quiera comunicar con otra por la red. El protocolo puede considerarse, con ciertas limitaciones, como un "idioma" que permite a las computadoras comunicarse, del mismo modo que una persona se comunica con otra.

Cuando se diseñan redes de computadoras, una de las consideraciones fundamentales es la transmisión física de datos de una estación de trabajo con otra. Para cumplir con esta tarea exitosamente, se deben resolver problemas de sincronización entre la estación transmisora y receptora, además se debe prever la correcta secuencia en la transmisión de los datos. La solución para ello está en un protocolo de comunicaciones, el cuál es responsable de la secuencia e integridad de los datos transmitidos en las estaciones de trabajo y nodos de una red.

Usando caracteres de control bien definidos, el protocolo de comunicaciones proporciona una forma ordenada y precisa de asegurar que, entre otras cosas, los datos que son enviados de una estación a otra lleguen con prontitud y de que se verifique que lleguen correctamente a la estación receptora, así como de notificar a la estación transmisora que los datos fueron recibidos con éxito.

También el protocolo debe ser capaz, de indicarle a la estación transmisora cuando los datos recibidos fueron erróneos y que intente un nuevo envío. Dado que en el mismo enlace físico se transportan "datos" como "caracteres de control", el protocolo debe estar capacitado para distinguir, a los datos de los caracteres de control.

Existen varios protocolos para una red. No es posible mezclar dos tipos diferentes de protocolos de manera directa. Para poder comunicar dos protocolos distintos se utilizan dispositivos especiales como los "bridges" . A continuación hablaremos de los protocolos más comunes que se utilizan en las redes de área local.

2.4.1. PROTOCOLO "CSMA/CD"

Protocolo CSMA/CD: Carrier Sense Multiple Access/Collision Detection (Acceso Múltiple con Sensor de Portadora/Detección de Colisiones).

Este protocolo está basado en el concepto: "escuchar antes de hablar" (listen before talking). Significa que antes de que la estación transmita, toma un momento para verificar que nadie más está usando (escuchando) el canal de comunicaciones. Si nadie está transmitiendo, entonces se establece la comunicación. De otra manera, espera un tiempo y vuelve a checar si la red está libre. El método no es lo más seguro, ya que si dos estaciones "escuchan" y transmiten al mismo tiempo, los mensajes chocarán (hay una colisión) y los datos se perderán. Para compensar esta dificultad, las estaciones volverán a transmitir si descubren que los datos no se recibieron de forma correcta. Para eliminar las posibles contingencias, se le agrega un comando: CSMA/CD. Las dos últimas siglas se refieren a la declaración: **Collision Detection: Detección de Colisiones.**

En el protocolo CSMA/CD cuando dos o más estaciones de trabajo transmiten información simultáneamente ocurren colisiones, cuando se "detectan" estas colisiones, las estaciones de trabajo intentan repetir el envío una vez más; este proceso se repite las veces que sea necesario hasta que la transmisión es exitosa, así se impide la pérdida de datos.

Esto se realiza de la siguiente manera: cuando existe una colisión y las estaciones detectan que los mensajes enviados no fueron recibidos, las tarjetas de red "arrancan" un reloj (temporizador) de tiempo aleatorio para reintentar la transmisión. La estación que primero termine su reloj intentará transmitir nuevamente el mensaje, evitando con ello, que tenga otra colisión con la misma estación con que "chocó" inicialmente. Esto no implica necesariamente que no se tenga una segunda colisión con alguna otra estación de la red; si esto sucediera, las estaciones realizarían el mismo procedimiento para intentar la retransmisión. El tiempo de estos relojes oscila aleatoriamente, entre los microsegundos y los milisegundos. Lógicamente, entre más transmisiones se intenten, más colisiones pueden ocurrir.

2.4.2. PROTOCOLO "TOKEN PASSING"

Protocolo Token Passing (Paso de testigo o de ficha).

Este protocolo utiliza otro método de transmisión de datos para evitar colisiones con los paquetes de información que se transmiten. Con este protocolo, cada estación de trabajo conectada a la red sólo puede transmitir información cuando recibe la señal de autorización (token) que circula por la red. Al recibir una estación de trabajo el 'token', sólo esa estación y ninguna otra puede transmitir en ese momento. Esto asegura que no haya más de un paquete de información en la red a la vez. El token circula por toda la red,

estación por estación, asegurando de esta manera que cada estación de trabajo tenga la misma oportunidad de transmitir.

Este es el protocolo que utilizan las redes Arcnet y Token Ring, basado en un esquema libre de colisiones, dado que la señal (token) se pasa de una estación a la siguiente. Con esto se garantiza que el canal de comunicaciones siempre está libre para transmitir mensajes, por lo que se pueden tener tiempos de respuesta predecibles aún con gran cantidad de actividad en la red.

Uno de los inconvenientes de este método es que, al llegar el token a la estación, regenera el mensaje antes de pasarlo a la siguiente estación. Esto origina una reducción en el rendimiento de la red, pero se asegura una transmisión exitosa desde la primera vez que se envía el mensaje. Token Ring opera a una velocidad de transferencia de 4 ó 16 Mbps.

2.4.3. PROTOCOLO "CSMA/CD" VS. "TOKEN PASSING"

¿Cuál es mejor?

La diferencia principal entre estas dos maneras (protocolos) de enviar datos a través de una red, es que en las redes del tipo "Token Passing", como lo son la Arcnet y la Token Ring, una señal token se encuentra siempre circulando a una cierta velocidad, y que cada vez que esta ficha pasa por una estación, se le encarga el envío de un paquete de datos (información) al servidor o alguna otra estación de trabajo en la red. Mientras que en las redes con protocolo CSMA/CD como lo es la red Ethernet, cada estación es libre de enviar su paquete en cualquier momento 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 (por esta razón, a las redes Ethernet también se les conoce como redes de "contención"). En caso de que dos o más paquetes se envíen al mismo tiempo, el protocolo detecta la colisión y pide a las estaciones que retransmitan nuevamente.

Algunos profesionales hablan de una supuesta superioridad de las redes "Token Passing" sobre las de protocolo "CSMA/CD". Los defensores de Token Passing atacan al protocolo de Ethernet, porque aseverán que la existencia de colisiones al enviar los paquetes de datos con este protocolo, genera un comportamiento impredecible e inconsistente, así como retrasos determinados en su funcionamiento. Mientras que las redes Token Passing tienen retrasos determinísticos que conducen a un funcionamiento predecible y a un acceso justo e igual, proporcionado por la ausencia total de colisiones en la red.

Esto tiene algo de razón, sin embargo, se pierde de vista el hecho de que la eficiencia de las redes Ethernet parten precisamente de la utilización común de un sólo canal de comunicaciones mediante la administración de colisiones. Además, la gran velocidad de

transferencia de información que ofrece Ethernet 10 Mbps (y ahora de 100 Mbps), hace que su rendimiento sea superior al de otras redes.

Por otro lado, los profesionales que defienden a Ethernet dicen que el protocolo CSMA/CD, se basa en el principio de que cada estación tiene la misma oportunidad de usar la red. De hecho, la especificación 802.3 de la IEEE incluye un algoritmo de justicia, que impide que cualquier estación de trabajo o grupo de estaciones monopolicen la red.

Es difícil comparar directamente la eficiencia de las redes Token Passing contra las de protocolo CSMA/CD. Se menciona más adelante que unas funcionan mejor que otras en cierto tipo de ambientes. Ciertamente el Token Passing ofrece la seguridad de que en el momento de tener una estación el "token" podrá enviar sus datos. Sin embargo, esto por lo general, se compensa por la mayor velocidad de transferencia de las redes con protocolo CSMA/CD.

Es cierto que las redes Ethernet tienen colisiones al enviar mensajes, pero éstas son una parte normal en la operación de las redes CSMA/CD. Las colisiones son típicamente infrecuentes si se hace un buen diseño de la red, y cuando ocurren duran unas cuantas millonésima de segundo. La lógica para manejar las colisiones se integra en los chips de la tarjeta de red. Como una salvaguarda, si una estación experimenta un alto nivel de colisiones, se reporta un error y se le remueve de la red.

Aunque es verdad que bajo condiciones normales de funcionamiento una red Token Passing es muy determinística y predecible, ¿qué sucedería si se llega a perder la señal "token" para poder enviar los datos en una red de este tipo?. Para este caso, se tiene una rutina de recuperación en la red, empezando con un proceso llamado "beaconing", durante el cuál se identifica al maestro del sistema (que generalmente es el servidor de archivos). Cuando se identifica al maestro se genera un nuevo "token". Mientras esto sucede toda la red esta parada, y es entonces, cuando la naturaleza predecible de las redes Token Passing desaparece. Adicionalmente, este proceso puede tomar, inclusive, algunos segundos.

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

También los algoritmos del método CSMA/CD son mucho más simples que los de Token Passing, dando como resultado que las tarjetas de red sean más pequeñas, sencillas y menos costosas. Además, las redes como Ethernet utilizan conexiones de red pasivas, de modo que las estaciones de trabajo que no están involucradas en una transmisión no afectan el flujo de la información transmitida de ninguna manera; mientras que en el método Token Passing se tiene que regenerar el "token" en cada estación de la red.

Esto hace que las redes con protocolo CSMA/CD tengan gran confiabilidad ya que son menos susceptibles de falla. En general, las redes Token Passing hacen un extenso uso de los componentes activos en las tarjetas de red y en los repetidores entre otros. También requieren de una relación entre señal y ruido de 23 dB, mientras que las redes Ethernet requiere de tan solo 13 dB. Por esta razón, es fácil ejecutar Ethernet de 10 Mbps en cable de par telefónico, mientras que IBM recomienda el cable tipo I que está fuertemente protegido con una malla metálica para redes Token Ring, aún la de 4 Mbps. La característica de señal a ruido, habla de una mayor Confiabilidad de las redes Ethernet sobre las Token Ring en condiciones similares de cableado.

Para situaciones en que crece de manera significativa el número de estaciones en una red, ambos protocolos sufren un cierto degradamiento en su velocidad real de transferencia (conocida como: "throughput"). Pero no es posible representar mediante una fórmula el grado de degradamiento de uno u otro protocolo; ya que en ambos casos, se comporta irregularmente conforme una red crece. Los factores principales que afectan el rendimiento de una red cuando ésta crece son:

- El poder del servidor de archivos.
- La capacidad de memoria RAM del mismo servidor.
- El número de estaciones de trabajo así como su capacidad.
- Los parámetros del sistema operativo de red.
- Por mencionar los más importantes.

Finalmente es posible agregar que en la práctica el protocolo CSMA/CD y el Token Passing funcionan extremadamente bien. Se podría pasar mucho tiempo discutiendo las ventajas y desventajas de uno u otro protocolo pero lo que se lograría, sería agregar confusión sobre cuál método de acceso funciona mejor. Con toda razón los puntos a analizar serían académicos en su mayor parte. Además los usuarios finales en general, no pueden saber si están conectados con un protocolo u otro; lo único importante, es que para ellos sea transparente el manejo de la información.

2.5. PROTOCOLOS DE COMUNICACIÓN IPX/SPX

IPX/SPX (Internetwork Packet Exchange/Sequence Pack Exchange) es el protocolo de comunicación de las redes NetWare, de la casa de Software Novell, el protocolo de comunicación es propietario y se usa solamente en este tipo de redes, debido a su gran aceptación, ha logrado ser uno de los sistemas de red de área local más popular, por lo que las compañías que fabrican y diseñan equipos han logrado encaminar el protocolo independiente de que éste no lo sea.

Su comportamiento en redes pequeñas es aceptable y aún en redes grandes su rentabilidad es buena. Los equipos de encaminamiento envían tramas de una red a otra utilizando un puente de información (Bridge) en lugar de encaminarlas.

NetWare emplea inherentemente el intercambio de paquetes, o el IPX como su protocolo de red. IPX esta basado en el protocolo XNS originalmente de Xerox, con algunas funciones menos para ahorrar memoria. El reducido tamaño de IPX es razón importante para el éxito de NetWare sobre otras redes más aparatosas, dado que las PC´s con sistema operativo MS-DOS siempre han batallado con el límite de los 640 KB. IPX proporciona servicios básicos, compartición de impresoras y servicios de seguridad, estos son suficientes para satisfacer las demandas de red de la mayoría de las PC´s.

Muchas aplicaciones se refieren al protocolo NetWare como IPX/SPX, SPX o intercambio de paquetes secuenciado, es cargado por omisión cuando se carga IPX en estaciones de trabajo y servidores NetWare, SPX proporciona un control de errores adicionales y en realidad son pocas las aplicaciones de red que lo emplean.

2.6. PROTOCOLOS DE COMUNICACIÓN TCP/IP

Los protocolos establecen una descripción formal de los formatos que deberán presentar los mensajes para poder ser intercambiados por equipos de cómputo; además definen las reglas que ellos deben seguir para lograrlo.

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel (e.g. la transmisión de flujos de bits a un medio físico) hasta aquellas de más alto nivel (e.g. el compartir o transferir información desde una computadora a otra en la red).

Tomando al modelo OSI (Open Systems Interconection) como referencia podemos afirmar que para cada capa o nivel que él define existen uno o más protocolos interactuando. Los protocolos son entre pares (peer-to-peer), es decir, un protocolo de algún nivel dialoga con el protocolo del mismo nivel en la computadora remota.

Conjunto de Protocolos TCP/IP Origen
➢ Desarrollados como parte del proyecto DARPA a mediados de los 70´s, dando lugar a la red ARPANET. ➢ Su objetivo fue que computadoras cooperativas compartieran recursos mediante una red de comunicaciones. ➢ ARPANET deja de funcionar oficialmente en 1990.

En 1973, la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA), de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objetivo la interconexión de redes, por lo que se le denominó "Internetting", y a la familia de redes de computadoras que surgió de esta investigación se le denominó "Internet". Los protocolos desarrollados se denominaron el Conjunto de Protocolos TCP/IP, que surgieron de dos conjuntos previamente desarrollados; los Protocolos de Control de Transmisión (Transmition Control Protocol) e Internet (Internet Protocol).

El protocolo de comunicación es flexible y permite la transmisión sin errores entre diferentes sistemas, ya que ha estado funcionando desde hace más de 15 años y debido a que es un protocolo de transmisión, puede enviar grandes volúmenes de información a través de redes no confiables, garantizando que estos serán recibidos sin errores al momento de alcanzar su destino final.

Cuando se utiliza TCP/IP, la información viaja en segmentos creados por TCP entre emisor y receptor para poder accesar a alguna aplicación. Los segmentos creados por TCP son encapsulados en IP, a este proceso se le llama Datagrama IP. Este permite que los segmentos TCP que fueron creados por alguna aplicación puedan ser transmitidos o encaminados en la red de área local o entre redes de área extendida.

Las redes con protocolo TCP/IP permiten que la información pueda enviarse de un sistema a otro sin que estos tengan que ser del mismo fabricante, por ejemplo una estación de trabajo de Windows NT de Microsoft puede intercambiar información con una computadora que contenga NetWare de Novell, siempre y cuando utilicen el mismo protocolo de comunicación que en este caso es TCP/IP.

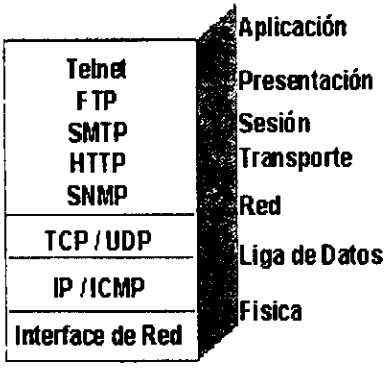
Conjunto de Protocolos TCP/IP
Su relación con el Modelo OSI

<table>
<tr><td>Aplicación</td><td rowspan="3">TELNET</td><td rowspan="3">FTP</td><td rowspan="3">SNMP</td><td rowspan="3">SMTP</td><td rowspan="3">DNS</td><td rowspan="3">HTTP</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td colspan="6">TCP</td></tr>
<tr><td>Red</td><td colspan="6">IP</td></tr>
<tr><td rowspan="2">Liga de Datos</td><td colspan="4">802.2</td><td>X.25</td><td>LLC/SNAP</td></tr>
<tr><td>802.3</td><td colspan="2">802.5</td><td colspan="2">LAPB</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td>Token Ring</td><td>FDDI</td><td colspan="2">Línea Síncrona WAN</td><td>SONET</td></tr>
</table>

TCP = TRANSFER CONTROL PROTOCOL
IP = INTERNET PROTOCOL

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP proponen cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Liga de Datos y Física son vistas como la capa de Interface a la Red. Por tal motivo para TCP/IP sólo existen las capas Interface de Red, la de Intercomunicación en Red, la de Transporte y la de Aplicación. Como puede verse TCP/IP presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de Liga de Datos y Físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse la capa de Interface de Red; siendo los más usuales el proyecto IEEE802, Ethernet, Token Ring y FDDI.

Modelo de capas de TCP/IP



Descripción del Modelo de Capas de TCP/IP

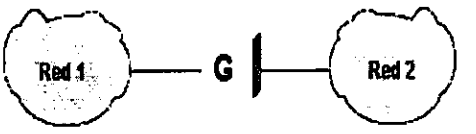
Capa de Aplicación.	Invoca programas que acceden servicios en la red. Interactuan con uno o más protocolos de transporte para enviar o recibir datos, en forma de mensajes o bien en forma de flujos de bytes.
Capa de Transporte.	Provee comunicación extremo a extremo desde un programa de aplicación a otro. Regula el flujo de información. Puede proveer un transporte confiable asegurándose que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota, esto lo hace añadiendo identificadores de cada una de las aplicaciones. Realiza además una verificación por suma, para asegurar que la información no sufrió alteraciones durante su transmisión.
Capa Internet.	Controla la comunicación entre un equipo y otro, decide qué rutas deben seguir los paquetes de información para alcanzar su destino. Conforma los paquetes IP que será enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación
Capa de Interface de Red.	Emite al medio físico los flujos de bit y recibe los que de él provienen. Consiste en los manejadores de los dispositivos que se conectan al medio de transmisión.

Arquitectura de Interconexión de Redes en TCP/IP Metas
➢ Independencia de tecnología de conexión a bajo nivel y la arquitectura de la computadora. ➢ Conectividad Universal a través de la red. ➢ Reconocimientos de extremo a extremo. ➢ Protocolos de Aplicación Estandarizados.

Arquitectura de Interconexión de Redes en TCP/IP Características
Protocolos de no conexión en el nivel de red. Conmutación de paquetes entre nodos. Protocolos de transporte con funciones de seguridad. Conjunto común de programas de aplicación.

Arquitectura de Interconexión de Redes en TCP/IP
Interconexión de Redes

Ø Las redes se comunican mediante compuertas.
Ø Todas las redes son vistas como iguales.



Para entender el funcionamiento de los protocolos TCP/IP debe tenerse en cuenta la arquitectura que ellos proponen para comunicar redes. Tal arquitectura ve como iguales a todas las redes a conectarse, sin tomar en cuenta el tamaño de ellas, ya sean locales o de cobertura amplia. Define que todas las redes que intercambiarán información deben estar conectadas a una misma computadora o equipo de procesamiento (dotados con dispositivos de comunicación); a tales computadoras se les denomina compuertas, pudiendo recibir otros nombres como enrutadores o puentes

Direcciones IP
➢ Longitud de 32 bits. ➢ Identifica a las redes y a los nodos conectados a ellas. ➢ Especifica la conexión entre redes. Se representan mediante cuatro octetos, escritos en formato decimal, separados por puntos.

Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) dependiendo del protocolo utilizado.

2.7. RED "ARCNET"

La red Arcnet utiliza el protocolo de comunicaciones "Token Passing", la topología de anillo y el cableado también en forma de anillo o de estrella (ver Figura 2.5). Arcnet significa: Red de Computadoras Recurso Agregado, y es una arquitectura de red muy simple y flexible, diseñada casi exclusivamente para redes pequeñas. Arcnet utiliza generalmente cable coaxial (RG-62 de 93 Ohms) como medio de transmisión.

Arcnet recorre todas las estaciones de trabajo de una red en forma de anillo, no por la posición física en que estén conectadas las estaciones, sino por el orden lógico que se les dá a cada una de ellas. Lo anterior significa que cada tarjeta de red lleva un número asignado de nodo, el cuál tiene que ser distinto de cualquier otro nodo de la red. Este número de nodo (node address) se direcciona físicamente (es decir, por Hardware) en cada tarjeta; sin embargo, algunos fabricantes ofrecen esta configuración a través de software y de hardware.

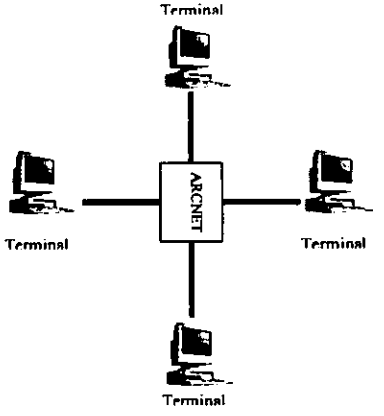


Fig. 2.5. Ejemplo de una red Arcnet tipo estrella físicamente.

En las redes Arcnet todo esto se desarrolla a una velocidad de 2.5 Mbps en el cableado.

Arcnet trabaja bien en los ambientes de oficina, donde hay un procesamiento ligero de transacción de archivos, o donde todas las estaciones de la red necesitan de un tiempo de acceso igual para desempeñar sus aplicaciones, generalmente con un número de estaciones de entre 10 a 25 como máximo.

2.8. RED "TOKEN RING"

En la red Token Ring la transmisión de paquetes de información se hace a través de 'tramas' por medio de un "token". Aquí una estación de trabajo podrá enviar información sólo cuando tenga el "token". Esto sucede cuando la estación toma el "token", cambia el primer bit de éste para identificarlo como un paquete de información (también conocido como "trama"), añade los datos y la dirección de destino, y envía la 'trama' por el cableado. Cada una de las estaciones de trabajo que están en la red, verifican si la 'trama' está direccionada a ellas; si no, la estación de origen retransmite la 'trama'. Cuando la estación destino recibe la 'trama', verifica que la información (por protocolo) sea correcta, copia la información de los datos, marca la 'trama' como recibida y regresa el "token" ya sin información al anillo.

Las fallas físicas tales como un rompimiento del cable, pueden causar que una estación de trabajo reciba una señal inválida de "su vecino de arriba" activo más cercano. Si esto ocurre, la estación de trabajo transmite una 'trama' de señales de error (MAC) para que la estación transmisora se dé cuenta que el paquete de información que le enviaron no fue recibido correctamente, e intente hacer una nueva transmisión. Mientras esto ocurre, la tarjeta automáticamente se remueve asimismo del anillo, se prueba a ella sola y al cable. Según el resultado, se reconecta o permanece desconectada del anillo. De esta manera, el anillo se recobra automáticamente.

Token Ring utiliza una topología de anillo conectado en estrella (ver Figura 2.6). Las estaciones se enlazan en una estrella alrededor de un concentrador ó MAU (Multiple Access Unit: Unidad de Acceso Múltiple). Los MAU a su vez, se conectan en anillo, todas las estaciones se configuran lógicamente en un anillo, sirviendo el MAU como un punto de conexión de las estaciones de trabajo y demás nodos.

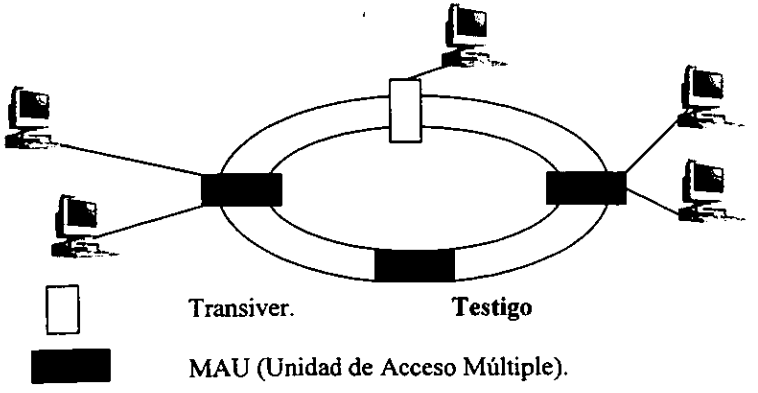


Fig. 2.6 Red Token- Ring con topología anillo.

2.8.1. COMPARACIONES ENTRE EL TOKEN RING DE 4 Y 16 MBPS

IBM ha creado Token Ring para que trabaje a dos velocidades de transmisión. A continuación haremos algunas comparaciones de estos dos sistemas de red.

El Token Ring de 16 Mbps ofrece dos funciones notables.

Primero: que el tamaño máximo de la 'trama' (paquete de información) es de aproximadamente 18 Kbytes, que es unas cuatro veces más largo que el Token Ring a 4 Mbps y unas 12 veces más largo que el de Ethernet que es de 1.5 Kbytes. Esto permite manejar un volumen más alto de información, ya que se requiere de menos transmisiones para una cierta cantidad de datos, tales como archivos largos de gráficas o de bases de datos.

Segundo: las redes Token Ring de 16 Mbps se caracterizan por permitir que dos 'tramas' de información viajen en el anillo simultáneamente en lugar de una, que es lo que permite el Token Ring de 4 Mbps. En el Token Ring de 4 Mbps, la estación transmisora receptora libera el "token" solo después de que recibió correctamente la información. A 4 Mbps la red casi siempre está en uso, pero a 16 Mbps, las 'tramas' de información gastan menos tiempo en la red, y se transmiten caracteres "de relleno" para llenar el espacio vacío que no se está ocupando, de esta manera se llena el ancho de banda que es capaz de soportar.

Token Ring es la solución idónea para aquellas compañías corporativas que no desean mezclarse con soluciones diferentes de las que ofrece IBM, ya que tiene una línea integrada de conectividad basada en Token Ring para sus Mainframe, minis y PC's.

NOTA:

Si bien el producto Token Ring es un producto confiable, Ethernet es una mejor alternativa en comparación con el Token Ring si se instala con cable de par trenzado, tomando como referencia el mismo nivel de presupuesto.

2.9. RED "ETHERNET"

Ethernet es el ambiente de comunicación entre PC's más utilizado en la actualidad. Ethernet se puede utilizar con las tres tecnologías de cableado, es decir, **con cable coaxial, cable de par trenzado (UTP) y con fibra óptica.** Este tipo de redes utiliza una topología de bus lineal con un protocolo de acceso CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

Hace algunos años, cuando Ethernet inició su penetración en el mercado, se encontraba restringida a una topología de bus que era limitada, debido a que todas las estaciones debían conectarse al mismo cable. Todavía hoy en dia, muchos de los productos Ethernet instalados conservan esa característica, en la que puede ser más difícil relocalizar o agregar estaciones a la red conforme ésta se expande. Lógicamente, mientras más largo es el bus, más difícil es aislar fallas. En las redes Ethernet cada estación se encuentra conectada bajo un mismo bus de comunicaciones, es decir, las estaciones de trabajo se

conectan al mismo cableado y por éste, se transmiten los paquetes de información hacia el servidor y/o los otros nodos (ver Figura 2.7).

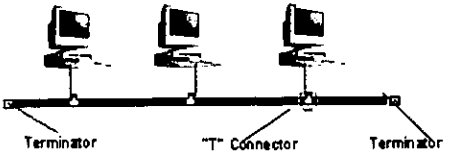


Fig. 2.7 Red Ethernet con topología bus.

Cuando dos estaciones de trabajo transmiten sus paquetes simultáneamente, una colisión ocurre y es necesaria una retransmisión. Ya que las estaciones aún están "escuchando" la red, saben que ha ocurrido una colisión e intentarán de nuevo la retransmisión de su paquete de información cada una de ellas. **El protocolo** es el responsable de detectar las colisiones, y además, incluye las reglas que determinan cuánto tiempo tendrán que esperar las estaciones de trabajo para realizar sus envíos nuevamente.

La velocidad de transmisión de Ethernet es de 10 Mbps, aunque ya existen productos en el mercado que operan a 100 Mbps utilizando el mismo protocolo CSMA/CD. Por lo contrario de lo que se pudiese pensar conforme al tipo de comunicación y operación, en el que se tienen tiempos de respuesta inconsistentes e impredecibles, su rendimiento es muy superior al de otro tipo de redes locales, ahora con la gran popularidad de Ethernet, han surgido diversas tecnologías que permiten la coexistencia de diversas topología bajo el protocolo CSMA/CD de Ethernet. Con ello, Ethernet tiene no solo las ventajas del "bus" y del "anillo" combinadas, sino que un gran número de fabricantes se han dedicado a proveer diversos tipos de concentradores y repetidores que facilitan el diseño de las redes Ethernet y que monitorean su funcionamiento.

Actualmente, este tipo de redes con cableado UTP y por la misma evolución de la tecnología, está regida bajo el estándar 10 Base T.

NOTA:

Si el presupuesto es la única medida de referencia en la instalación de una red, Ethernet es la mejor opción por su costo más bajo. También si se busca una estandarización para diversos ambientes y alta velocidad, Ethernet es lo más adecuado. Si se requiere integración completa para equipos y sistemas IBM, se recomienda en gran medida el Token Ring de 16 Mbps. Actualmente Arcnet sólo la podemos recomendar para algunas aplicaciones de automatización de procesos, para redes con terminales 'punto de venta' o para aquellos casos en que las aplicaciones que se comparten generen poco tráfico en la red, como lo son los procesadores de texto entre otros. Sin embargo, por la escasez y costo de los productos para redes Arcnet, siempre será más adecuado inclinarse por Ethernet.

2.10. RED "FDDI" (Fiber Distribuited Data Interface)

A mediados de la década de los ochenta, las estaciones de trabajo incrementaron grandemente su popularidad debido a las altas ventas de PC's de escritorio. Estas máquinas ofrecieron soporte de red típicamente para Token Ring y Ethernet; pero en poco tiempo, los usuarios se dieron cuenta que en ciertas aplicaciones, sobre todo donde se manejaban grandes cantidades de información (como en las bases de datos), un pequeño grupo de estaciones de trabajo podían generar mucho tráfico, consumiendo el ancho de banda existente en el Token Ring de 4 Mbps o los 10 Mbps de Ethernet, por lo que un nuevo estándar de red era necesario.

Así, en 1986 nace el estándar FDDI el cuál especifica a una LAN en anillo con protocolo Token Passing de alta velocidad, utilizando como medio de transmisión fibra óptica. FDDI incluye las especificaciones del nivel físico y del nivel de enlace del modelo OSI, por lo que es análogo al IEEE 802.3, 802.4 y 802.5. FDDI es utilizado generalmente para una de las tres aplicaciones siguientes:

1).- Redes Backbone (redes de columna). Estas redes proporcionan una alta velocidad en la línea de comunicaciones, a la cuál, otras redes pueden conectarse a ella.

2).- Redes de Salas de Cómputo. Estas redes conectan a grandes Mainframes, Minicomputadoras, y periféricos en una sala de cómputo donde se requiera gran velocidad de transmisión de información.

3).- LAN's de alta velocidad de datos. Estas redes conectan minicomputadoras de muy alta velocidad, estaciones de trabajo, o computadoras personales que requieran de una LAN rápida y de un ancho de banda que pueda soportar aplicaciones tales como vídeo y diseño asistido por computadora (CAD).

FDDI especifica una topología en la que existen dos anillos de fibra óptica (como canal de comunicaciones) independientes y de rotación inversa, que proporcionan una velocidad de 100 Mbps cada uno de ellos. Cada anillo de fibra puede soportar hasta 1,000 estaciones de trabajo. Las estaciones pueden estar separadas hasta 2 kilómetros y la circunferencia del anillo puede llegar hasta 10 kilómetros usando repetidores.

El esquema de "token múltiple" está basado en la necesidad de ejecutar sobre la red aplicaciones de tiempo real, por lo que la temporización está estructurada de modo que una estación de trabajo puede tener la certeza de capturar el testigo en el momento que lo desee.

2.11. CONECTIVIDAD EN REDES DE AREA LOCAL

A partir de la gran aceptación de las redes, los fabricantes se lanzaron a desarrollar equipos proponiendo nuevas posibilidades en ésta área. Las tendencias actuales indican una orientación definida hacia la CONECTIVIDAD, entendiéndose éste término como: la

solución para integrar los distintos equipos de diferentes marcas, modelos, sistemas operativos y protocolos de comunicaciones que utilicen. Nosotros podemos definir CONECTIVIDAD: **Es la capacidad o habilidad que tiene un equipo para conectarse con otro, haciendo compatibles el Hardware con el Software ya adquiridos de los diversos fabricantes como la solución al problema de interconexión.** Ahora el reto importante de esta tecnología, es ofrecer equipos confiables de alto rendimiento, que hagan uso de la infraestructura ya instalada por el usuario.

Hoy en día, la popularidad de las redes es indiscutible, gran parte de su éxito se debe a su capacidad de poder interconectar casi cualquier tipo de equipo, localmente o a grandes distancias. Los años ochenta se caracterizaron por la interconexión de computadoras en red, ahora en los noventas se busca más la habilidad de conectar entre si dos o más redes, para formar una red de redes, a esto se le conoce como "Internetworking"(interconexión de redes).

Existen básicamente cuatro tipos de dispositivos capaces de interconectar redes, y están divididos según la categoría donde operen en base a el modelo OSI. Estos dispositivos son los siguientes:

a) REPETIDORES (operan sólo a nivel físico).
b) PUENTES (operan a nivel de enlace de datos).
c) RUTEADORES (operan a nivel de red).
d) COMPUERTAS ó GATEWAYS (son convertidores de protocolos y operan a todos los niveles del modelo OSI).

A continuación, presentamos una explicación de los conceptos fundamentales de la operación de cada uno de los cuatro dispositivos mencionados anteriormente.

REPETIDORES

Son el producto más simple para enlazar redes de área local idénticas, y operan a nivel físico en el modelo OSI. Los repetidores extienden físicamente el enlace de una red, regenerando las señales (bits) que le llegan de un medio de transmisión y retransmitiéndolas a otro. Los medios de transmisión conectados por medio de un repetidor pueden ser de naturaleza distinta; por ejemplo, cable coaxial con par trenzado. También es posible conectar varios segmentos entre sí utilizando un solo repetidor multipuertos. La figura muestra la relación que existe en el Nivel Físico del Modelo OSI cuando se comunican dos redes iguales mediante un repetidor.

Un repetidor amplifica el nivel (de voltaje) de la señal de una red, ya que como se sabe, una señal al propagarse por medio de transmisión (cualquiera que sea) sufre, gradualmente, una disminución de amplitud (atenuación) y distorsión de su forma. Por esta razón, las normas (apoyadas por los fabricantes) fijan los limites de la longitud máxima de cada medio de transmisión para asegurar que la atenuación y distorsión no impidan la interpretación correcta de las señales recibidas. Si la longitud del medio de transmisión

excede la distancia máxima que establece la norma, debe insertarse un repetidor (o repetidores) a lo largo del medio para restaurar el nivel y forma de las señales.

Sin repetidores, la longitud máxima del medio de transmisión depende de dos cosas: la naturaleza del medio y la velocidad de transmisión. Por ejemplo, la IEEE 802.3 establece que para una velocidad de transmisión de 10 Mbps la longitud máxima es de 110 metros si se usa cable UTP (10 Base T), pero se puede alcanzar una distancia de hasta 250 metros con este mismo tipo de cable si la velocidad de transmisión se reduce a 1 Mbps. También la IEEE 802.3 indica que para los mismos 10 Mbps, la longitud máxima es de 500 metros si se usa cable coaxial grueso (10 Base 5), y de 185 metros si se usa cable coaxial delgado (10 Base 2).

Los repetidores interconectan segmentos para construir una sola red física. El número de repetidores que pueden conectarse en cascada para formar esta red está limitado por el Control de Acceso al Medio (MAC) utilizado, ya que existe un tiempo máximo de retardo que debe respetarse.

Los repetidores, como 'enlace' de la capa física del modelo OSI, no efectúan parte alguna del procesamiento de un nivel más alto que se requiere en las redes más complejas, ya que únicamente pasan bits directamente de un medio a otro. Así los repetidores sólo pueden comunicar redes con formatos de protocolos similares.

Generalmente los repetidores enlazan redes locales dentro de un solo edificio. Una de sus desventajas es que si la señal viene acompañada con ruido, también lo "regenera" (amplifica) a la par de la señal. Otra desventaja es que crea un mayor congestionamiento en la red.

PUENTES (BRIDGES)

Cuando se utilizan repetidores, las tramas enviadas por una estación se propagan a todos los segmentos de la red sin importar la localización física de la estación receptora, generando tráfico inútil en algunos segmentos de la red. Para resolver este problema se pueden utilizar "puentes", los cuáles permiten aislar el tráfico local de los diferentes segmentos de la red.

Con un grado de complejidad más elevado que los repetidores, los puentes conectan redes locales a nivel de la capa de enlace de datos del modelo OSI, y más específicamente en la subcapa MAC del modelo de la IEEE 802.

Los puentes permiten: interconectar redes que utilicen el mismo o diferente protocolo MAC, extender el enlace de una red y aumentar el número de estaciones que pueden conectarse a ella más allá de los límites permitidos por el protocolo MAC en una red sin puentes y, debido al aislamiento de tráfico, aumentan el desempeño de la red en su conjunto mejorado su disponibilidad.

Cuando un puente se conecta a dos o más redes locales, puede conocer las direcciones MAC (las direcciones MAC son las direcciones de las tarjetas de red) de las

estaciones que pueden ser alcanzadas directa o indirectamente a través de cada uno de los segmentos.

En esencia, de acuerdo a la norma IEEE 802.1, un puente lee todas las direcciones de origen y destino de todos los paquetes de información (tramas) que circulan por los segmentos a los cuales está conectando. Si la dirección de destino de un mensaje se encuentra en el mismo segmento sobre el cuál se originó el mensaje, el puente no permite que el paquete salga de ese segmento evitando con ello, tráfico inútil en los otros segmentos de la red: el puente realiza, en este caso, una especie de "filtrado".

Una característica muy importante de los puentes (así como de los repetidores) es que son transparentes para los usuarios y por lo tanto fáciles de instalar. Los puentes se conectan a la red y sin intervención del usuario funcionan automáticamente. La información de enrutamiento necesaria para su operación la obtienen mediante el mecanismo de aprendizaje antes descrito. Debe recordarse que cuando una estación de trabajo envía una información a otra, no envia el paquete de datos dirigido al puente sino a la estación receptora, esto hace que el usuario no tenga que preocuparse tampoco de la existencia de rutas alternas para su envío, ya que los paquetes de datos sólo contienen las direcciones de las estaciones fuente y destino (además claro, de la información propia).

Como los puentes funcionan en el nivel MAC, son independientes de los protocolos empleados en las capas superiores y permiten interconectar redes que utilicen protocolos diferentes, tales como TCP/IP, SPX/IPX, etc. En otras palabras, en las redes pueden coexistir diferentes tipos de protocolos de la capa 3 (capa de red) y superiores. En redes conectadas por puentes, las capas superiores del modelo OSI que residen en las estaciones de los usuarios eliminan cualquier incompatibilidad, lo que es muy importante para grandes organizaciones donde existen ambientes de cómputo y comunicaciones variados, y desean un ambiente de red homogéneo y sencillo.

Un puente, a diferencia de un repetidor, almacena la información que recibe y verifica que no tenga errores antes de procesarla. El almacenamiento y procesamiento de la información realizado por los puentes introduce un retardo que no existe en un repetidor y disminuye por lo tanto su rendimiento.

RUTEADORES (ROUTERS)

Los ruteadores conectan redes a nivel de capa de red del modelo OSI (Nivel 3), y ofrecen conectividad con enrutamiento selectivo de paquetes de datos, siguiendo los métodos establecidos por el protocolo de la capa de red que utilizan.

Los ruteadores pueden enviar paquetes sobre diferentes vías en una red dependiendo de ciertos criterios, tales como la vía con menor costo, la más rápida o más segura. Los ruteadores, a diferencia de los puentes, aprovechan la existencia de vías alternas en la red. Los ruteadores pueden servir para interconectar redes locales a redes de área amplia o redes locales entre sí. Para interconectar redes locales que se encuentran físicamente cercanas un ruteador se conecta directamente a las redes que interconecta, mientras que

para redes locales geográficamente dispersas los ruteadores se conectan a través de una red de área amplia (por ejemplo, una línea telefónica privada).

Los ruteadores utilizan un direccionamiento (lógico) de nivel 3 de tipo jerárquico (red estación) para enrutar los paquetes de datos entre las diferentes redes. Además, utilizan sólo la parte de red de la dirección para tomar sus decisiones de enrutamiento, lo que indica que sirven para interconectar redes separadas más que para formar una red lógicamente unificada como lo hacen los puentes. Esta característica facilita la administración de la interconexión de redes, sobre todo cuando el tamaño de la red es considerable.

Los ruteadores no son transparentes a las estaciones de los usuarios, ya que deben ser direccionados directamente por éstos para transmitir un paquete de datos de una red a otra. Cuando una estación en una red local quiere enviar un paquete a una estación que no se encuentra en la misma red, envía una 'trama' (subcapa MAC) dirigida a un ruteador conteniendo el paquete (capa de red) que debe ser transmitido a la otra red. El ruteador utiliza la dirección de red de la estación destino contenida en el paquete para determinar si puede enviarlo directamente a su destino final o necesita pasar por otro ruteador.

Los tipos de ruteadores se definen por las características con que fueron construidos, y pueden ser de Hardware o de Software. Los ruteadores multiprotocolo existen en ambos casos, los ruteadores simples, generalmente son de software.

COMPUERTAS (GATEWAYS)

Las compuertas (gateways) son los dispositivos de interconexión más complejos que existen, ya que permiten la comunicación entre redes que utilizan protocolos totalmente diferentes, por ejemplo, TCP/IP, ISO, SNA y DECnet entre muchos otros. Para lograrlo, las compuertas realizan una función completa de "conversión" de una arquitectura a otra sin modificar los datos transmitidos, de modo que los protocolos utilizados en la red fuente puedan ser entendidos en la red destino.

Este dispositivo opera en los niveles superiores al nivel de red (tercer nivel) del modelo de referencia OSI (transporte, sesión, presentación y aplicación) o su equivalente en cualquier arquitectura propietaria.

Al nivel más alto, las compuertas permiten que ciertas aplicaciones se comuniquen entre sí. Por ejemplo, diferentes correos electrónicos o diferentes aplicaciones de transferencia de archivos.

Las compuertas por las funciones que proporcionan, son lógicamente, más costosas y lentas que los puentes o los ruteadores, ya que efectúan más procesamiento para llevar a cabo la conversión de protocolos. Sin embargo, no hay que olvidar que estos dispositivos ofrecen un servicio muy importante y específico al permitir la comunicación entre estaciones de trabajo que utilizan protocolos totalmente distintos en todas sus capas. En este sentido, la gran aceptación del concepto de sistemas abiertos y la adopción de normas

universales deberá facilitar. aún más en el futuro, la interconexión de estaciones conectadas con diferentes redes.

Los Protocolos de Comunicaciones juegan un papel muy importante ya que son los responsables de la secuencia y la integridad de todos los datos transmitidos entre las Estaciones de Trabajo; además son el fundamento sobre el que se desarrollan las tarjetas de red para que las Estaciones de Trabajo en una red se comuniquen una con otra.

Existen básicamente cuatro tipos de dispositivos para lograr la interconectividad entre redes que son:

Los **Repetidores** por su parte enlazan redes iguales y se utilizan simplemente para extender el alcance de una red, trabajan sólo en el Nivel Físico del Modelo OSI. Los **Puentes** aíslan el tráfico de red ó una sección de la misma y trabajan en el Nivel Físico y de Enlace. Los **Ruteadores** aprovechan la existencia de vías alternas en la red ó redes para el envío de información y trabajan en el Nivel Físico, de Enlace y de Red en el Modelo OSI. Las **Compuertas** permiten la comunicación entre redes de diferente protocolo y operan en los Niveles superiores del Modelo OSI, como son el Nivel de Transporte, Sesión, Presentación y Aplicación.

Al evaluar diferentes opciones para la interconexión de redes locales, se debe tener cuidado de considerar los criterios que se aplican en la evaluación, ya que además de las razones de costo y rendimiento, deben considerarse otros factores como: capacidades de crecimiento y expansión, facilidad de uso y configuración, y capacidades para la administración de la red.

Capítulo III

TECNOLOGIAS DE CABLEADO EN REDES DE AREA LOCAL

TECNOLOGIAS DE CABLEADO EN REDES DE AREA LOCAL

3.1. ANTECEDENTES

El objetivo en este capítulo es explicar con detalle todo lo relacionado con el Cableado en redes locales. Para iniciar describiremos las topologías más comunes, siguiendo con las características de los diferentes tipos de cable que se pueden usar para construir una red. Hablaremos también del cableado estructurado y porqué es tan importante su instalación en la nueva generación de redes. Por último, mencionaremos los requisitos que se deben cumplir al conectar el cableado de red con los equipos de interconexión y, lo que es muy importante, las Normas y estándares de cableado para redes de área local.

A continuación hacemos una descripción de las topologías más comunes.

3.2. TOPOLOGIA EN REDES DE AREA LOCAL

La topología se refiere a la forma física de cómo se conecta y se cablean las estaciones de trabajo y demás nodos de una red, que bien pueden ser impresoras, unidades de respaldo, bibliotecas de CD-ROM y Fax-Modem entre otros. La elección de una topología u otra afectará la facilidad de la instalación, el costo por la longitud de cable empleado y la Confiabilidad de la red. Cinco son las topologías básicas en el cableado de redes locales que son:

1) Bus (Lineal)
2) Anillo
3) Estrella
4) Arbol
5) Malla

3.2.1. TOPOLOGIA DE BUS (Lineal)

En la topología de "bus" todas las estaciones de trabajo de una red, están conectadas a un medio único y pasivo de comunicaciones llamado "bus", como por ejemplo, un cable coaxial. La topología de "bus" es fácil de instalar y requiere de menos cable que cualquiera de las demás. En esta topología, las estaciones de trabajo se van "conectando" al "bus" con conectores tipo "T", los cuales permiten "derivar" la señal hacia las tarjetas de red manteniendo la continuidad del cable. También se requiere que en cada uno de los extremos del "bus" se conecten "TERMINADOR", estos "terminadores" deben ser de la misma impedancia del cable. Así por ejemplo, en redes Ethernet con cable coaxial, estos

terminadores son de 50 Ohms; mientras que para redes Arcnet estos terminadores son de 93 Ohms.

El principio de las redes con "bus lineal", se basa en la ausencia de una computadora central. Las redes de "bus" (Figura 3.1) permiten que los mensajes (datos) sean transmitidos a todas las estaciones de trabajo y otros nodos simultáneamente a través del cable. Cuando un elemento de la red reconoce que un mensaje va dirigido a él, lo saca del "bus". Como consecuencia de ésta independencia, aumenta notablemente la Confiabilidad propia de la red, así el "bus" requiere que cada tarjeta de red (o nodo) pueda transmitir, recibir y resolver problemas.

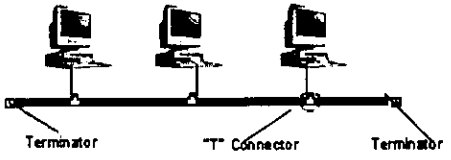


Fig. 3.1 Topología bus.

Actualmente, la red más conocida con topología de "bus" es la Ethernet, que permite que una gran cantidad y diversidad de productos se conecten a ella en puntos intermedios. Se explicó en el Capítulo 2 que Ethernet, usa el protocolo CSMA/CD para determinar lógicamente, qué elemento de la red tendrá acceso para transmitir la información en ese momento. Sobre esta topología están basadas las redes locales punto-a-punto, destacando: LANtastic, Personal Netware, Windows para Trabajo en Grupo, Windows 95 y Windows NT.

El número mínimo de dispositivos o computadoras conectadas a este tipo de topología es 100. Esto se debe al método de acceso que utiliza Ethernet.

Ventajas

- La falla en una computadora no afecta a la red
- Las conexiones a la red son flexibles y sencillas
- Es una topología económica en cuestión del cable, conectores y terminales

Desventajas

- Limitada en distancia y número de dispositivos conectados
- Difícil de aislar cuando hay problemas de cableado.
- Degradación del desempeño de la red con el crecimiento de dispositivos
- Frágil. Si el cable se desconecta o se troza, la red deja de funcionar en su totalidad, esto debido a perdida de impedancia

3.2.2. TOPOLOGIA DE ANILLO

En la topología de anillo las estaciones de trabajo y demás nodos de una red se conectan uno a continuación de otro como se muestra en la figura 3.2, construyendo físicamente un anillo. Aquí la información pasa de una estación a la siguiente a través de las tarjetas de red (que actúan como repetidores) conectadas entre sí por medio del cableado; de tal manera, que el cable termina en la misma estación de donde se inició. Esto hace que la topología de anillo sea más difícil de instalar que la topología de "bus" o estrella.

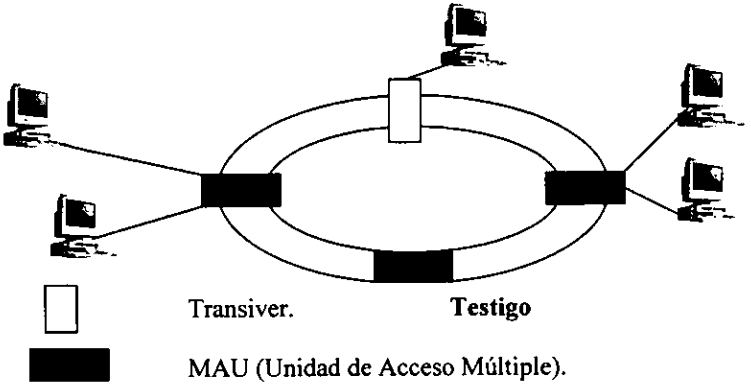


Fig. 3.2 Topología anillo.

En este tipo de redes, la información viaja en una sola dirección, presentando una desventaja fundamental: ya que como cada estación de trabajo repite activamente todos los mensajes, si una de las estaciones falla se rompe el anillo, ocasionando que toda la red se detenga ó se "caiga". Sin embargo, se han hecho algunas implementaciones en las tarjetas de red para solucionar este problema. Hoy en día, gracias a estas innovaciones y mejoras en las tarjetas, la falla de una estación no significa la caída total de la red. Arcnet y Token Ring son una muestra del uso de la topología de anillo.

Ventajas

- Si el cable de un dispositivo falla no se afecta la integridad del anillo
- Igualdad de acceso a todos los dispositivos
- El desempeño de la red esta garantizado

Desventajas

- Un alto costo en el cableado y las conexiones, así como en el concentrador
- Si el concentrador falla el anillo se rompe

3.2.3. TOPOLOGIA ESTRELLA

Uno de los tipos más antiguos de topologías de redes es la estrella, la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico. De la misma manera que las llamadas telefónicas de un cliente a otro cliente se manejan mediante una estación central de comunicación todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones, conocido como concentrador de cableado, el cual controla el flujo de datos. Como se ilustra en la figura 3.3 , esta arquitectura facilita la adición de nuevas estaciones de trabajo a la LAN. Todo lo que se requiere es un cable que vaya del punto central de conexión (concentrador) a la tarjeta de interface de red de cada nueva microcomputadora.

Otra ventaja de la topología de estrella es que el administrador de la red puede asignar a ciertos nodos un status mayor que a otros. Por tanto, la computadora central tenderá a buscar las señales de estas estaciones de trabajo prioritarias antes de reconocer a otros nodos. Para redes que tengan algunos usuarios clave que requieran respuestas inmediatas a sus solicitudes en línea, esta topología de estrella puede ser de extrema utilidad.

Por último, una arquitectura de estrella hace posible contar con diagnósticos centralizados de todas las funciones de la red como todos los mensajes a través del concentrador central, es fácil de analizar todos los mensajes transmitidos por las estaciones de trabajo y producir informes que revelen los archivos que utiliza cada nodo.

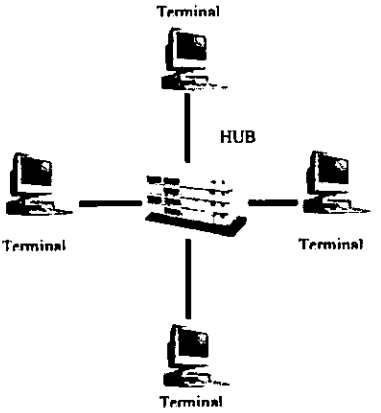


Fig. 3.3 Topología estrella.

La principal deficiencia de una arquitectura estrella es que si algo le sucede al concentrador central, falla la LAN completa. Esta es, precisamente, la misma deficiencia de los sistemas de minicomputadoras de usuarios múltiples, basados en un concentrador central.

3.2.4. TOPOLOGIA DE ARBOL

La topología de árbol también conocida como "Estrella Distribuida", es una extensión de la arquitectura en estrella, ya que se forma por la interconexión de varias topologías de ese tipo. Esto permite establecer una jerarquía, clasificando a las estaciones de trabajo en grupos y/o niveles según el nodo a que están conectados respecto a la distancia jerárquica con el nodo central o principal.

De características similares a las redes en forma de estrella, la falla de una estación de trabajo no afecta el funcionamiento de las otras; además usando concentradores o hubs, se reduce el número de líneas conectadas y la longitud del cableado de las estaciones hacia el servidor principal. De este modo, se aumenta la posibilidad de conectar un mayor número de estaciones desde distintos puntos de la red. Esto es ideal para armar redes donde se tengan estaciones de trabajo localizadas en dos ó más pisos de un edificio.

3.2.5. TOPOLOGIA DE MALLA

La topología de malla es una configuración totalmente distribuida donde cada estación de trabajo está conectada con cada una de las estaciones restantes. Esto permite múltiples facilidades de interconexión y de comunicación entre todas las estaciones. Es claro que las redes con topología malla son más grandes e importantes que cualquiera de otro tipo. El costo de estas redes es alto (mucho mayor si se le compara con la topología de bus y/o estrella), pero se compensa por su gran disponibilidad ya que con estas redes, se puede lograr el máximo aprovechamiento de las líneas de transmisión.

Entre mayor es el número de estaciones conectadas en topología de malla, mayor es el costo de la red, pero a cambio se tendrá una gran Confiabilidad ante las posibles fallas y frente a las futuras necesidades de reconfiguración. Esta topología puede soportar tráfico elevado de datos con retardos mínimos de tiempo, debido a que se tienen varias rutas para el flujo de la información.

3.3. TECNOLOGIAS DE CABLEADO EN REDES DE AREA LOCAL

El cableado en las redes locales se refiere al medio físico usado para interconectar entre sí las estaciones de trabajo de los usuarios con otros dispositivos o nodos de red, creando de esta manera una red que pueda transportar información entre las mismas.

La elección de un tipo de cableado a utilizar depende de varios factores a considerar como:

a) Tipo de ambiente donde se va a instalar.
b) Tipo de equipo a conectar.
c) Tipo de aplicación y requerimientos.
d) Capacidad económica (relación "costo/beneficio" esperada).

En el mercado se pueden encontrar tres tipos de cables que se usan para instalar redes locales:

- Par Trenzado.
- Cable Coaxial.
- Fibra Optica.

3.3.1. EL CABLE DE PAR TRENZADO

El par trenzado (ó cable tipo telefónico) es el más común y más usado de todos. Se forma por dos alambres de cobre en el interior que se encuentran forrados por una cubierta plástica de diferente color y torcidos uno contra el otro, que a su vez se encuentran protegidos por una cubierta aislante de plástico en la capa exterior. Esta es la característica principal que los distingue con el nombre de "Twister Pair" (Par Trenzado). La forma trenzada de este tipo de cable sirve para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor y evita la inducción de campos electromagnéticos. Fig. 3.4

Fig. 3.4 Cable UTP Nivel 5

En general, el cable de par trenzado viene en conjuntos típicos comerciales de 2, 3, 4, 6, 12, 16, 25, 50, 100 y hasta de 300 pares de cables. Sin embargo, aunque para redes locales sólo se necesiten dos pares de cable para conectar una estación de trabajo a la red, la norma establece que se deben conectar cuatro pares tanto el conector (plug) como en la roseta de salida de datos. Por esta razón, en redes de área local se utiliza casi siempre el cable de par trenzado de 4 y 25 pares, cuando se usa esta tecnología.

Existen tres tipos distintos de cables dentro de la clasificación de par trenzado para redes de computadoras, éstos cables son conocidos como UTP, FTP y STP. El cable UTP (Unshielded Twister Pair: Par Trenzado sin Blindaje) tiene los conductores de cobre trenzados más delgados y menos protegidos por la cubierta plástica exterior si se compara con el cable STP, pero además una diferencia notoria radica en el hecho de que los cables UTP no están protegidos por una cubierta metálica que se encuentra entre los pares trenzados y la cubierta plástica exterior como en los cables STP y que sirve para eliminar y/o reducir la interferencia que pueden generar otras señales.

Los cables UTP se pueden encontrar en cinco Categorías diferentes, donde cada Categoría tiene características físicas y eléctricas propias. Además estos cables son muy económicos, flexibles y permiten manipular una señal a una distancia máxima de 110 metros sin el uso de repetidores.

- CATEGORIA 1 Y 2. Diseñados para voz y transmisiones lentas de hasta 1 Mbps., ninguna de estas categorías es apropiada para red de datos.
- CATEGORIA 3. Diseñado para transmisiones de datos de hasta 10 Mbp; por lo general se usa para redes Ethernet.
- CATEGORIA 4. Diseñado para transmisiones de datos de hasta 16 Mbps; por lo general se usa para redes Token Ring.
- CATEGORIA 5. Diseñado para transmisiones de datos de hasta 100 Mbps; se encuentra en redes de alta velocidad como Fast Ethernet.
- Niveles 6 y 7. Propuesta de la empresa Anixter para tener cable de par trenzado para la transmisión de 1 Gbps; la cuál estaría empleada en redes como Gigabit Ethernet y ATM.

NOTA:
Los otros aspectos del cableado como la longitud, la topología, los esquemas de cableado y los requisitos de interfaz para conexiones, están reglamentados por la Norma EIA/TIA568.

Por otro lado, los cables de conductores trenzados más gruesos y forrados por una cubierta metálica, además de estar cubiertos por una capa aislante en el exterior se les conoce como STP (Shielded Twister Pair: Par Trenzado Blindado). Los cables STP son más caros y menos flexibles que los UTP, pero permiten un rango de operación de hasta 500 metros sin el uso de repetidores como es el caso de las instalaciones de redes tipo Token Ring STP de 4 ó 16 Mbps.

Así como el cable UTP se puede encontrar en cinco Categorías, el cable STP puede hallársele en cuatro "Tipos" diferentes conocidos como: Tipo 1, Tipo 2, Tipo 3 y Tipo 4.

El cable FTP (Foiled Twisted Pair: Pares Trenzados Envueltos por una Lámina), realmente son cables UTP envueltos por una lámina metálica, generalmente de aluminio la cual reduce las emisiones al exterior del propio cable y lo proteje de las interferencias que le pudieran inducir por radiaciones, pretendiendo con esto mejorar su EMC (Compatibilidad Electromagnética) y su EMI (Interferencias por Emisiones Electromagnéticas).

Es importante mencionar que sí es posible transmitir audio y vídeo en cable UTP Categoría 5 si se realiza COMPRESION DE DATOS en el vídeo. También debemos destacar que si con el cable UTP Categoría 5 se puede alcanzar una velocidad de 100 Mbps, con el cable STP-A se pueden alcanzar velocidades de transmisión de hasta 550 Mbps.

La diferencia entre el UTP categoría 5 y el STP-A radica en que el primero no es blindado y el segundo si lo es, por lo que la transmisión de información es mas confiable. Dentro de las características del STP-A se tienen las siguientes:

- Todos los componentes son probados para un funcionamiento eléctrico de hasta 300 MHz.
- El ancho de banda de 600 MHz acomoda aplicaciones de multimedia (simultáneamente vídeo y datos).
- Acomoda aplicaciones para datos superiores a 100 Mbps.

3.3.2. EL CABLE COAXIAL

El cable coaxial se compone de un alambre de Cobre duro en su parte central que constituye el núcleo, este núcleo se encuentra cubierto por un material aislante de plástico (Fig. 3.5). Este material aislante a su vez, está rodeado por una malla metálica conductora de tejido trenzado y finalmente, todo el conjunto está protegido por una cubierta plástica exterior también aislante, que pueden transportar una señal eléctrica a mayor distancia entre más grueso es el conductor. En redes locales se utilizan dos tipos de cable coaxial, el RG-58/U de 50 Ohms (10Base2), conocido como cable coaxial delgado y que puede alcanzar una distancia de 185 metros sin el uso de repetidores) y el RG-68/U (10Base5), también de 50 Ohms llamado cable coaxial grueso que puede alcanzar una distancia de hasta 500 metros sin uso de repetidores. El cable coaxial grueso es más caro y menos flexible. Por tal razón cuando tiene que colocarse en instalaciones donde ya existen ductos para cableado ó tuberías con espacio reducido, y sobre todo, limitado en las esquinas o dobleces, resulta más conveniente utilizar el cable coaxial delgado debido a que las nuevas instalaciones de ductos para cableado, por lo general, son muy costosas. Este es un factor importante en la implantación de una red local.

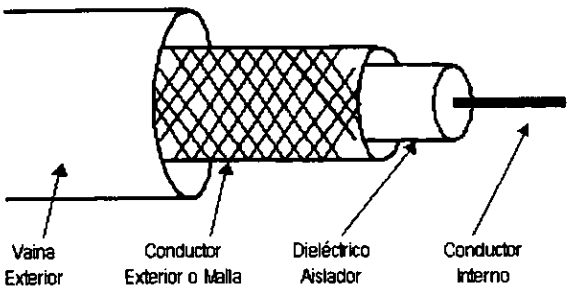


Fig. 3.5 Estructura Cable Coaxial.

La construcción del cable coaxial produce una buena combinación de un gran ancho de banda con una muy buena inmunidad al ruido. Los cables coaxiales se han empleado con mucha frecuencia en redes de área local.

En general, la alternativa de colocar cable coaxial en redes locales tiene una relación de costo/beneficio muy buena; aunque cada día su uso disminuye por que ahora se prefiere el cable de par trenzado por su menor costo y facilidad de instalación sobre todo.

Se pueden citar como características propias de los cables coaxiales las siguientes:

- Es una tecnología muy conocida y altamente comercial.
- Compatibilidad con Ethernet y Arcnet. Ancho de banda de 10 Mbps. Muy buena tolerancia a interferencias debidas a factores ambientales.
- Muy buena protección física del cable por su construcción ante esfuerzos mecánicos.
- Es un medio "pasivo" donde la energía es provista por las estaciones de trabajo del usuario a través de las tarjetas de red.
- Uso de conectores especiales para la conexión física de las estaciones de trabajo de una red (conector BNC en forma de "T").
- Generalmente usado con topología de bus lineal.
- Bajo costo y simple de derivar. Gran inmunidad al ruido.
- Buena Confiabilidad aunque limitada.

3.3.3. FIBRA OPTICA

La fibra óptica es la tercera tecnología de cables que se utiliza para instalar redes locales. El cable de fibra óptica se elabora de dos tipos de vidrio sometidos a alta pureza y con diferente índice de refracción, uno para la parte interior y otro para la parte exterior del cable. Esta diferencia en los índices de refracción en la fibra, sirve para que cuando un rayo de luz (información) entre por uno de los extremos del cable no se disipe hacia el exterior, logrando que pueda salir por el otro extremo.

Los rayos de luz pueden entrar a la fibra óptica si el rayo se halla contenido dentro de un cierto ángulo denominado CONO DE ACEPTACIÓN. Un rayo de luz puede perfectamente no ser transportado por la fibra óptica si no cumple con el requisito del cono de aceptación. El cono de aceptación está directamente asociado a los materiales con los cuales la fibra óptica ha sido construida. La Fig. 3.6 ilustra todo lo dicho. Respecto a atenuaciones producidas dentro de otros medios de transmisión, la fibra óptica presenta niveles de atenuación realmente bajos que permiten transmitir luz por varios kilómetros sin necesidad de reconstruir la señal (regenerar).

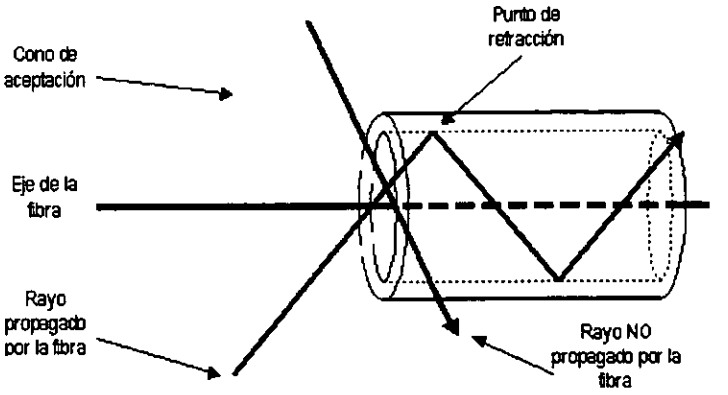


Fig. 3.6 Cono de aceptación en Fibras Ópticas.

La fibra óptica, a su vez, se encuentra cubierta con una capa de silicón, luego tiene una cubierta de amortiguamiento que la protege de la humedad, después se forra con una capa llamada: miembro de esfuerzo a tensión, la cuál permite ser jalada a través de los ductos y finalmente se cubre todo lo anterior con una capa de protección aislante en la parte exterior, Fig. 3.7. Sin embargo, es extremadamente flexible ya que se pueden realizar giros de hasta 360 grados sin problemas de afectar ó trozar el cable.

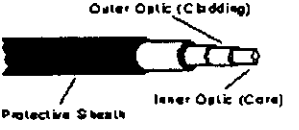


Fig. 3.7 Fibra Óptica.

El diámetro de la fibra interior usada para redes de área local es de 62.5 micras y el de la fibra exterior es de 125 micras. Comúnmente la fibra óptica presenta una atenuación máxima de 4 dB/Km. Las distancias máximas obtenidas para redes locales son de 2 Km. de nodo a nodo sin el uso de repetidores.

El cable de fibra óptica se emplea normalmente por tres razones básicas:

a) Para aquellos casos en donde las grandes distancias son un factor considerable en la implantación de una red local.

b) Cuando es necesaria una alta capacidad de comunicaciones y donde se requiera de un gran ancho de banda, como es el caso de los "Backbone".

c) Cuando el ruido, medio ambiente ó cualquier tipo de interferencia son factores importantes a considerar.

Se conoce que un sistema de transmisión óptico tiene tres componentes: el medio de transmisión, la fuente de luz y el detector. Para el caso de redes con fibra óptica el medio de transmisión es una fibra ultradelgada de vidrio (Dióxido de Silicio a la alta pureza); la fuente de luz bien puede ser un diodo LED (Diodo Emisor de Luz) o un diodo láser, cualquiera de los dos tipos de diodos emiten pulsos de luz cuando se aplica un voltaje en sus terminales. El detector es un fotodiodo que genera un pulso eléctrico en el momento de recibir un rayo de luz. Al colocar un LED o un diodo láser en el extremo de una fibra óptica y un fotodiodo en el otro extremo, se tiene una transmisión de información unidireccional que acepta una señal eléctrica, la convierte y la transmite por medio de pulsos de luz y, después, la reconvierte en una señal eléctrica en el extremo receptor.

Para la transmisión de la información en redes locales vía fibra óptica, se utiliza una fibra como transmisor y otra como receptor. Por esta razón, generalmente se fabrican en conjuntos de mínimo dos fibras por cable.

Ahora listamos algunas de sus características y ventajas principales:

- La fibra óptica consiste en un núcleo central muy fino y delgado de vidrio que tiene un alto índice de refracción a la luz.
- Este núcleo es rodeado por otro medio que tiene un índice de refracción más bajo, que lo aisla del ambiente y evita que la luz transmitida salga hacia el exterior.
- Físicamente la fibra es muy fina, liviana, durable y por lo tanto instalable en muy poco espacio. Sin embargo, todavía es cara.
- Cada fibra proveé, un camino de transmisión único de extremo a extremo en forma unidireccional. Es decir la transmisión es de punto a punto entre los dos extremos de la fibra.

Son pulsos de luz los que se introducen en un extremo, usando un diodo láser o LED. La reflexión de los pulsos dentro de la fibra es la forma de transmisión de los datos. Se pueden transmitir voz, datos y vídeo simultáneamente y en tiempo real. Se usa para aplicaciones de alta velocidad y alta capacidad de tráfico.

- No genera señales eléctricas o magnéticas, ni interferencias.
- La fibra óptica no es afectada por interferencia eléctrica, ruidos, temperatura. radiación o agentes químicos.
- Tiene una excelente tolerancia a factores ambientales.
- El ancho de banda es mucho más alto que con cualquier otro medio, alrededor de los Gbps.
- La fibra óptica es altamente confiable, es difícil de derivar y se tiene muy poca pérdida de señal.

- Alcance de 2 kilómetros sin uso de repetidores.
- Requiere de un mantenimiento sólo realizable por personal entrenado.
- Compatibilidad con Ethernet, Token Ring y FDDI (Fiber Data Distributed Interface: Interface de Datos Distribuidos por Fibra).
- Ofrece la mayor capacidad de adaptación a nuevas normas de rendimiento y a otro tipo de tecnologías .

NOTA: Es conveniente recordar que FDDI es un estándar de transmisión a 100 Mbps mediante fibra óptica que se ajusta a cualquier arquitectura de RED.

CONSIDERACIONES IMPORTANTES DE LA FIBRA OPTICA

La fibra óptica que se utiliza en redes locales, es sumamente delgada, ligera, fuerte y flexible. Puede jalarse como si fuera cualquier otro cable y debido a su ligereza, es muy posible que pueda meterse en ductos ya demasiado llenos que no pueden admitir el diametro ni el peso del cable coaxial. Esto es de gran ayuda cuando la única alternativa que se tiene es hacerle espacio en un ducto donde se tenga un gran número de cables.

Un punto negativo de las fibras ópticas radica en el hecho de que el equipo necesario para instalar fibra óptica es caro y se requiere de entrenamiento para su buen uso. El empalme ó unión de dos ó más fibras no es tan sencillo, y menos lo es su derivación. Este último aspecto puede ser visto como una ventaja: la seguridad de la información es excelente. Las fibras ópticas son unidireccionales y el costo de las tarjetas de red y demás equipo, es mucho mayor que sus equivalentes de tipo eléctrico. Las ventajas que ofrecen las fibras ópticas son muchas, que se está invirtiendo tiempo y dinero por parte de los fabricantes para mejorar su tecnología y reducir su costo.

Las fibras ópticas proporcionan un ancho de banda extremadamente grande y tienen una pérdida en señal muy pequeña, razón suficiente por la que se emplean para distancias muy largas entre repetidores. Las fibras no se ven afectadas por variaciones de voltaje y corriente en líneas de potencia, por interferencia electromagnética o por químicos corrosivos dispersos en el aire; de tal forma, que pueden emplearse en ambientes industriales expuestos a condiciones muy severás en las que, el par trenzado o cable coaxial serían totalmente inadecuados. Las fibras no son conductoras, y por lo tanto, no transmitirán descargas eléctricas a los servidores o equipo de red.

Otra ventaja inherente a la fibra es que se adapta igualmente a todos los estándares y velocidades de red.

Por otra parte, la ventaja de la fibra óptica en cuanto a su velocidad mayor de transmisión, no se utiliza hoy en día por los dispositivos con los que actualmente se cuenta. Por ejemplo, si se instala fibra óptica en una red Token Ring, la velocidad a transmitir sigue siendo 4 ó16 Mbps, y no a 100 ó 200 Mbps que son velocidades a las que puede transmitir la fibra óptica fácilmente. Existen tarjetas de red de fibra óptica para FDDI que se han diseñado para Token Ring, Ethernet y un gran número de tecnologías. Incluso la FDDI (de 100 Mbps) no se acerca a la capacidad de ancho de banda que la fibra otorga.

3.4. ESTANDARES "IEEE" PARA LOS DIFERENTES TIPOS DE CABLE

En el estándar IEEE 802 están definidos los siguientes tipos de cableados y sus limitaciones. Este documento se presenta a continuación de manera resumida.

10 Base T: Par trenzado UTP

Se refiere al Ethernet de 10 Mbps basado en par trenzado de categoría 3 o mayor, permite disminuir la carga de tráfico en la red por medio de concentradores. La longitud máxima de un segmento es de 110 metros entre sus extremos. Por medio de un concentrador, se pueden tener en topología estrella desde 8 hasta 208 estaciones. Originalmente fue pensado para aprovechar el tendido telefónico existente.

10 Base 2: Cable Coaxial Delgado

Es de los cables más usados en México, construye una topología de bus lineal con una longitud máxima de cableado de 185 metros por segmento. Su armado se realiza con conectores "BNC" tipo "T" para cable coaxial de 50 Ohms, el cuál se conecta en cada tarjeta de red, además se requiere de un par de "terminadores" de 50 Ohms que se conectan uno en cada extremo de la red.

10 Base 5: Cable Coaxial Grueso

Es el cableado estándar de Ethernet en topología bus, con longitud máxima de 500 metros por segmento, requiere un "transceiver" (adaptador-emisor) entre la computadora y el cableado de la red. Soporta hasta 100 estaciones por segmento. Casi todas las tarjetas de red tienen soporte para este tipo de cable a través del puerto AUI de la tarjeta (el puerto AUI es un conector de tipo DB-15).

Características del cable coaxial grueso (cable thick).

- Distancia por segmento de 500 metros como máximo (1,650 pies)
- Puede tener hasta 100 nodos por segmento.
- Soporta hasta 4 repetidores, alcanzando una distancia de hasta 2,500 metros (8,250 pies).
- Mínima distancia de 2.5 metros entre "derivaciones" para nodos.
- Las "derivaciones" hacia las estaciones de trabajo se hacen con conectores tipo "n" o con conectores tipo "vampiro".
- La conexión de la estación al "bus" se hace por el puerto "aui" a traves de "transceivers".
- Máxima distancia de 50 metros del "bus" a la estación de trabajo.
- Se requiere de un terminador de 50 Ohms en cada extremo del cable.

10 Base F (Fibra Optica).

Se instala en configuración estrella y/o anillo con una longitud máxima de 2,000 metros por segmento sin el uso de repetidores, generalmente requiere de concentradores y conectores especiales caros todavía; el ancho de banda que proporciona esta tecnología es muy amplio y permite la transmisión de voz, datos y vídeo sin ningún problema, inclusive el ancho de banda queda sobrado para futuras aplicaciones. Es prácticamente inmune al ruido y se necesita personal capacitado para su instalación.

La fibra multimodo puede alcanzar distancias 1 a 3 Km., debido a sus características técnicas. Este tipo de material se usa como columna vertical entre edificios o departamentos. Pensando en el futuro, puede ser usado en la mayoría de las tecnologías.

100 Base T (Fast Ethernet)

100 Base T es el heredero de 10 Base T. El estandar IEEE que lo define es el IEEE 802.3u, mantiene el mismo acceso al medio CSMA/CD y la mayoría de las reglas de cableado tradicional de 10 Base T. Una de las características principales de 100 Base T es que puede ser usado a 10 o 100 Mbps. Existen tres diferentes medios de transmisión para implementar una red 100 Base T.

100 Base TX

Es la especificación para ejecutar Ethernet a 100 Mbps, sobre un cable de par trenzado sin blindar (UTP) de doble par y cable de par trenzado blindado (STP) de tipo de doble par. La especificación 100 Base TX esta descrita para conectar RJ45 y DB9. Proporciona señalización de 125 MHz sobre cada par de cable, que sólo puede proporcionar un 80 % de la tasa de productividad debido a su esquema de codificación llamado 485B. La configuración de los conectores RJ45 para 100 Base TX es idéntica al de 10 Base T, transmitiendo a través de los cables 1 y 2 y recibiendo a través de los cables 3 y 6.

100 Base T4

Es la especificación para ejecutar Ethernet a 100 Mbps, a través de un cable UTP de categorías 3, 4 ó 5 de cuatro pares. Proporciona señalización de 25 MHz sobre tres pares con un 133 % de tasa de productividad como resultado de un esquema de codificación llamado 8B6T.

100 Base FX

Es la especificación de capa física Ethernet a 100 Mbps para cableado de fibra óptica 62.5/125 micras de dos hilos. Admite los conectores estándar MIC, ST o SC, la señalización para 100 Base FX utiliza el esquema de codificación 4B5B, que proporciona un 80 % de salida total. Por lo tanto, la señalización es de 125 MHz a través de un solo hilo.

GIGABIT ETHERNET

Es una extensión del estándar IEEE 802.3 o Ethernet 10/100 Mbps y conserva el mismo protocolo de acceso al medio (MAC; Media –Access Control); CSMA/CD (Acceso Múltiple con Detección de Portadora y Detección de Colisiones) y es conocido también como el estándar IEEE 802.3z.

La arquitectura básica de la tecnología Gigabit Ethernet es a través de canales de fibra óptica y esquemas de codificación 8B/10B, los cuales son utilizados para señalización de los datos.

Al operar en modo full-duplex, el trabajo de Gigabit Ethernet será exactamente igual al de Fast Ethernet, sólo que más rápido de 100 a 1000 Mbps. Pero al operar en modo half-duplex, se afectará el trabajo de Gigabit Ethernbet, adicionando al protocolo CSMA/CD dos nuevas características: una es con la extensión de la portadora (carrier) de la señal y la otra es una modificación al paquete de datos.

3.5. EVOLUCION DE LOS SISTEMAS DE CABLEADO

Los sistemas de cableado para servicios de Telecomunicaciones han experimentado una constante evolución con el correr de los años. Hace una década, las "redes" de cableado que se instalaban en los edificios se hacían con cable tipo telefónico que era instalado por las compañías de teléfonos. Este conjunto de cables era capaz de manejar las comunicaciones de voz, pero para poder apoyar las comunicaciones de datos, se tenía que instalar un segundo sistema privado de cables. Los sistemas de cableado para teléfonos fueron en su oportunidad especificados e instalados por las compañías de teléfonos; mientras que el cableado para datos estaba determinado por los proveedores del equipo de cómputo (es lo que se conoce como cableados propietarios). Desde entonces el cableado de los edificios ha evolucionado de sistemas propietarios específicos de un fabricante a sistemas abiertos de cableado estructurado que cumplan con las Normas, y que se puedan adaptar a los requerimientos de voz, datos y vídeo que sean necesarios.

3.6. EL SISTEMA DE CABLEADO ESTRUCTURADO

En el clima actual de los negocios, el tener un sistema confiable de cableado para comunicaciones es tan importante como tener un suministro de energía eléctrica en el que se pueda confiar. En el mundo de hoy, el poder proveer de comunicaciones de voz y de datos por medio de un sistema de cableado estructurado "universal" es requisito básico e imprescindible de los negocios. Estos sistemas de cableado estructurado proveen la plataforma o base sobre la que se puede construir una estrategia general para los sistemas de información.

Se puede definir a un sistema de cableado estructurado como un conjunto de cables y accesorios que dotan a un edificio o construcción, con una infraestructura flexible de comunicaciones que permite el montaje posterior de servicios de información,

independientemente de su tecnología específica; es decir, que puede aceptar y soportar sistemas de cómputo y de teléfono múltiples, sin importar quién fabricó los componentes del mismo. Las ventajas reales de este sistema, es que además de contar con una buena infraestructura de cableado para más de 10 años, es que se puede conectar donde antes pudo haber estado una computadora, una extensión telefónica ó viceversa, mediante unos cambios simples que no requieren de un experto en comunicaciones o informática.

En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella y/o de árbol, facilitando la interconexión y la administración del sistema. Esta disposición permite la comunicación con prácticamente cualquier dispositivo, en cualquier lugar y en cualquier momento. El cableado estructurado está compuesto por distintos módulos o subsistemas que se instalan bajo una jerarquía física determinada. Sólo aquellos subsistemas que se requieran para dar conectividad y servicios a un lugar específico y en un momento determinado, son activados; mientras que el resto del cableado permanece inactivo hasta que surjan las nuevas necesidades. Fig. 3.8.

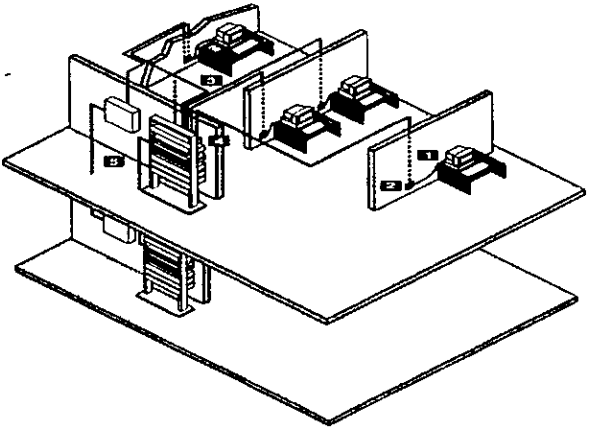


Fig. 3.8 Cableado Estrcuturado.

El sistema de cableado estructurado debe regirse por un conjunto de recomendaciones que son:

- MODULARIDAD. Debe ser diseñado para crecimiento a futuro, es decir que tenga capacidad para incorporar nuevos o posibles incrementos de usuarios a la red de distribución ya existente, así como la posibilidad de modificar la distribución interna.

- INTEGRADOR DE SERVICIOS. Deberá facilitar el intercambio de información entre los recursos disponibles: teléfonos, telefax, LAN's, sistemas de audio y vídeo, seguridad, etc.

- SENCILLO DE ADMINISTRAR. La numeración deberá ser estándar.

- DISEÑO. Permite maximizar la productividad con una inversión mínima, es decir pueden hacerse cambios de manera local y no afectarán a todo el sistema, además de que se maneja el mismo tipo de cable, el mismo hardware en puntos de administración , etc.

- CONFIABLE. En caso de fallas se tienen trayectorias de respaldo, las cuales a su vez cuentan con capacidad de crecimiento.

Se deberán tomar en cuenta otras consideraciones para lograr un sistema de cableado bien diseñado, por ejemplo los estándares industriales para longitud máxima de un segmento de cable y el número máximo de estaciones de trabajo o ramas, la conexión apropiada a tierra de los equipos, la susceptibilidad a la interferencia y el manejo general del cable.

En términos generales, el Cableado Estructurado se compone de 5 subsistemas que son los siguientes:

1) Cables de Parcheo.
2) Salidas de Información.
3) Cable Horizontal.
4) Productos para Interconexión.
5) Cable Principal o "Backbone".

El resultado final que se debe obtener de sistema de un cableado estructurado es que sea flexible, controlable, económico y, al mismo tiempo, capaz de satisfacer las necesidades actuales y futuras. El cableado estructurado debe ser "abierto" y capaz de dar soporte a todos los ambientes físicos, las aplicaciones y los requerimientos de rendimiento deseados.

Capítulo IV

IMPLEMENTACION DE LA INTRANET

IMPLEMENTACION DE LA INTRANET

4.1. ANTECEDENTES

Las Intranets nacieron, como Internet, de la voluntad de las empresas usuarias. El término aparece en la prensa en 1995. Sin embargo, números organizaciones utilizaban ya varios años antes las tecnologías de Internets para necesidades internas.

Internet se define como un conjunto de redes, redes de ordenadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. También Internet es conocida como la "red de redes", lo que se quiere decir con esto es que Internet esta conformado por millones de redes en todo el mundo, las cuales se comunican entre ellas a través de un protocolo denominado TCP/IP.

Intranet se define como una red privada de ordenadores desarrollada con tecnologías de Internet tales como el navegador o el gestor de correo electrónico, a la vez que utiliza los mismos protocolos y estándares abiertos que permiten que ordenadores de diferentes tipos se puedan comunicar entre ellos, como base para el desarrollo de los sistemas de gestión de una empresa. Fig. 4.0

Fig. 4.0 Intranet

La primera razón que llevó a estas empresas a utilizar de modo interno las tecnologías de Internet es el acceso fácil a las aplicaciones. En efecto, muchas de ellas se pueden descargar directamente desde la red. Provienen del ámbito público o están disponibles en forma de versión de demostración. Las funcionalidades pueden evaluarse así rápidamente con un menor costo. Los que aún no han descubierto esta mina que representa Internet se sorprenderán por sus aplicaciones sorprendentes y a precios a menudo muy atractivos. La explicación económica es relativamente simple: al utilizar la

red como canal de distribución y de venta, los editores de programas eliminan los costos intermedios, en particular los de distribución.

Muchas empresas han descubierto así la aproximación de la Intranet descargando un servicio Web del ámbito público, instalando y generalizando poco a poco su utilización en el interior de la empresa. Esta primera ola se vio reflejada por una simple frustración de no estar conectado completamente a Internet.

Los editores de aplicaciones, por el contrario, han amplificado notablemente "el movimiento Intranet". Han hecho de él un fenómeno de moda como ocurre con la informática regularmente. Aun con el riesgo de estropear el término y hacer desconfiados a los usuarios. Cada editor de programas tiene su "suite" Intranet: Netscape, sin duda, pero también Sun, Oracle, Microsoft, SCO, Novell, IBM, Digital, Apple. Una de las razones del rápido incremento en el número de Intranets es debido a que cualquier organización que posea una red ya tiene la infraestructura necesaria para desarrollar una Intranet. Esto hace que las Intranets tengan un costo efectivo y que contribuyan a incrementar las comunicaciones dentro de la empresa de una forma muy sencilla.

Entre sus múltiples ventajas se encuentran:

- Interoperabilidad. Se tiene acceso a todos los servicios de Internet, pero restringidos al uso interno de la empresa y a todos los productos de la red.

- Escalabilidad. Se puede dar acceso fácilmente a nuevos usuarios de la empresa a dichos servicios sin molestias para los que ya la están utilizando.

- Seguridad. Se produce una gran mejora en la seguridad de la red local al evitar el acceso de usuarios no autorizados a nuestros servicios Internet.

- Disminución de los Costos. Permite una disminución de los costos de correo, papel, y de la factura telefónica al simplificar las comunicaciones internas y el intercambio de información.

- Aumento de la Efectividad. Si está bien diseñada permite una mejora de la efectividad al tener acceso de forma sencilla a una serie de servicios que simplifican el servicio y mejoran el tiempo de acceso a la información.

4.2. INSTALACIÓN DEL SERVIDOR

Deberá estar formateado el disco duro previamente, conteniendo el sistema operativo MS/DOS, así como correctamente instalada la unidad de CD-ROM.

WINDOWS NT SERVER 4 se presenta en un CD, pero puede llevar además tres discos. Con dichos discos se llevan a cabo los primeros pasos de la instalación y se inicia Windows

NT Server. Posteriormente se transferirán los archivos del sistema al disco duro del servidor.

Para proceder a su instalación puede hacerlo de dos maneras distintas.

1. Si dispone de discos de inicio de Windows NT, inserte el disco de inicio de instalación de Windows NT Server en la unidad A: inserte el CD en su unidad y conecte la computadora para iniciar la instalación.

Después, cuando se le indique, introduzca el Disco No. 2 de instalación de Windows NT Server y pulse enter.

2. Si no dispone de discos para iniciar Windows NT, introduzca el CD en su unidad y colóquese en el directorio **D:\I386** si va a realizar la instalación en una computadora con un procesador Intel, (si la controladora del CD-ROM es de tipo SCSI no tendrá ningún problema, pero si es IDE, es posible que deba copiar los archivos y subdirectorios de dicho directorio al disco duro del servidor e indicarlo posteriormente con los parámetros adecuados).

El comando a utilizar es **WINNT.EXE** (en caso de realizar una actualización desde una versión anterior de Windows NT, deberá utilizar **WINNT32**).

Una vez escrito el comando y pulsado **[Enter]**, le pedirá el nombre de la ruta de acceso donde se encuentran los archivos de WINDOWS NT Server (le indica por defecto, **D:\I386**). Modifíquelo e indique la ruta correspondiente (si esta instalado desde un disco duro temporal) o admita la indicada por defecto y pulse **[Enter]**.

Le pedirá que le introduzca tres discos de alta densidad previamente formateados para que los genere.

Introduzca el primero y pulse **[Enter]** para que genere el Disco No. 3 de instalación de Windows NT Server.

Después, introduzca el segundo y pulse **[Enter]**, para que genere el Disco No. 2 de instalación de Windows NT Server.

Posteriormente, introduzca el tercero y pulse **[Enter]** para que genere el disco etiquetado de Inicio de instalación de Windows NT Server.

Cuando haya finalizado de generar este último disco, procederá a copiar distintos archivos a un directorio temporal del disco duro.

Después de un tiempo mostrará un aviso indicando que ha acabado el proceso de la instalación basado en MS-DOS. Inserte el disco de inicio de instalación de Windows NT Server en la **unidad A:** y pulse **[Enter]** para reiniciar el equipo y continuar con la instalación.

Después, cuando se le indique, introduzca el **Disco No. 2** de instalación de Windows NT Server y pulse **[Enter]**.

En ambos métodos, mostrará una pantalla de bienvenida Windows NT Server. Puede escoger varias opciones: pulsar **[F1]** para ver distintas pantallas de ayuda sobre el proceso de instalación, **[R]** para proceder a reparar una instalación previa que estuviera dada, **[F3]** para salir sin instalar o **[Enter]** para continuar con el proceso.

Le mostrará una pantalla de aviso donde le indica que puede pulsar **[I]** para seleccionar manualmente los controladores **SCSI** o **[Enter]** para que intente la detección automática.

Cuando haya procedido al reconocimiento y carga de los controladores necesarios, le mostrará una pantalla desde donde podrá pulsar **[S]** para configurar otros controladores (incluyendo aquellos para lo que dispone de un disco de soporte de dispositivo distribuído por el fabricante) o **[Enter]** para continuar aceptando los controladores detectados.

Una vez pulsado **[Enter]** continuará el proceso y le mostrará el contrato de licencia de Windows NT Server. Pulse **[F8]** para indicar que acepta el contrato.

Le mostrará la configuración detectada para su equipo. Puede realizar correcciones moviéndose con las teclas de dirección, pulsar **[Enter]** y realizar los cambios oportunos.

Verá la lista de particiones existentes así como el espacio disponible para añadir otras. Puede eliminar la partición seleccionada pulsando [E] y crear una nueva partición en el espacio libre con **[C]** o **[Enter]** para instalar Windows NT Server en la partición seleccionada.

Ahora podrá indicar si desea convertir la partición al sistema de archivos **NTFS (NT File System)**, que es el sistema desarrollado para Windows NT que permite nombres de archivo de hasta doscientos cincuenta y seis caracteres, ordenación de directorios, atributos de acceso a archivos, reparto de unidades en varios discos duros, reflexión de discos duros y registro de actividades, o bien permanecer con el sistema **FAT (File Allocation System)** que cuenta con nombres de archivos de hasta ocho caracteres, mas tres caracteres de extensión y no reúne ninguna de las otras características indicadas anteriormente para el sistema **NTFS.**

Le mostrará un aviso indicando que no es conveniente convertir la partición al sistema **NTFS** si va a necesitar acceso para otros sistemas operativos como **MS-DOS, OS/2 o Windows 3.x.** Pulse **[C]** para convertir la partición.

Deberá indicar el directorio donde va a instalar los archivos, el programa de instalación presenta una pantalla especial si detecta en el equipo una versión de Windows 95, Windows 3.x o Windows NT 3x para que decida entre instalar en el directorio predeterminado o especificar uno nuevo. Pulse **[Enter]** para aceptar la ubicación por default **(C:\WINNT)** y le mostrará una pantalla de aviso donde le indicará que se va a proceder a un reconocimiento exhaustivo de su disco o de sus discos duros, Pulse **[Enter]** para aceptarlo.

Después de un momento le indicará que la primera fase de la instalación ha terminado Retire el disco de la **unidad A:** y pulse **[Enter]** para reiniciar el equipo y continuar con la segunda fase de la instalación.

Cuando se reinicie el equipo, se realizarán distintos chequeos y se procederá a realizar la conversión del sistema de archivos **FAT** al sistema **NTFS.** Al finalizar la conversión se volverá a reiniciar el equipo entrara a Windows NT Server para continuar con la instalación.

Le mostrará una pantalla desde donde le indicará las etapas que quedan hasta finalizar la instalación:

1. **Obtener información acerca de su equipo**

2. **Instalar la red de Windows NT**

3. **Finalizar la instalación**

Marque en el botón **Siguiente.**

En función del programa de instalación utilizado, es posible que le muestre una pantalla donde deberá elegir el tipo de instalación **(típica, portátil, compacta o personalizada).**

Cuando se le indique, escriba su nombre y el de su organización, vuelva a marcar el botón siguiente y escriba la clave de 10 dígitos que viene incorporada en la parte posterior de la caja del CD. Cuando lo haya hecho, marque **siguiente**

Indique el modo de licencia de cliente que desea: Por servidor y el número de sesiones concurrentes será el número de licencias de acceso que tiene contratadas.

Cuando lo haya indicado, marque siguiente e indique el nombre que va a dar al servidor y oprima **Siguiente.**

Indique el tipo de servidor que está instalando (controlador principal de dominio, controlador de reserva o servidor independiente).

Los dominios son un sistema que da la posibilidad de dividir redes extensas en redes parciales reducidas que simplifican el trabajo de administración. Comprenden un grupo de computadoras, usuarios y recursos de la red que cuentan con una base de datos de seguridad común.

Un controlador principal de dominio es una computadora que administra la base de seguridad de dicho dominio.

Un controlador de reserva es una segunda computadora que contiene una copia de la base de datos se seguridad del controlador principal de dominio.

Un servidor independiente es aquella computadora que va a actuar de servidor de archivos y aplicaciones de la red pero no va a administrar la base de datos de seguridad del dominio.

Indique ahora la contraseña del administrador del sistema (deberá escribirla dos veces por motivos de seguridad) marque **Siguiente**.

Indique que si desea crear un disco de emergencia (contendrá información de la configuración del hardware del servidor y deberá utilizarlo en caso de que se produzca un problema de corrupción) y vuelva a marcar **Siguiente**.

Si le muestra una pantalla preguntando si desea instalar los componentes más comunes o si muestra la lista de componentes para poder elegir, seleccione esta última opción y marque **Siguiente**.

De la lista de componentes de Windows NT, seleccione aquellos que desea instalar (si algún componente aparece en color gris significa que no se han seleccionado todos los accesorios de dicho componente. Marque detalles para ver cuales son y selecciónelos si lo desea).

Cuando haya finalizado, marque **Siguiente**.

Le volverá a mostrar la pantalla desde donde le indica las fases que quedaban hasta finalizar la instalación.

1. **Obtener información acerca de su equipo**
2. **Instalar la red de Windows NT**
3. **Finalizar la instalación**

Marque **Siguiente** para continuar con el proceso.

Indique ahora si el equipo va a participar o no en la red, si va a estar conectado con algún adaptador de red y si va a tener acceso remoto a ella.

Marque **Siguiente** y le pedirá que indique si instala Microsoft Internet Información Server, que le permitirá compartir información desde este servidor en su intranet o en Internet.

Vuelva a marcar **Siguiente** para aceptarlo y, en la pantalla donde deberán aparecer los adaptadores de red de que dispone, indique **Comenzar la búsqueda** para que localice el adaptador de red utilizado. Cuando lo haya encontrado, marque **Siguiente**.

Le mostrará los protocolos de red que se usarán en la red. Entre ellos se muestra **NetBEUI**, que deberá seleccionarlo si el servidor se va a comunicar con otros equipos de una red Microsoft que utilicen este producto (Windows para trabajo en grupo, Windows NT 3.x o LAN Manager 2.x). **Puede añadir mas protocolos marcando seleccionar de la lista.**

Marque **Siguiente** cuando haya finalizado.

Verá los servicios de red seleccionados se podrán añadir mas si marca seleccionar de la lista. Cuando haya acabado, marque **Siguiente**.

Vuelva a marcar **Siguiente** para que se instalen todos los componentes seleccionados y otros necesarios para el sistema.

En función de la tarjeta detectada le mostrará la interrupción **(IRQ)** y la dirección del puerto de E/S de la tarjeta de red indicada. Marque continuar para aceptar los valores o modifíquelos si no son los correctos.

Indique que **NO desea utilizar DHCP** para que pueda asignar una dirección IP de forma manual (si se utiliza DHCP se realizará la asignación de la dirección IP de forma automática).

Al cabo de un momento le pedirá que **indique la dirección IP** correspondiente, la **mascara de subred** y la **dirección IP del gateway** o puerta de enlace predeterminada. Cuando finalice, **marque Dirección DNS** e indique el nombre de dominio Internet para esta computadora en el apartado Dominio. Cuando lo haya hecho **marque Dirección Wins** e indique la dirección IP del servidor principal de WINS (WINS es la respuesta de Microsoft al servicio de nombres de dominio de Internet que posibilita la transmisión de los nombres de dominio de Windows a dicho servicio para evitar inconsistencias y duplicaciones). Cuando haya acabado, pulse **Aceptar**. Fig. 4.1.

Ahora podrá deshabilitiar los enlaces de red u organizar el orden en el que buscará información en la red. Marque **Siguiente** para continuar.

Vuelva a marcar **Siguiente** para iniciar la red y completar la instalación.

Indique el nombre del dominio en que actuará este controlador principal de dominio que será **cfemex.com**, en orden de búsqueda de servicio DNS agregue el IP del servidor, marque **Siguiente**.

Al cabo de un momento le volverá a mostrar la pantalla desde donde le indica las etapas que quedaban hasta finalizar la instalación:

1. **Obtener información acerca de su equipo.**

2. **Instalar la red de Windows NT.**

3. **Finalizar la instalación.**

Marque **Finalizar** y empezará a configurar el equipo ejecutar Windows NT.

Muestra ahora las opciones de instalación deseadas dándole varias marcadas por default. Marque **Aceptar** para continuar y le indicará que no existe el directorio

C:\WINNT\System32\inetsrv y le pedirá permiso para crearlo. Una vez concedido el permiso le mostrará otros directorios donde se van a instalar las opciones. Vuelva a marcar Aceptar y de permiso para crearlos.

Después de un tiempo de instalación, le indicará los controladores ODBC (biblioteca de vínculos dinámicos que una aplicación preparada puede utilizar para acceder a un determinado origen de datos). **Seleccione SQL Server y marque Aceptar**.

Le pedirá el adaptador de vídeo instalado en la computadora. Marque **Aceptar** e indique la paleta de colores y el tamaño del área del escritorio. Marque **Aceptar** para guardar la configuración que acaba de comprobar.

Cuando haya finalizado, vuelva a marcar **Aceptar** y empezará con el copiado de archivos. Cuando acabe, configurará la mensajería, creará los iconos, establecerá la seguridad con los archivos del sistema y guardará la configuración.

Prepare un disco y copiará los archivos de configuración. Cuando haya finalizado, borrará los archivos temporales y habrá acabado la instalación.

Retire el disco flexible y el disco compacto de la unidad de **CD-ROM** y elija **Reiniciar el equipo para entrar en Windows NT Server**.

Cuando finalice la carga del sistema, le pedirá que pulse conjuntamente las teclas **[Ctrl] + [Alt] + [Supr]** (ya esta activo el servidor y se pueden conectar los usuarios desde las estaciones de trabajo). Cuando haya pulsado las teclas, le pedirá el nombre del usuario, su contraseña y el dominio al que se va a conectar (para poder iniciar una sesión y administrar el servidor). Cuando lo haya escrito, marque **Aceptar** e iniciará la sesión. Le mostrará una pantalla de bienvenida, marque Cerrar y verá el escritorio de Windows NT Server 4

Marque el botón Inicio, que se encuentra en la parte inferior izquierda de la pantalla, seleccione **Apagar el equipo**, después, estando marcado **Cerrar sistema**. Marque Si y, cuando se le indique, ya puede apagar la computadora.

4.3. INSTALACIÓN DE TCP/IP EN EL SERVIDOR

En el caso de que no hubiera instalado **TCP/IP** durante el proceso de instalación de **Windows NT SERVER 4**, siga los pasos siguientes para proceder a su instalación y configuración:

1. Dentro del **menú Inicio**, seleccione **Configuración**, Después **Panel de control**, marque dos veces el botón izquierdo de ratón sobre el **Icono Red** y seleccione **Protocolos.**

2. Le mostrará la lista de los protocolos que tiene actualmente instalados.

3. Si no aparece **Protocolo TCP/IP**, marque **Agregar** y selecciónelo de la lista que le muestra (si le muestra un mensaje indicándole que se encuentra bloqueada la base de datos de servicios, deberá esperar a que se desbloquee para poder continuar).

4. Le preguntará si desea utilizar **DHCP**. Conteste **NO** indique la dirección donde se encuentra el CD con los archivos de la instalación de Windows NT y marque Continuar.

5. Cuando haya finalizado de copiar los archivos que necesita, verá que se encuentra en la **lista de los protocolos** que están instalados actualmente.

6. Marque **Cerrar** y procederá a establecer los enlaces.

7. Deberá indicar la dirección IP que desee dar al equipo, la mascara de subred y la dirección IP del Gateway o puerta de enlace predeterminada si dispone de una.

8. Cuando lo haya escrito, marque **Dirección DNS** e indique el dominio para este equipo en **TCP/IP**, el nombre de host debe corresponder con el que dió para identificar a este equipo, **Indique la dirección IP** del servidor DNS que va a utilizar, marcando **Agregar**, escribiéndola y marcando, de nuevo **Agregar**. Fig. 4.1

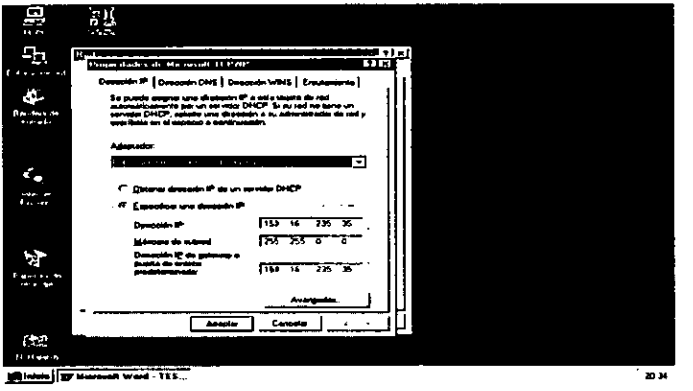


Fig. 4.1 Configuración de Dirección IP.

9. Marque **Aceptar**, si le muestra un mensaje diciendo que no ha indicado una dirección de WINS principal. **Marque SI** y volverá a la pantalla principal de **RED**. Marque **Aceptar** o **Cerrar** y ya estará configurado.

10. Deberá volver a iniciar el servidor para que entre en funcionamiento el nuevo protocolo.

4.4. CONFIGURACION Y ADMINISTRACION DEL SERVIDOR

La responsabilidad de configurar y administrar el servidor de la red corresponde al administrador.

Una vez instalado el sistema operativo, se ha de proceder a la configuración de la red teniendo que realizar, entre otros, los siguientes pasos:

- Desarrollar la estructura de directorios.
- Copiar los programas de aplicaciones y los datos.
- Dar de alta a los grupos y usuarios.
- Establecer la administración de seguridad.
- Localización de problemas.
- Establecer la seguridad del servidor.

4.4.1. DESARROLLO DE LA ESTRUCTURA DE DIRECTORIOS

Se puede emplear un número limitado de estructuras de directorios en un servidor y se debe estudiar cuidadosamente la que mejor se adapta a las necesidades de cada empresa.

Cuando se planea la disposición de los directorios, se deben considerar tres circunstancias importantes:

- La simplicidad de la estructura. No se debe hacer que la estructura de directorios sea tan complicada que los usuarios no puedan encontrar los programas ni los archivos de datos.
- La seguridad. Muchas de las previsiones de seguridad de un sistema operativo de red son relativas a los directorios y subdirectorios.
- La lógica. Los archivos deben estar agrupados lógicamente para aumentar la eficiencia de la red.

4.4.2. CREACION DE GRUPOS

Los usuarios de la red pueden agruparse para poder compartir los datos, concediendo a un grupo privilegios para un subdirectorio, los miembros del grupo pueden acceder a archivos compartidos que no están accesibles a otros usuarios de la red. Además se pueden dirigir

mensajes a todos los componentes de un grupo. La mayoría de las aplicaciones del correo electrónico también pueden enviar correo a todos los miembros de un grupo de la red.

Se suelen definir normalmente los grupos de dos formas: por la función o por el proyecto.

Un grupo funcional, incluye a todas las personas que realizan una tarea en particular.

Un grupo de proyecto esta compuesto por personas que trabajan en un proyecto particular.

El proceso de crear grupos consta de tres pasos básicos y se realizan con la utilidad Administrador de usuarios para dominios:

- Introducir el nombre del grupo.
- Definir las características del grupo que se esta añadiendo a la red.
- Añadir los usuarios (o miembros) del grupo.

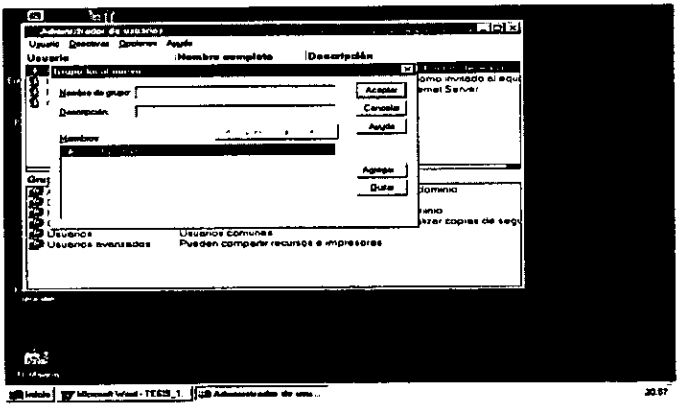


Fig. 4.2 Creación de Grupos.

4.4.3. CUENTAS DE GRUPOS GLOBALES

Estas cuentas están formadas únicamente por usuarios del dominio en el que se crearon y no pueden contener a otros grupos.

Sin embargo, se les pueden asignar privilegios en otros dominios que confían en aquel al que pertenece el grupo global, además de en su propio dominio.

Cuando una utilidad de Windows NT denomina a un grupo global, normalmente lo hace indicado, además del nombre, el dominio en el que se creo (por ejemplo CONTABILIDAD\GRUPO1).

4.4.4. CUENTAS DE GRUPOS LOCALES

Los grupos locales están formadas por usuarios y grupos globales.

Puede contener, además de usuarios y grupos globales de su propio dominio, a usuarios y grupos globales de otros dominios que confían en el dominio en donde se crearon.

Unicamente se les pueden asignar privilegios en el dominio en el que se crearon pero no en otros dominios distintos. Cuando se procedió con la instalación se crearon los grupos siguientes:

- Administradores.
- Administradores del dominio.
- Invitados.
- Operadores de impresión.
- Usuarios del dominio.
- Usuarios.

4.4.5. ADMINISTRADORES

Es una cuenta de grupo local que se crea tanto en dominios y servidores como en estaciones de trabajo Windows NT. Sus miembros tienen completa autoridad sobre el equipo o el dominio donde residen con la excepción de poder acceder a los archivos creados por el sistema de archivos NTFS (estos archivos solo pueden ser utilizados por la persona que los creo y ni siquiera un administrador puede acceder a ellos).

Pueden añadir estaciones al dominio, asignar derechos de usuario, crear y administrar grupos locales y globales, crear y administrar cuentas de usuario, formatear discos duros de servidores, mantener perfiles locales, auditar eventos, cerrar el servidor, saltarse el cierre del servidor, y compartir y dejar de compartir directorios e impresoras.

Si adiciona una cuenta de usuario a este grupo ya tiene todos los privilegios de administrador.

4.4.6. ADMINISTRADORES DEL DOMINIO

Es una cuenta de grupo global que se crea en cada dominio.

Los miembros de esta cuenta se adicionan automáticamente a la cuenta de grupo local de Administradores. Por tanto, todos los usuarios del grupo Administradores del dominio también lo son del grupo Administradores (si no desea que esto ocurra, deberá eliminar, uno a uno, a los usuarios que no quiera que tengan esos privilegios del grupo Administradores).

4.4.7. INVITADOS

Es una cuenta de grupo local que se crea tanto en dominios y servidores como en estaciones de trabajo Windows NT. Sus miembros pueden acceder como invitados al equipo o al dominio donde residen pero con unos privilegios limitados.

4.4.8. OPERADORES DE IMPRESIÓN

Es una cuenta de grupo local que se crea en cada dominio. Sus miembros pueden administrar impresoras del dominio, es decir, pueden compartir,detener la compartición y administrar las impresoras del dominio.

4.4.9. USUARIOS DEL DOMINIO

Es una cuenta de grupo local que se crea en cada dominio. Todas las cuentas de usuario de un dominio se incluyen en este grupo y, a su vez, se incluyen en el grupo de **Usuarios**.

4.4.10. USUARIOS

Es una cuenta de grupo local que se crea tanto en dominios y servidores como en estaciones de trabajo Windows NT. Casi todos los usuarios formarán parte de este grupo y, por ello, podrán acceder a los recursos de la red, pero no podrán conectarse al **PDC** y a los **BDCs** del dominio.

4.5. DEFINICIÓN DE USUARIOS DE LA RED

Existen dos tipos de usuarios: los globales y los locales.

4.5.1. CUENTAS DE USUARIOS GLOBALES

Estas cuentas se crean en el servidor y pueden ser usadas en los dominios en que se autoricen, además de en el que pertenezcan.

En ellas se pueden asignar privilegios de red, aunque es más común incluir las cuentas de usuarios en grupos para asignar privilegios al grupo, así se hace más sencillo modificar los privilegios de un número grande de usuarios. Normalmente a estas cuentas se les denomina **cuentas de usuario.** Fig. 4.3.

4.5.2. CUENTAS DE USUARIOS LOCALES

Estas cuentas se originan en una red que no corre con Windows NT y, por tanto, no pueden ser usadas fuera del dominio en el que se crearon. Sin embargo, pueden incluirse tanto en grupos globales como locales.

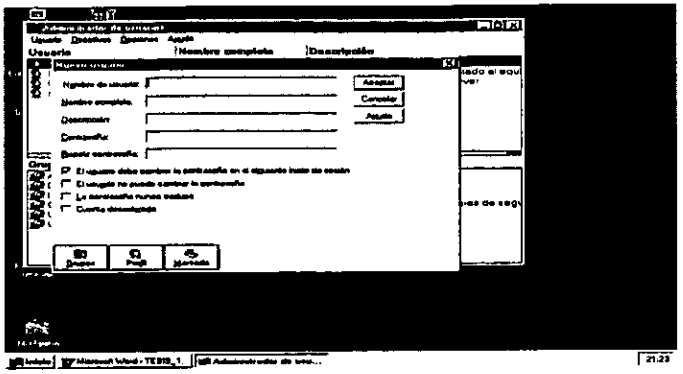


Fig. 4.3 Cuentas de Usuario.

Este tipo de cuentas son mas difíciles de administrar que las globales, también permiten a usuarios de **LAN Manager, IBM LAN Server o NetWare** participar en dominios de **Windows NT**.

4.6. LA ADMINISTRACION DE SEGURIDAD

La administración de seguridad se usa para asignar derechos a los usuarios y grupos para trabajar dentro de directorios y archivos.

Hay que distinguir entre permisos estándar y permisos de acceso especial tanto a nivel de directorios como de archivos.

4.6.1. PERMISOS DE DIRECTORIOS

Cuando se establecen permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio o sus archivos.

Estos permisos sólo puede establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Una vez establecidos los permisos, únicamente afectaran a los archivos y subdirectorios que dependan de él y que se creen posteriormente, los que ya existían no se verán afectados.
Un asterisco colocado a continuación de un grupo de permisos significa que sus subdirectorios no heredan los permisos concedidos.

Cuando se especifican los permisos aparecen a su lado dos abreviaturas de permisos individuales que son: los permisos para el directorio y los permisos para los archivos.
Los permisos que se pueden otorgar para directorios son:

- **Sin acceso (Ninguno).** Impide cualquier acceso al directorio y a sus archivos.

- **Agregar(WX) (Sin especificar).** Permite agregar archivos y subdirectorios al directorio pero no permite acceder a los archivos (a no ser que se cuente con otros permisos).

- **Agregar y leer (RWX) (RX).** Permite ver nombres de archivos y subdirectorios, cambiar los subdirectorios, ver los datos de los archivos, ejecutar archivos de aplicación, y agregar archivos y subdirectorios al directorio.

- **Cambio (RWXD) (REXD).** Permite ver nombres de archivos y subdirectorios, ir a los subdirectorios, cambiar los subdirectorios, ver los datos de los archivos, ejecutar archivos de aplicación, agregar archivos y subdirectorios, cambiar los datos de los archivos, y eliminar archivos y subdirectorios.

- **Control total (Todos) (Todos).** Es el máximo nivel y permite todas las acciones tanto a nivel de archivos como de subdirectorios.

- **Lectura (RX) (RX).** Permite ir a los subdirectorios, ver los nombres de archivos y subdirectorios pero no permite acceder a los archivos (a no ser que se cuente con otros permisos).

- **Listado (RX)(Sin especificar).** Permite cambiar los subdirectorios y ver los nombres de archivos y subdirectorios, pero no permite acceder a los archivos. Fig. 4.4.

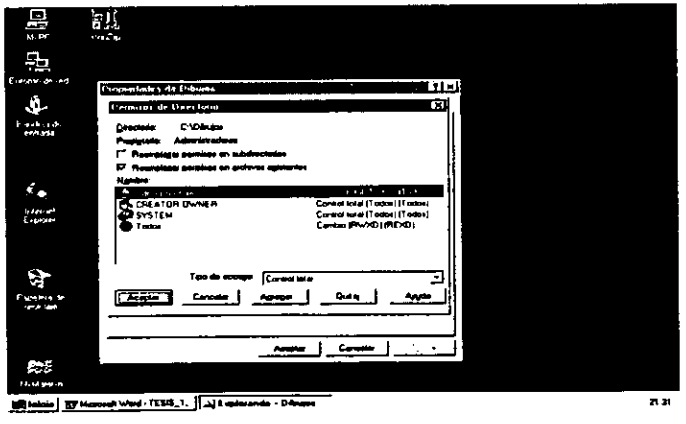


Fig. 4.4 Permisos estándar de directorios.

Estos permisos son acumulables, pero el permiso sin acceso elimina a los demás.

Si a un usuario o grupo se le otorga el permiso de Control completo sobre un directorio, podrá eliminar sus archivos independientemente de los permisos que tengan estos.

4.6.2. PERMISOS DE ARCHIVOS

Cuando se establecen permisos sobre un archivo se define el acceso de un usuario o de un grupo a dicho archivo. Los archivos que se crean en un directorio adoptan los permisos del directorio de que forman parte.

Estos permisos sólo puede establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Cuando se especifican los permisos aparecen a su lado unas abreviaturas que definen los permisos para los archivos.

Solo es posible establecer permisos para directorios de unidades formateadas para ser usadas por el sistema NTFS.

Los permisos estándar para archivo que se pueden otorgar son:

- **Sin acceso (Ninguno).** Impide cualquier acceso al archivo.
- **Cambio (REXD).** Permite ver nombres y datos de los archivos, ejecutar archivos de aplicación, cambiar los datos de los archivos y eliminarlos.
- **Control total (Todos).** Es el máximo nivel y permite realizar todas las acciones con ellos.
- **Lectura (RX).**Permite ver los nombres y datos de los archivos y ejecutar archivos de aplicación.

Estos permisos son acumulables, pero el permiso Sin acceso elimina a los demás.

Si a un usuario o grupo se le otorga el permiso de Control completo sobre un directorio, podrá eliminar sus archivos independientemente de los permisos que tengan estos.

4.6.3. PERMISOS DE ACCESO ESPECIAL

Generalmente, todo los que necesitará para proteger los directorios y los archivos son los permisos estándar que se han descrito anteriormente.

Sin embargo, si desea crear un sistema personalizado de permisos, puede utilizar los permisos especiales de acceso.

Puede establecer permisos especiales de acceso para directorios, para todos los archivos de los directorios seleccionados o para los archivos seleccionados (los no seleccionados mantendrán sus actuales permisos). Fig. 4.5.

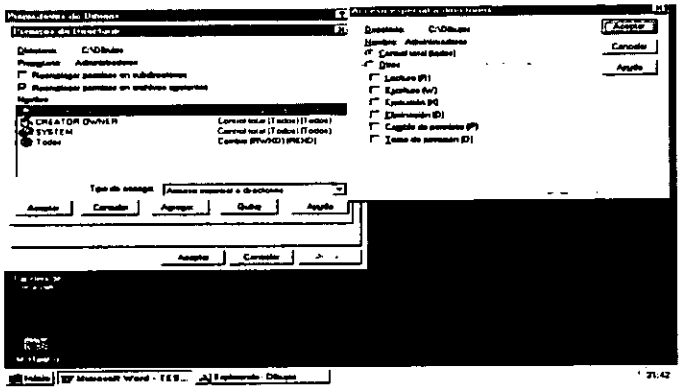


Fig. 4.5 Permisos especiales de directorio.

Los permisos de acceso especial para directorios son:

- **Cambio de permisos (P).** Permite cambiar los permisos del directorio.
- **Ejecución (x).** Permite cambiar a otros subdirectorios del directorio.
- **Eliminación (D).** Permite eliminar el directorio.
- **Escritura (W).** Permite agregar subdirectorios y archivos.
- **Lectura (L).** Permite ver los nombres de los directorios y archivos.
- **Toma de posesión (O).** Permite tomar posesión del directorio.

Los permisos de acceso especial para archivos son:

- **Cambio de permisos (P).** Permite cambiar los permisos del archivo
- **Ejecución (X).** Permite ejecutar un archivo de aplicación.
- **Eliminación (D).** Permite eliminar el archivo.

- **Escritura (W).** Permite modificar los datos del archivo.
- **Lectura (L).** Permite ver los datos del archivo.
- **Toma de posesión (T).** Permite tomar posesión del archivo.

4.6.4. SEGURIDAD DEL SERVIDOR

Dentro del concepto de seguridad del servidor se pueden distinguir cuatro apartados:

- La seguridad física.
- La seguridad de los datos.
- La protección de acceso a la computadora.
- La protección de acceso a los datos.

4.6.5. SEGURIDAD FISICA DEL SERVIDOR

El lugar donde va a estar situado el servidor es sumamente importante para su seguridad. El servidor necesita estar protegido contra distintos factores externos que pueden alterar el funcionamiento de la red.

Estos factores externos son: electricidad estática, el calor, el frío, el polvo y la humedad, los ruidos eléctricos, los altibajos de tensión y los cortes de corriente, la suciedad, los incendios y el agua, así como debe estar protegido contra robo y destrucción.

4.6.6. PROTECCION CONTRA ELECTRICIDAD ESTATICA

Se han de tomar algunas precauciones para proteger al servidor de las cargas estáticas, ya que el rendimiento de este afecta a toda la red.

Entre las precauciones que se han de tomar esta la de tratar regularmente las alfombras con productos antiestáticos, utilizar fundas protectoras para las alfombras e instalar el servidor sobre una superficie conectada a una toma de tierra.

No utilizar plásticos ni material sintético, ya que generan electricidad estática.

4.6.7. PROTECCION CONTRA EL CALOR, EL FRIO, EL POLVO Y LA HUMEDAD

El calor y el frío excesivos son riesgos potenciales para el buen funcionamiento del servidor.

Para proteger el servidor, lo mejor es tener una buena instalación de aire acondicionado que mantenga la temperatura de la habitación entre 18° y 26° C y asegure una buena circulación de aire en la sala, que evite la acumulación de polvo.

Así mismo, el aire acondicionado evitara una concentración grande de humedad que pueda interferir en el buen funcionamiento del servidor.

4.6.8. PROTECCION CONTRA RUIDOS ELECTRICOS, VARIACIONES DE TENSIÓN U CORTES DE CORRIENTE

Los ruidos eléctricos son causados por las inconsistencias del suministro de la corriente a la computadora. Para proteger al servidor contra los ruidos eléctricos, puede recurrirse a la instalación de una línea dedicada de suministro eléctrico.

No hay que conectar otros dispositivos a este suministro de corriente, porque pueden generar ruidos que anulen las ventajas de la protección ofrecida por la fuente de corriente dedicada.

La conexión a la fuente de energía se ha de realizar con cable estándar de tres hilos.

Debe prevenirse contra los altibajos de tensión y contra el corte de la corriente. Para ello, lo mejor es complementar la instalación con un sistema de alimentación interrumpida o SAI (**UPS, Uniterrumpible Power Suply**). El SAI permite al servidor continuar activo durante cierto tiempo ante un eventual corte de la corriente.

Puede también tomarse la precaución de instalar un SAI en cada una de las estaciones que trabajen con aplicaciones criticas para protegerse de los daños producidos por la perdida de datos durante un corte de energía.

Además, cada dispositivo de la red podría tener un filtro de energía eléctrica como protección de las sobretensiones.

En caso de instalar un SAI, deberá configurar el software correspondiente. He aquí los apartados que habría que configurar para su uso con Windows NT:

- Ejecute el icono **SAI** del **Panel de Control**. Verá la siguiente figura. Fig.4.6.

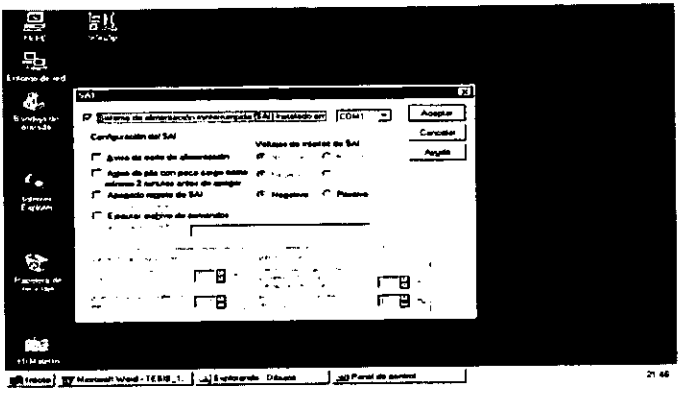


Fig. 4.6 Configuración del UPS.

- En Sistema de alimentación ininterrumpida (SAI) en donde deberá indicar el puerto serie en el que se encuentra instalado el SAI.

Además deberá indicar los siguientes apartados:

En el bloque Configuración del SAI se encuentran las siguientes opciones:

- **Aviso de corte de alimentación**. Si su SAI puede enviar un mensaje cuando se produzca un corte en la alimentación eléctrica. seleccione esta opción (corresponde al permiso para transmitir (CTS) de la conexión del puerto serie del SAI).

- **Aviso de pila con poca carga como mínimo 2 minutos antes de apagar**. Si su SAI puede enviar un aviso cuando la pila tenga poca carga, seleccione esta opción (corresponde a la detección de portadora de datos (DCD) de la conexión del puerto serie del SAI).

- **Apagado remoto de SAI**. Indica esta activado el apagado remoto del SAI (corresponde a la línea terminal de datos preparada (DTR) de la conexión del puerto serie del SAI).

- **Voltajes de interfaz de SAI**. Si ha activado alguno de los apartados anteriores, deberá indicar Positivo o Negativo (en dichas casillas) para indicar el voltaje de interfaz del SAI).

- **Ejecutar archivo de comandos**. Al marcar esta opción (e indicar el nombre de un archivo de comandos). Podrá ejecutar dicho archivo inmediatamente antes del apagado del sistema (habrá un tiempo máximo de treinta segundos para la ejecución completa del archivo de comandos).

En el bloque Características del SAI se encuentran las siguientes opciones:

- **Duración estimada de la pila**. Indica la duración de la pila cuando se encuentra totalmente cargada (el rango esta entre 2 y 480 minutos y el valor por defecto es 2).

- **Tiempo de recarga de la pila por cada minuto de ejecución**. Si selecciono Aviso de corte de alimentación y no selecciono Aviso de pila con poca carga como mínimo 2 minutos antes de apagar. Deberá seleccionar esta opción (el rango esta entre 5 y 250 minutos y el valor por defecto es de 100).

En el bloque Servicio de SAI se encuentran las siguientes opciones:

- **Tiempo entre el corte de alimentación y el primer mensaje de advertencia**. Indica el tiempo que transcurrirá entre el corte de alimentación eléctrica y el envío del primer mensaje de aviso a los usuarios (el rango esta entre 0 y 120 segundos y el valor por defecto es 5).

- **Retardo entre mensajes de advertencia**. Indica el intervalo entre los mensajes sucesivos que se irán enviados a los usuarios cuando se haya producido un corte de alimentación eléctrica (el rango esta entre 5 y 300 segundos y el valor por defecto es 120).

- Cuando haya finalizado, marque Aceptar y, si no ha iniciado el servicio UPS. Le indicará si desea iniciarlo ahora. Marque SI para hacerlo.

4.6.9. SEGURIDAD DE LOS DATOS

Es importante que los datos que están ubicados en el servidor de la red se encuentren bien protegidos.

Para que los datos se encuentren perfectamente protegidos, hay que considerar dos apartados.

- Seguridad del almacenamiento en el disco duro.

- Copias de seguridad de los datos.

4.6.10. SEGURIDAD DEL ALMACENAMIENTO EN EL DISCO DURO

Actualmente, la unidad básica de almacenamiento de la información es el disco duro. Su capacidad esta en constante incremento (en la actualidad oscila entre 1,2 GB y 10 GB).

La forma más común de organizar el almacenamiento de la información es a través de un único disco (cuenta con la ventaja de la simplicidad de su configuración), aunque, dependiendo del tamaño de la empresa, se puede considerar la posibilidad de trabajar con dos o más discos duros asociados.

Cada disco duro del sistema tiene asignado un número (comenzando por el cero) y se asignan de forma diferente en función del tipo de disco:

- **SCSI.** En una controladora primaria de este tipo los números van del cero al seis (aunque posee otra dirección que suele estar reservada para el adaptador del bus). Cuando esta controladora se completa puede recurrirse a una controladora secundaria y así sucesivamente hasta un total de cuatro (lo que permitiría disponer de hasta un total de 28 unidades).

- **IDE y ESDI.** En una controladora primaria de estos dos tipos, los números van del cero al uno. Cuando esta controladora se completa se puede recurrir a una segunda controladora (lo que permitiría disponer de hasta un total de cuatro discos).

Todos los discos duros deben estar formateados a bajo nivel para poder utilizarse.

4.6.11. PARTICIONES

La partición hace que un disco duro, o una parte de él, pueda ser utilizada como medio de almacenamiento.

Por medio de las particiones el disco duro se puede dividir en unidades lógicas de las que cada una permitirá el acceso a una parte del disco duro.

Las particiones pueden ser de dos tipos:

- **Particiones primarias**, que son reconocidas por el BIOS de la computadora como capaz de iniciar el sistema operativo desde ellas. Para ello, dispone de un sector de arranque.

Pueden existir hasta un máximo de cuatro particiones primarias de las cuales solamente una puede estar activa en cada momento.

Con un programa de inicialización adecuado se podría seleccionar entre los diferentes sistemas operativos para su arranque (cada uno deberá estar en su propia partición primaria).

- **Particiones secundarias** que se forman en las áreas del disco duro que no tienen particiones primarias y que están contiguas.

Puede haber, como máximo una partición secundaria (en este caso, el disco duro no podría tener mas de tres particiones primarias).

4.6.12. UNIDADES LOGICAS

Las particiones deben estar formateadas para establecer letras de unidades que van de la C: en adelante (con la excepción de la unidad CD-ROM que se reserva la letra D:).

La partición primaria corresponde a la unidad C:

Las particiones secundarias se pueden dividir en una o varias unidades lógicas.

4.6.13. COPIAS DE SEGURIDAD DE LOS DATOS

Pero que ocurre si por error, distracción, etc. se llegara a producir una perdida de datos importante, pues no pasaría nada si se cuenta con un buen sistema de copias de seguridad de dichos datos que permita restaurar la información prácticamente al mismo nivel que se encontraba antes de su perdida.

Antes de empezar con las copias de seguridad, es necesario determinar quien va a ser el responsable o los responsables de su realización.

Algunos administradores de red dejan los procesos de copias de seguridad a usuarios individuales, lo que significa que cada uno de ellos se responsabiliza únicamente de guardar sus propios archivos.

Esta forma de actuar no es buena, ya que los usuarios no dedican el tiempo ni la periodicidad necesaria para realizar unas copia de seguridad adecuada de sus archivos.

Por tanto, es mucho más positivo que sea un administrador de la red, como responsable de mantener el funcionamiento y mantenimiento del sistema, el que se encargue de las copias de seguridad o delegue en otros usuarios que pertenezcan a un grupo de operadores de copia.

4.6.14. RESPALDO DIARIO DE LOS ARCHIVOS

El proceso del respaldo de los archivos casi siempre necesita bastante tiempo para su realización. Por tanto, es conveniente que solo realice el respaldo diario de los archivos que hayan sido modificados.

Primero, deberá determinar cuales son los archivos de la red que deben respaldarse. Por lo general, los programas de aplicaciones y del sistema operativo no suelen sufrir variaciones y, por tanto, no necesitan respaldarse diariamente.

En cambio, los archivos, con datos de los usuarios y de configuración de los programas o del sistema operativo son los que sufren variaciones, por tanto deberá respaldarlos diariamente.

Para ello, podrá realizar dos métodos de respaldo:

- **Respaldo diferencial.** Se realiza con los archivos cuyo bit de archivos se puso a uno en el ultimo respaldo completo, pero no se restaura a cero (dicho bit de archivación) para que los archivos vuelvan a respaldarse al día siguiente.

- **Respaldo incremental.** Se realiza con los archivos cuyo bit de archivación se puso a uno en el ultimo respaldo completo pero se restaura a cero (dicho bit de archivación) para que los archivos no se vuelvan a respaldar al día siguiente (a no ser que se hayan vuelto a modificar).

Para poder localizar fácilmente el respaldo realizado en ultimo lugar,, es muy recomendable poner en cada uno la fecha y la hora en que se hizo.

4.6.15. RESPALDO SEMANAL DEL SISTEMA COMPLETO

Este método consiste en realizar un respaldo completo de todo el contenido del servidor y, al igual que el método diario, es recomendable que se realice en unidades de cinta.

De este modo, en caso de tener que restaurar el contenido del servidor se realizara de forma fácil y rápida.

Es el método mas adecuado, porque permite tener pocas copias y, de esa forma, poder encontrar fácilmente la adecuada.

4.6.16 COPIADO MENSUAL DE LOS ARCHIVOS

Por lo general, el copiado de los archivos es suficiente conque se realice una vez al mes, asegúrese de que tiene copiados los archivos en un medio o soporte diferente (cinta, disco, CD) las copias de seguridad para que en caso de perdida o deterioro de la cinta pueda recuperar la información.

El objetivo del copiado es distinto al del respaldo de los archivos, por lo que tendrá que seguir diferentes procedimientos entre los cuales se encuentran las siguientes:

- Determinar que directorios y archivos son los que van a copiarse.

- Determinar si los archivos van a ser borrados, después de ser copiados.
- Es recomendable comprimir los archivos antes de copiarlos, ya que reducirá el espacio de almacenamiento y el tiempo que tardara en realizarse el proceso.
- Indicar quien va a realizar el procedimiento de copiado y borrado de los archivos que no desea guardar en el servidor.
- Pedir que saquen un listado de los archivos que se han copiado.
- Guardar en lugar seguro las copias de los archivos.

4.7. INTERNET INFORMATION SERVER (IIS)

Windows NT Server 4.0 incorpora **Internet Informacion Server 2.0 (IIS)** que permite incorporar en su empresa las tres siguientes tecnologías de Internet:

- Un servidor **World Wide Web (WWW)**.
- Un servidor **File Transfer Protocol (FTP)**.
- Un servidor **Gopher**.

Puede, si lo desea, incorporar estos servicios para Internet Information Server 3.0 que viene incorporada en el **Service Pack 3.0** (se puede obtener gratuitamente de Microsoft) y que cuenta con mejoras con respecto a la versión 2.0 que incorpora de origen Windows NT 4.0 Server.

Para poder realizar la instalación de **IIS 3.0**, deberá comprobar los siguientes apartados:

- Tener instalado convenientemente TCP/IP en los equipos que van a participar en la Intranet.
- Buscar un servidor Windows NT que actúe como servidor IIS (si va tener mucho trabajo, deberá estar dedicado sólo a dicha tarea).
- Deshabilitar cualquier servidor WWW, FTP o Gopher de dicho servidor IIS.
- Tener formateado los volúmenes de dicho servidor con e sistema de archivos NTFS para garantizar el mayor nivel posible de seguridad.
- Habilitar la auditoría si piensa que necesita monitorizar el servidor para evitar violaciones de la seguridad.

- Poner en funcionamiento un servidor WINS (si todos los equipos son de Microsoft) o un archivo hosts (si hay equipos que no son de Microsoft pero teniendo en cuenta que cualquier equipo que se añada a la red hará modificar todos los archivos).

4.7.1. INSTALACION IIS

Desde el equipo que va a actuar de servidor IIS siga los pasos siguientes para proceder a su instalación (una vez este instalado el servidor Windows NT y el Service Pack 3 que incluye el Internet Información Server 3.0), habiendo iniciado la sesión como un usuario miembro del grupo Administradores:

- Ejecute la utilidad **Instalación de Internet Server**, que esta incluida dentro de Microsoft Internet Server, que forma parte del menú Programas del botón Inicio. Fig. 4.7.

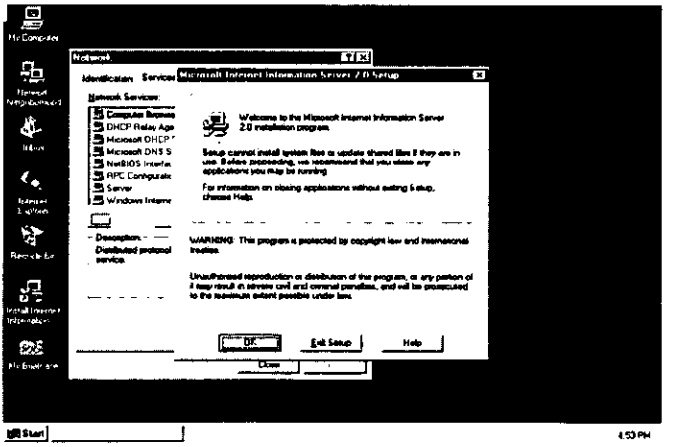


Fig. 4.7 Instalación del IIS.

- Le mostrará una pantalla de bienvenida. **Marque Aceptar**.

- De la pantalla que le muestra, marque Agregar/Eliminar. Especifique el lugar donde se encuentran los archivos de instalación de IIS 3.0 (por defecto, están en **C:\WINNT\system32\inetsrv**) y marque **Aceptar.**

- Le muestra las posibles opciones a instalar, que son:

- Administrador de servicio Internet. Permite instalar el programa de administración para gestionar los servicios.

- Servicio World Wide Web. Crea un sitio WWW en dicho servidor.

- Ejemplos del servicio WWW. Instala archivos HTML de ejemplo.
- Administrador de servicios Internet (HTML). Instala la versión HTML para poder administrar los servicios a través de un explorador.
- Servicio Gopher. Crea un sitio Gopher en dicho servidor.
- Servicio FTP. Crea un sitio FTP en dicho servidor.
- Administración y controladores ODBC. Instala controladores ODBC (Open Database Connectivity) para poder tener acceso a bases de datos.

Compruebe que todas las opciones estén marcadas (en caso contrario, hágalo) y marque Aceptar. Fig. 4.8.

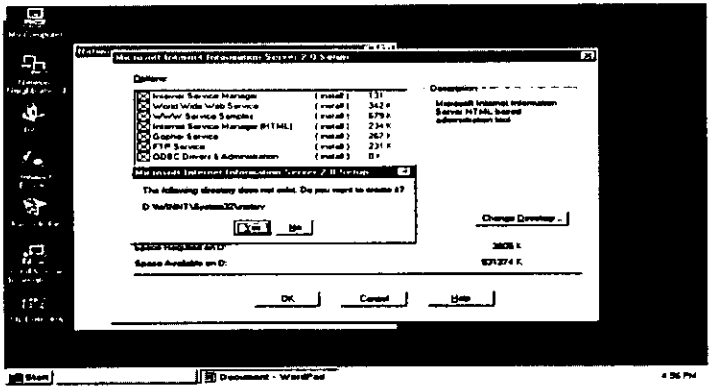


Fig. 4.8 Seleccionando opciones del IIS.

- Se crearán los siguientes directorios por default D:\InetPub\wwwroot, D:\InetPub\ftproot, D:\InetPub\gophroot, presionar yes para crear los directorios. Fig. 4.9.

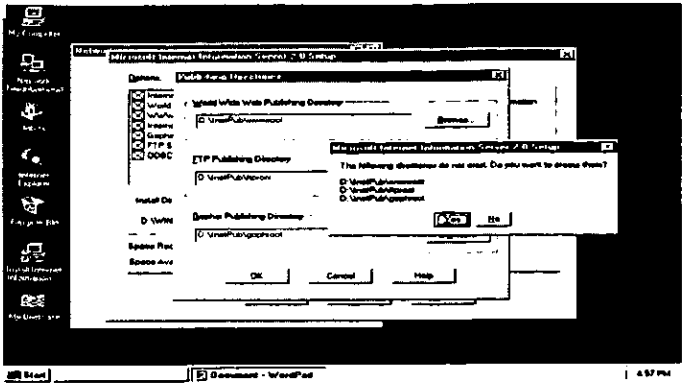


Fig. 4.9 Creación de directorios de trabajo para la Intranet.

- Si ha seleccionado instalar los controladores ODBC, es posible que aparezca una pantalla con SQL Server como única opción. Marque Aceptar.

- Procederá al copiado de los archivos necesarios para instalar lo que se indico (en el caso de que se produzca algún error por haber archivos abiertos, desinstale todas las utilidades IIS y vuelva a instalarlas otra vez desde **Agregar un servicio** de Servicios del **icono Red**).

- Cuando haya finalizado, marque **Aceptar.**

- Reinstale de nuevo el Service Pack 3 (recuerde que es necesario reinstalarlo cada vez que añada algún programa al servidor).

En caso de no tener la opción Microsoft Internet Server (Común), que forma parte del menú Programas del botón Inicio, es que no esta instalado IIS. En ese caso, instálelo desde Agregar un servicio de Servicios del icono Red.

4.7.2. ADMINISTRACION DE IIS

Para administrar IIS, siga los pasos siguientes:

1. Ejecute la utilidad **Administrador de servicios Internet**, que esta incluida dentro de la Microsoft Internet Server (Común), que forma parte del menú Programas del botón Inicio.

2. En ella puede observar que en el equipo Principal se encuentran instalados los servicios **WWW, Gopher y FTP**.

Los tres posibles estados en que pueden encontrarse los servicios son: En servicio, En pausa y Deteniendo. Fig. 4.10.

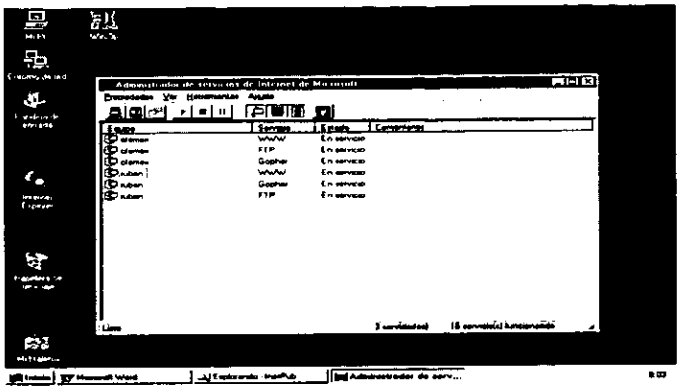


Fig. 4.10 Estados de los servicios IIS.

3. Todas las opciones que hay en el menú Propiedades son:

   - Conectar al servidor. Conecta a un servidor IIS para poder observar y administrar los servicios que están actuando.

   - Buscar todos los servidores. Busca en la red para identificar todos los servidores IIS que existen. Una vez detectados se mostrarán, junto con sus servicios en la lista.

   - Propiedades del servicio. Si tiene seleccionado un servicio y elige esta opcion, podra observar y modificar las propiedades de dicho servicio.

   - Iniciar servicio. Permite iniciar el servicio seleccionado.

   - Detener servicio. Permite detener el servicio seleccionado.

   - Hacer una pausa en el servicio. Permite hacer una pausa en el servicio seleccionado.

4. Todas las opciones que hay en el menú Ver son:

   - **FTP**. Si elige solo esta opción, verá únicamente todo lo referente a los servidores FTP.
   - **Gopher**. Si elige solo esta opción, verá únicamente todo lo referente a los servidores Gopher.
   - **WWW**. Si elige solo esta opción, verá únicamente todo lo referente a los servidores WWW.

   - Todos. Si elige esta opción, verá todo lo referente a los tres tipos de servidores

- Ordenar por servidor. Si elige esta opción, la lista se ordenara por el nombre del servidor donde están instalados.

- Ordenar por servicio. Si elige esta opción, la lista se ordenara por el nombre del servicio instalado.

- Ordenar por comentario. Si elige esta opción, la lista se ordenara por el comentario.

- Ordenar por estado. Si elige esta opción, la lista se ordenara por el estado en que se encuentra el servicio.

- Ver servidores. Si elige esta opción, verá el nombre de los servidores donde hay instalados servicios IIS. Si marca el signo + que hay a la izquierda del servidor, se mostrarán los servicios que hay instalados en el así como su estado.

- Ver servicios. Si elige esta opción, verá el nombre de los servicios IIS instalados. Si marca el signo + que hay a la izquierda del servicio, se mostrará el servidor donde esta instalado así como su estado.

- Ver informe. Si elige esta opción, verá la pantalla por defecto.

5. En el menú Herramientas se puede acceder al Administrador de claves.

4.7.3. CONFIGURACION DEL SERVICIO WWW

Para configurar el servicio WWW siga los pasos siguientes:

1. Ejecute la utilidad Administrador de servicios Internet, sitúese sobre el servicio WWW, pulse dos veces el botón izquierdo del ratón y le mostrará la figura siguiente. Fig. 4.11.

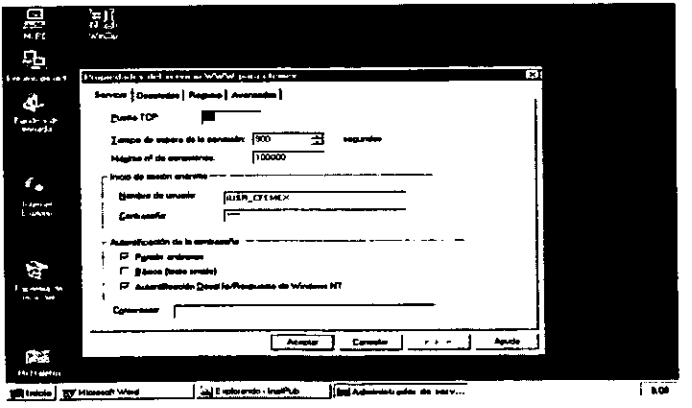


Fig. 4.11 Configurando servicio WWW.

2. Se encuentra en la **pantalla Servicio** que cuenta con los siguientes apartados:

   - **Puerto TCP.** Determina el puerto que esta utilizando este servicio. Por defecto es el 80, pero puede cambiarlo por cualquier número de puerto TCP único (si lo cambia, para que tenga efecto, deberá reiniciar el equipo).

   - **Tiempo de espera de la conexión.** Indica el tiempo de inactividad (en segundos) que ha de pasar para que el servidor desconecte al usuario

   - **Máximo nº de conexiones.** Indica el número máximo de conexiones simultaneas que se pueden establecer con el servidor.

En el bloque **Inicio de sesión anónimo** se encuentran las siguientes opciones:

- **Nombre de usuario.** Establece la cuenta de usuario que se va a utilizar para controlar los permisos de todas las conexiones anónimas. Deberá comprobar que esta cuenta tenga el permiso de lectura sobre el directorio **C:\WINNT\InetPub\wwwroot.**

- **Contraseña.** Al crear la cuenta, se le asigno una contraseña aleatoria (que solo se usa dentro de Windows NT y que no puede estar en blanco). Si cambia la contraseña deberá asegurarse de que coincida tanto en el Administrador de usuarios para dominios como en el Administrador de servicios de Internet.

En el bloque Autentificación de la contraseña se encuentran las siguientes opciones:

- Permitir anónimos. Indica si se van a permitir accesos anónimos al servidor.

- Básica (texto simple). Indica que los nombres de usuarios y sus contraseñas se van a enviar sin codificar antes de la transmisión.

- Autentificación Desafío/Respuesta de Windows NT. Indica que se va a utilizar una codificación automática de los nombres de usuario y sus contraseñas.

3. Si se marca Directorios. Fig. 4.12, verá la siguiente pantalla:

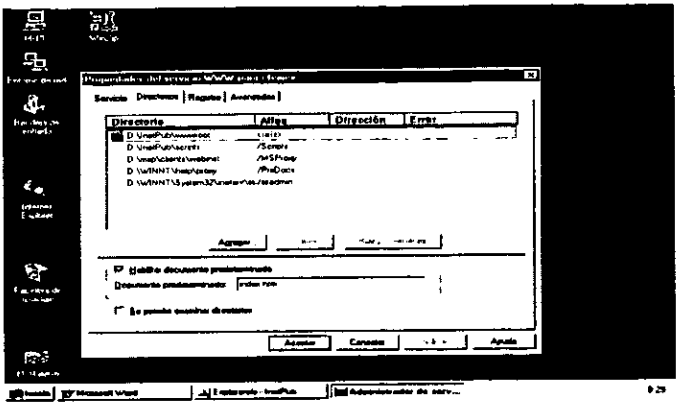


Fig. 4.12 Opciones de la etiqueta directorios en WWW.

En ella se muestran los directorios utiliza WWW.

En el cuadro se encuentran: en **Directorio** la ruta de los directorios usados, en **Alias** la ruta usada para los directorios virtuales que corresponde realmente con el directorio usado, en **Dirección** muestra la dirección IP para el servidor virtual que usa dicho directorio y en **Error** muestra los errores del sistema para dicho directorio.

Si selecciona un directorio y marca **Agregar** o Editar **Propiedades**, podrá modificar los permisos del directorio.

Si selecciona un directorio y marca **Eliminar**, eliminara dicho directorio.

Los apartados Habilitar Documento Predeterminado y Se Permite Examinar Directorios se utilizan para establecer las presentaciones que aparecen sin un usuario remoto no especifican un archivo en concreto (las opciones por defecto son que no se permite examinar directorios, y se presentara el documento **DEFAULT.HTM** a todos los usuarios que se conecten al servidor y no especifiquen ningún archivo). Sustituimos default.htm por nuestra página principal.htm para poder navegar por la Intranet, de esta forma al abrir el Internet Explorer se podrá accesar a todos los servicios disponibles. Fig. 4.13.

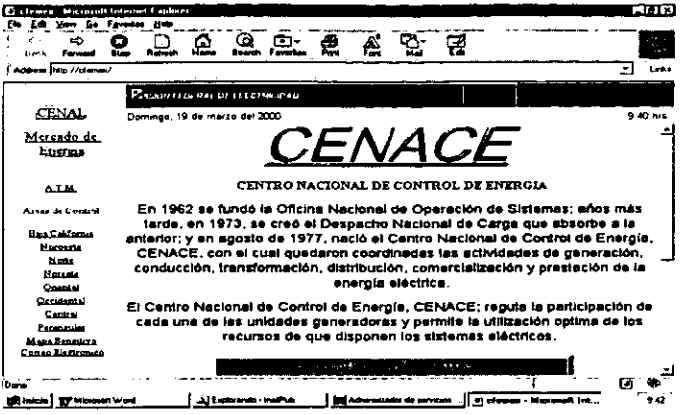


Fig. 4.13 Página principal del servicio WWW para la Intranet.

4. Si marca Registro. Fig. 4.14, verá la siguiente pantalla:

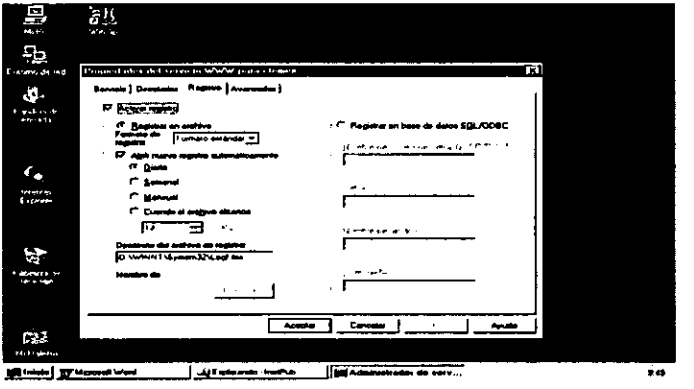


Fig. 4.14 Etiqueta registro en el WWW.

En ella se muestran los siguientes apartados:

- Activar registro. Indica que se activa el registro de la actividad de dicho servicio.

En el bloque **Registrar** en archivo se indica que se guarden en un archivo los datos de la actividad. En el se encuentran las siguientes opciones:

- **Formato de registro.** Indica el tipo de formato de registro a utilizar.

- **Abrir nuevo registro automáticamente**. Indica la frecuencia con la que se generara un nuevo registro. Puede ser: Diario, semanal, Mensual o Cuando el archivo alcance un determinado tamaño.

- **Directorio del archivo de registro**. Muestra la ruta donde se encuentran los archivos de registro (el nombre del archivo esta formado por un prefijo mas los dos últimos dígitos del año, el número del mes, el número del día y la extensión LOG).

En el bloque **Registrar en base de datos SQL/ODBC** se indica que se guarden en una tabla ODBC los datos de la actividad. En ella se encuentran las siguientes opciones:

- Registrar en base de datos **SQL/ODBC**. Se indica que se guarden en una tabla ODBC los datos de la actividad. Deberá indicar las siguientes opciones:

  - Nombre de origen de datos ODBC (DSN). Indica el origen de datos ODBC a utilizar.

  - Tabla. Indica el nombre de la tabla donde se guardarán los datos de la actividad.

  - Nombre de usuario. Indica un nombre de usuario valido para el equipo donde se encuentra la base de datos.

  - Contraseña. Indica la contraseña de dicho usuario.

5. Si marca Avanzadas. Fig. 4.15, verá la siguiente pantalla:

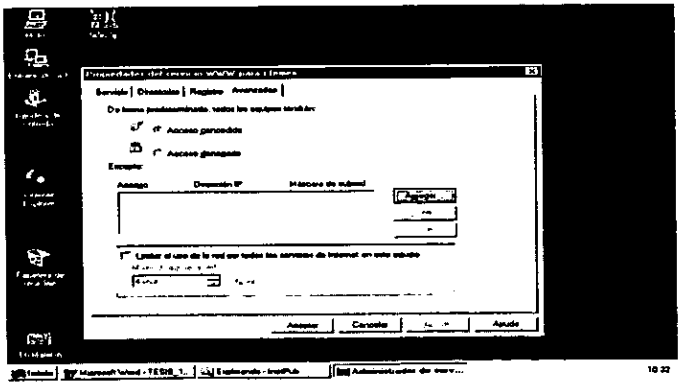


Fig. 4.15 Etiqueta avanzadas en el WWW.

En ella se muestran los siguientes apartados:

- **Acceso concedido**. Indica que todos los equipos tienen acceso a este servicio.

- **Acceso denegado**. Indica que todos los equipos tienen denegado este servicio excepto aquellos que están indicados en la lista (habrá que indicar la dirección IP de dichos equipos).

- **Máximo uso de la red.** Si marca Limitar el uso de la red por todos los servicio de Internet en este equipo deberá indicar el ancho de banda máximo que podrán utilizar los equipos para utilizar este servicio.

La utilidad que incorpora Windows NT para acceder a un servidor WWW es Microsoft Internet Explorer con la dirección http://nombre de su equipo/ (que para nuestro caso es **cfemex**, además puede indicar otros subdirectorios donde se encuentren paginas HTML).

Para crear o modificar paginas HTML puede usar cualquier procesador de textos que permita guardar en archivo HTML o un editor HTML como Microsoft Front Page (que también se incluye en Windows NT) que le permitirá incluir vinculos con otros archivos del sistema.

4.7.4. CONFIGURACION DEL SERVICIO FTP

Para configurar el servicio FTP siga los pasos siguientes:

1. Ejecute la utilidad **Administrador de servicios Internet**, sitúese sobre el servicio FTP pulse dos veces el botón izquierdo del ratón y le mostrará la siguiente pantalla:

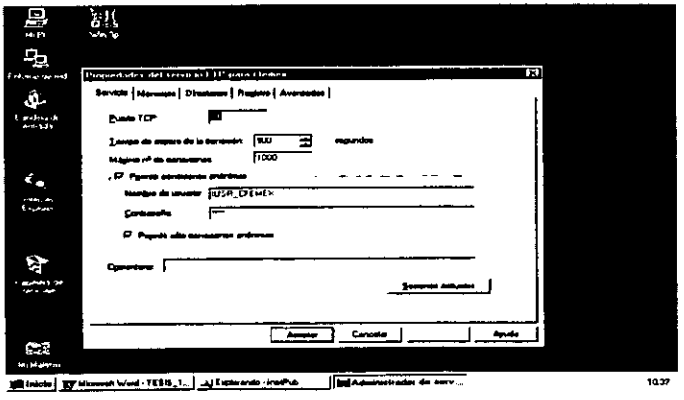


Fig. 4.16 Servicio FTP del IIS.

2. Se encuentra en la pantalla Servicio, que cuenta con los siguientes apartados:

   - **Puerto TCP.** Determina el puerto que esta utilizando este servicio. Por defecto, es el 21; pero puede cambiarlo por cualquier número de puerto TCP único (si lo cambia, para que tenga efecto, deberá reiniciar el equipo).

   - **Tiempo de espera de la conexión.** Indica el tiempo de inactividad (en segundos) que ha de pasar para que el servidor desconecte al usuario.

   - **Máximo n- de conexiones.** Indica el número máximo de conexiones simultaneas que se pueden establecer con el servidor.

En el bloque Permitir conexiones anónimas se encuentran las siguientes opciones:

   - Nombre de usuario. Establece la cuenta de usuario que se va a utilizar para controlar los permisos de todas las conexiones anónimas. Deberá comprobar que esta cuenta tenga el permiso de Lectura sobre el directorio **C:\WINNT\InetPub\ftproot**.

   - Contraseña. Al crear la cuenta, se le asigno una contraseña aleatoria (que solo se usa dentro de Windows NT y que no puede estar en blanco). Si cambia la contraseña deberá asegurarse de que coincida tanto en el Administrador de servicios de Internet.

   - Permitir solo conexiones anónimas. Al marcar esta casilla, los usuarios no podrían iniciar sesión con sus nombres de usuario y sus contraseñas, sino que únicamente podrán hacer conexiones anónimas (ftp anonymous).

- **Comentario.** Especifica el texto que se presentara en la pantalla principal.

- **Sesiones actuales.** Al marcar este botón, verá los usuarios FTP actuales.

3. Si marca **Mensajes**, verá la pantalla donde podrá indicar el mensaje de bienvenida, de salida y el que mostrará cuando se alcance el número de conexiones máximas.

4. Si marca **Directorios**, verá la pantalla donde se muestran los directorios que utiliza FTP.

En el cuadro se encuentran: en Directorio la ruta de los directorios usados, en Alias la ruta usada para los directorios virtuales que se corresponde realmente con el directorio usado y en Error muestra los errores del sistema para dicho directorio.

Si selecciona un directorio y marca **Agregar** o **Editar Propiedades**, podrá modificar los permisos del directorio.

Si selecciona un directorio y marca **Eliminar**, eliminara dicho directorio.

En el apartado **Estilo** de la lista de directorios, deberá estar dicho directorio.

En el apartado **Estilo de la lista de directorios**, deberá indicar el formato en que desea que se muestren los archivos.

5. Si marca **Registro**, verá una pantalla donde se muestran los siguientes apartados:

   - Activar registro. Indica que se active el registro de la actividad de dicho servicio.

   - Abrir nuevo registro automáticamente. Indica la frecuencia con la que se generara un nuevo registro. Puede ser: Diario, semanal, mensual o Cuando el archivo alance un determinado tamaño.

   - Directorio del archivo de registro. Muestra la ruta donde se encuentran los archivos de registro (el nombre del archivo esta formado por un prefijo mas los dos últimos dígitos del año, el número del mes, el número del día y la extensión LOG).

En el bloque Registrar en base de datos SQL/ODBC se indica que se guarden en una tabla ODBC los datos de la actividad. En ella se encuentran las siguientes opciones:

- Nombre de origen de datos ODBC (DSN). Indica el origen de datos ODBC a utilizar.

- Tabla. Indica el nombre de la tabla donde se guardarán los datos de la actividad.

- Nombre de usuario. Indica un nombre de usuario valido para el equipo donde se encuentra la base de datos.

- Contraseña. Indica la contraseña de dicho usuario.

6. Si marca **Avanzadas**, verá una pantalla donde se muestran los siguientes apartados:

   - Acceso concedido, Indica que todos los equipos tienen acceso a este servicio.

   - Acceso denegado. Indica que todos los equipos tienen denegado este servicio excepto aquellos que están indicados en la lista (habrá que indicar la dirección IP de dichos equipos).

   - Máximo uso de la red. Si marca Limitar el uso de la red por todos los servicios de Internet en este equipo, deberá indicar el ancho de banda máximo que podrán utilizar los equipos para utilizar este servicio.

La utilidad que incorpora Windows NT para acceder a un servidor FTP es Microsoft Internet Explorer con la dirección ftp://nombre de su equipo/.

4.8. SERVICIO DE ACCESO REMOTO (RAS)

El servicio de acceso remoto (RAS) proporciona acceso remoto a la red a usuarios y administradores que se encuentran en distinta ubicación del lugar en donde se encuentra el servidor, así como permite también conectarse con Internet.

Podrán conectarse telefónicamente para compartir archivos e impresoras, correo electrónico y acceso a base de datos SQL de la misma manera que si estuvieran conectados directamente a la red.

Hay don métodos de acceso remoto:

- **Con control remoto.** Es el mas antiguo de los dos. Se puede conectar a la red para utilizar sus recursos a través de un software especial que hace que la computadora remoto duplique la pantalla, el teclado y el ratón de la computadora local, pero los programas se ejecutan en la computadora local.

- **Con nodos remotos.** Esta tecnología hace que una computadora remota se conecte a través de un módem, a un servidor de acceso remoto. De esta manera los programas se ejecutan en la computadora r5emoto transfiriéndose a través de la red.

4.8.1. METODOS DE COMUNICACIÓN DE RAS

Los métodos de comunicación usados por RAS son:

- **Módem analógico.** RAS soporta una gran variedad de módem que pueden ser configurados para soportar llamadas entrantes y salientes a través de la red telefónica conmutada.

Utiliza tres tipos de protocolos de módem:

SLIP. El Protocolo Internet de Línea Serie es un protocolo antiguo desarrollado para el entorno UNIX. Opera sin control de errores, control de flujo o seguridad, pero consigue un buen rendimiento con pequeños bloques de datos. RAS soporta SLIP para llamadas salientes permitiendo acceder a equipos UNIX e Internet.

PPP. El Protocolo Punto a Punto es un protocolo SLIP mejorado con control y recuperación de errores. RAS soporta PPP para llamadas salientes y entrantes.

Protocolo RAS. El protocolo RAS esta desarrollado por Microsoft para soportar NetBIOS en todas las versiones RAS.

- **Módem Nulo.** Es un cable que conecta dos computadoras usando sus puertos serie RS232C. De esta manera, se puede conectar una computadora a un a red usando RAS y sin necesidad que adaptador de red.

- **RDSI**. La Red Digital de Servicios Integrados. Es lo mas avanzado actualmente en comunicaciones digitales. Utiliza dos routers y una línea telefónica digital para enviar los datos a 64Kb/seg.

- **X25.** Este método lento pero eficaz permite conectarse a una red utilizando dos routers y un sistema basado en paquetes que viaja a través de la red telefónica se puede utilizar para distancias cortas y poco volumen de datos.

4.8.2. INSTALACION DEL SOFTWARE DE RAS

Para instalar el software RAS se deben seguir los siguientes pasos:

1. Ejecute el icono **Red** de **Panel de control**.

2. Marque **Servicios** y Después **Agregar**

3. De la lista de servicios disponibles, seleccione **Servicio de acceso remoto** y marque **Aceptar.**

4. Introduzca el CD-ROM de la instalación de Windows NT, escriba la ubicación **D:\I386** y marque **Continuar.**

5. Cuando se haya copiado los archivos se mostrará una pantalla indicándole los Dispositivos correspondientes de RAS.

6. Marque **Instalar Módem** o **Instalar Pad x25.**

7. Si ya ha instalado el módem marque **Aceptar** y verá la pantalla Instalación de acceso remoto.

8. Puede **Agregar** otro dispositivo para RAS.

9. Marque **Continuar**.

10. Si tiene instalado el protocolo **NetBEUI**, le preguntará si desea permitir el acceso a clientes remotos de **NetBEUI** a Toda la red o Solo este equipo.

11. Si tiene instalado el protocolo **TCP/IP**, le preguntará si desea Permitir a los clientes **TCP/IP** remotos acceder a toda la red o solo este Equipo. Fig. 4.16.

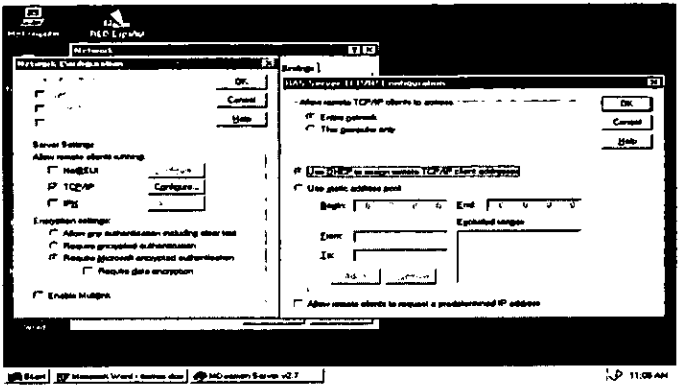


Fig. 4.16 Configurando Acceso Remoto (RAS).

12. Si tiene instalado el protocolo **IPX**, le Preguntará si desea permitir a los clientes IPX remotos acceder a toda la red o solo este equipo.

Indique si desea **Asignar Números de Red Automáticamente o Asignar Números de Red.**

13. Continuará la instalación y al cabo de un momento le preguntará si desea activar la propagación de multidifusion NetBIOS. **Marque NO**, a no ser que desee lo contrario.

14. Mostrará un mensaje que ha terminado la Instalación, **marque Aceptar**.

15. Marque cerrar para salir del icono red.

16. Si tiene instalado el protocolo IPX/SPX y no le a asignado un número de red, le mostrará un mensaje diciéndolo.

17. Cuando se le indique confirme que desea reiniciar la computadora

4.9. INSTALACION DEL CORREO ELECTRONICO (Mdaemon)

MDaemon es diseñado para administrar cualquier número de cuentas de usuarios individuales y es ademas complementado con un grupo de herramientas para administrar cuentas y formatos de mensajes, MDaemon hace posible proveer cuentas de e-mail para una completa LAN con un pequeño mailbox ISP POP3 esto hace posible proveer coreo electronico a una red entera con una fracción del costo normalmente asociado para hacer esto.

El proceso de instalación pedirá alguna información básica tal como el nombre de la compañía para registrar, el directorio raíz donde se llevara acabo la instalación, en este

directorio es donde se crearán las carpetas que serán usadas por MDaemon, además el proceso de instalación provee un wizard que lleva paso a paso en la configuración, y que puede ser usado como guía en los escenarios mas comunes de configuración.

Una vez hecha la instalación de MDaemon se procederá a configurar el dominio primario en la pantalla de **Primary Domain Configuration**. Fig. 4.17.

Que se muestra a continuación:

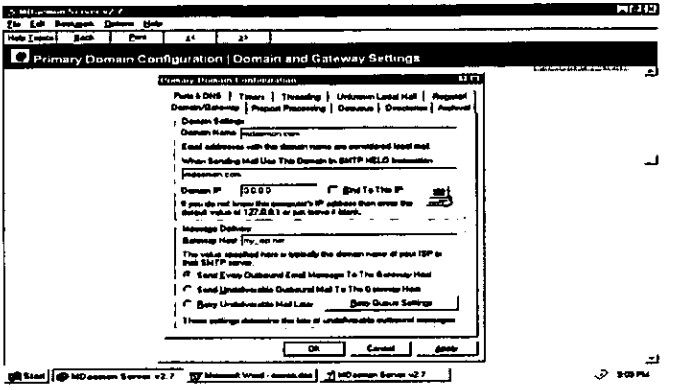


Fig. 4.17 Configuración del dominio primario.

Aquí se deberá de introducir el nombre del dominio primario, este es el nombre del dominio que las cuentas de usuario usaran para sus cuentas de correo electrónico, comúnmente el valor introducido aquí será el nombre del dominio que corresponde al que el servidor de DNS resuelve para la dirección IP o alias de la maquina local, alternativamente se podría escoger un dominio ficticio.

Dentro de la ventana de **Primary Domain Configuration** existe la opción de configuración de puertos y DNS . Fig. 4.18.

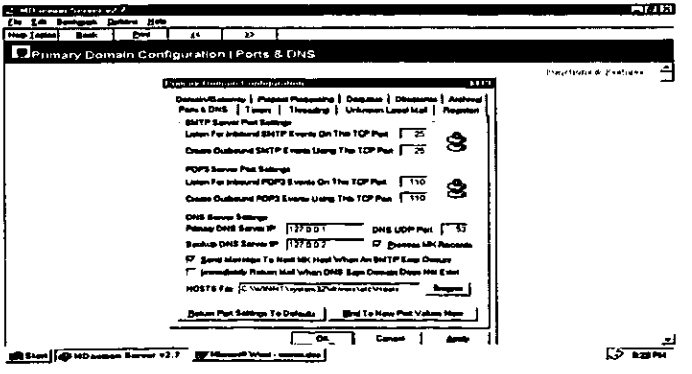


Fig. 4.18 Configuración puertos y dns.

Aquí se deberá configurar en la parte de **SMTP Server Port Setings** en la opción de **Listen For Inbound SMTP Events On This TCP Port** el puerto por el cual se llevara a cabo el monitoreo de las conexiones de entrada de los clientes de SMTP, en la opción de **Create Outbound SMTP Events Using This TCP Port** se deberá especificar el puerto que se usara cuando se envié correo a otros servidores de SMTP.

En la sección **POP3 Server Port Settings** se especificaran los puertos que tendrán la misma función que en la sección anterior solo que ahora estos puertos serán utilizados para POP3 en lugar de SMTP.

En la sección siguiente **DNS Server Settings** en la opción de **Primary DNS Server IP Address** se deberá introducir la dirección IP de del servidor DNS que se desee que MDaemon consulte para resolver direcciones de hosts remotos.

La opción **Backup DNS Server IP Address** es para dar una dirección IP de algún servidor secundario de DNS, es importante resaltar que este valor es opcional.

La opción **Host File** es para que MDaemon resuelva primero una dirección a través del archivo de Windows HOSTS, este archivo contiene la dirección IP del dominio en cuestión y MDaemon no necesitará consultar al servidor DNS, aquí se deberá especificar la ruta completa del archivo HOSTS del ambiente Windows en el que se este trabajando.

Otra opción que se considera importante dentro de esta pantalla de configuración es la de **Timers** que aparece en la siguiente pantalla (Fig. 4.19):

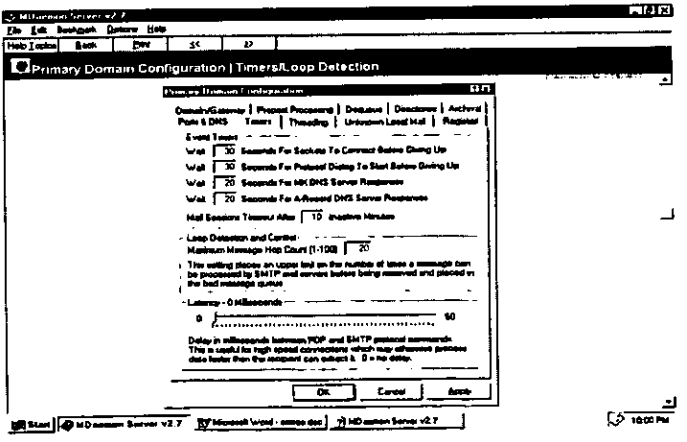


Fig. 4.19 Configuración del tiempo de espera.

Debido a que en esta opción se configura el valor del tiempo de latencia o Latency, que es la espera en milisegundos entre los protocolos POP y SMTP, esta opción es usada para cuando se tienen conexiones de alta velocidad en el que los datos llegan mas rápido de lo que el recipiente puede extraerlos.

Una vez configurado lo anterior se puede proceder a crear las cuentas de usuario que residirán en nuestro servidor integrándolas al dominio en el que nos encontramos de la manera siguiente: en el **menú principal de MDaemon** ir a la opción de **Accounts** después seleccionar la opción de **New** donde nos aparecerá la siguiente pantalla (Fig. 4.10):

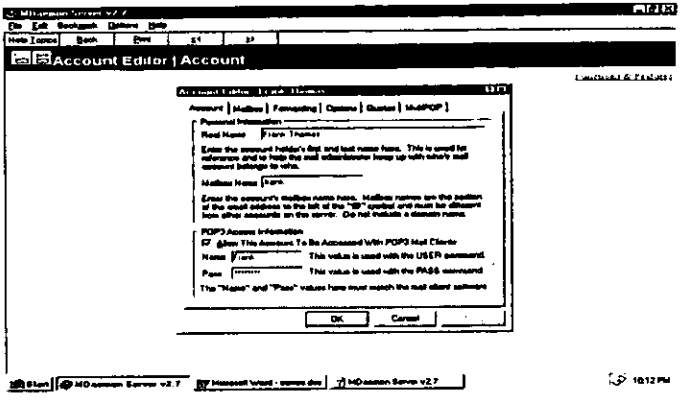


Fig. 4.20 Creación de cuentas de correo.

En la opción de **Real Name** se deberá introducir el nombre completo del usuario al que se le generara la nueva cuenta de correo electrónico.

La opción de **Mailbox Name** es para especificar un nombre único para el mailbox para el usuario, aquí se deberá especificar el nombre que se le dio en la parte derecha de la arroba (@) en la cuenta del usuario, no deberá darse un nombre parecido al de ningún host, este nombre del mailbox deberá ser único y no deberá contener espacios en blanco.

La opción de **Allow This Account To Be Accessed With POP3 Mail Clients** es solo para especificar si estará o no permitido el acceso con POP3.

La opción de **Name** es para especificar el nombre que tendrá la sesión de POP, en este caso deberá ser el nombre del usuario.

La opción **Pass** es para especificar el password de la cuenta del usuario de correo electrónico.

En la pestaña de **Mailbox** que se ve en la pantalla mostrada a continuación (Fig. 4.21):

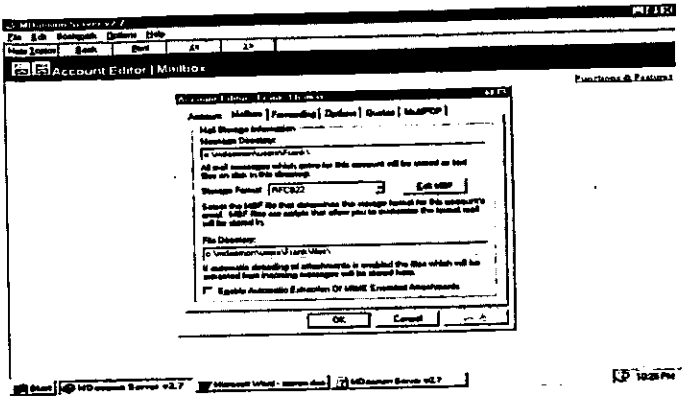


Fig. 4.21 Etiqueta del mailbox.

Se deberá especificar en el cuadro de **Message Directory** el directorio donde residirán los mensajes de correo destinados para este mailbox en especifico.

En la opción de **Storage Format** permite pegar un archivo MBF al directorio del mailbox, el cual provee un método de sistema de compatibilidad de correo el cual puede ser usado para integrar otro software de correo con **MDaemon Server 2.7**.

La opción de **File Directory**: aquí se deberá introducir el directorio de entrada donde se colocaran los archivos que estarán contenidos dentro de un mensaje de entrada en la cuenta de correo estos archivos se conocen comúnmente como archivos atachados al correo.

Para editar alguna cuenta de correo que ya exista se deberá seleccionar la opción en el menú principal de **Accounts** después la opción de **Edit** y aparecerá la siguiente pantalla (Fig.4.22):

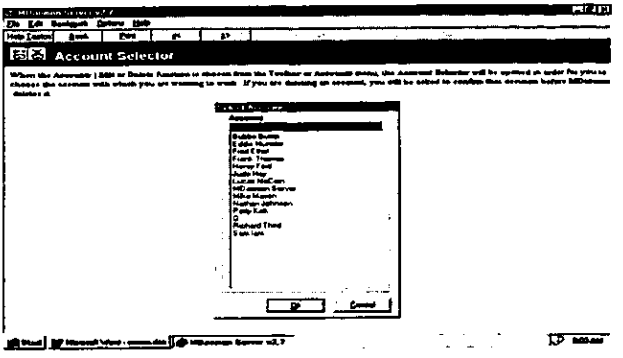


Fig. 4.22 Edición de cuentas de correo.

Aquí se deberá seleccionar la cuenta que se desee editar dando doble click sobre esta, después de dar doble click nos aparecerá la pantalla en la cual dimos de alta la cuenta, permitiéndonos editar los datos referentes a la cuenta seleccionada.

Para borrar una cuenta se deberá ir al **menú principal de MDaemon** y en la opción de **Account** se deberá seleccionar la opción **Delete**, una vez seleccionada aparecerá la pantalla anterior donde tendremos la lista de cuentas existente, de la que se deberá seleccionar la cuenta para ser borrada, después de haber seleccionado la cuenta aparecerá una pantalla de confirmación antes de ser borrada por MDaemon.

4.9.1. VISUALIZACION DEL CORREO ELECTRONICO

Para entrar en el correo de Windows y ver las carpetas de un usuario ejecute programas y seleccione Internet Mail, se mostrarán las cuatro carpetas que se crearon por defecto (Fig. 4.23):

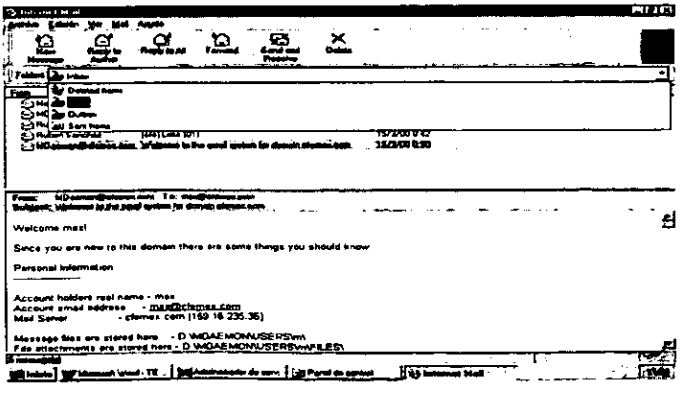


Fig. 4.23 Carpetas de usuario en Internet Mail.

- **Bandeja de entrada.** Es donde esta el correo que recibe el usuario.

- **Bandeja de salida**. Es donde se encuentra temporalmente el correo enviado a otros usuarios hasta su entrega.

- **Elementos eliminados.** Contiene una copia de los mensajes eliminados.

- **Elementos enviados.** Contiene una copia de los mensajes enviados.

En caso de que haya instalado **Microsoft Outlook**, el correo de Windows parasará a denominarse **Microsoft Exchange** y le mostrará además las siguientes cinco carpetas:

- **Calendario.** Con esta utilidad podrá programar su agenda para citas, reuniones y eventos.

- **Contactos.** Con esta utilidad podrá guardar información acerca de aquellas personas o empresas con las que mantiene correspondencia.

- **Diario.** Con esta utilidad podrá registrar automáticamente las actividades siguientes: correo electrónico, documentos y bases de datos creadas, convocatorias de reunión,. ETC. O bien manualmente las actividades siguientes: tareas llevadas a cabo, citas, documentos y bases de datos que ya existen, cartas, convensiones, etc.

- **Notas.** Con esta utilidad (que es el equivalente de las notas adhesivas de papel) podrá incluir preguntas, ideas, avisos, textos, etc., que podrá tener abiertas en la pantalla mientras trabaja.

- **Tareas.** Con esa utilidad pudra llevar un seguimiento sobre aquellas ocupaciones personales o profesionales que se desee hasta su finalización.

Si vuelve a marcar otra vez el mismo icono, volverá a subir un nivel y verá las carpetas personales (que son las que se describieron anteriormente) y las carpetas compartidas de Internet Mail (son aquellas carpetas donde se guarda mensajes que pueden ser vistos por todos los usuarios).

Para retroceder, seleccione una carpeta y pulse dos veces el botón izquierdo del ratón sobre ella.

Puede crear carpetas si selecciona el lugar deseado, abre el menú **Archivo**, selecciona **Folder** y luego **Create**, indicar el nombre que desea darle y marca **Aceptar.**

También puede eliminarlas si selecciona **Delete** en **Folder.**

Si selecciona la etiqueta **Ver**, **Preview Pane** y **Split Vertically**, dividirá la pantalla en dos partes. En la parte izquierda se encontraran los mensajes recibidos, enviados o que no se han enviado (depende de la carpeta en donde estemos ubicados), descritas anteriormente y en la parte derecha el contenido de los mensajes en la carpeta que este seleccionada. Fig. 4.24.

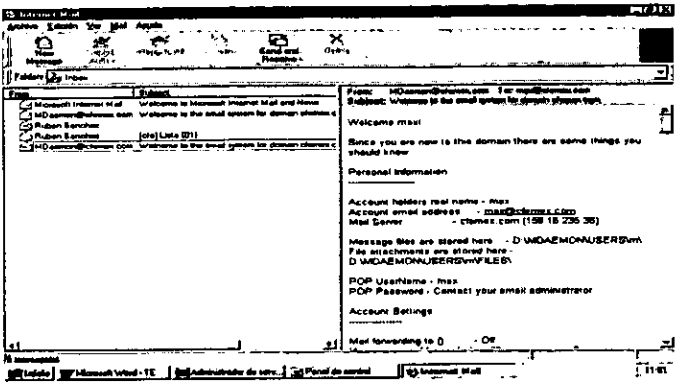


Fig 4.24 Visualización del Inbox.

4.9.2. CONFIGURACION DEL INTERNET MAIL PARA ENVIAR Y RECIBIR CORREO ELECTRONICO

Para poder enviar y recibir correo es necesario configurar el Internet Mail. Abrir **Internet Mail**, seleccionar **Mail** y después **Options** (Fig. 4.25), marque la etiqueta **Server** e introduzca los datos correspondientes al servidor del correo y a la cuenta de correo del usuario.

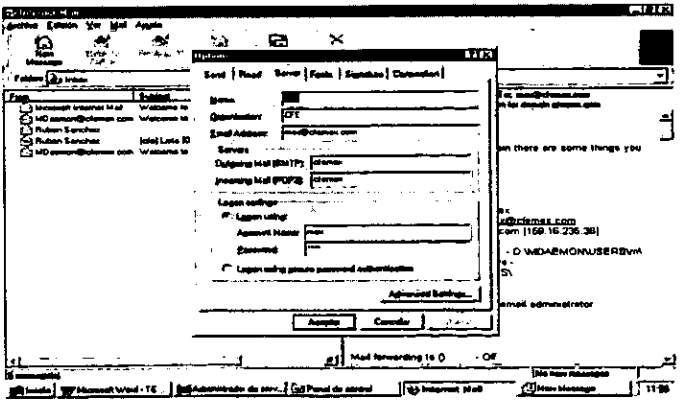


Fig. 4.25 Configuración del correo electrónico.

- En el apartado Name introduzca el nombre completo del usuario o el alias.

- En Organización introduzca el nombre del departamento o de la empresa a la que pertenece.
- Introducir la dirección de correo del usuario previamente creada con el MDaemon, la cual esta definida por nombre de usuario@nom_dominio.com
- En servidor de correo saliente (SMTP) introducir la dirección del servidor de correo.
- En servidor de entrada de correo (POP3) introducir la dirección del servidor de correo.
- En nombre de la cuenta de correo introdir la que se creo con el MDaemon.
- En password introducir la contraseña asignada a esta cuenta de correo en el MDaemon.
- Pulsar la tecla de Aceptar para tomar la s configuraciones asignadas en el Internet Mail.

De esta forma quedará configurado el Internet Mail para enviar y recibir correo en la Intranet.

4.9.3. ENVIO DE CORREO ELECTRONICO

Para iniciar el envío de correo electrónico seleccionar el botón de **Nuevo Mensaje** (Fig. 4.26), y le mostrará la siguiente pantalla.

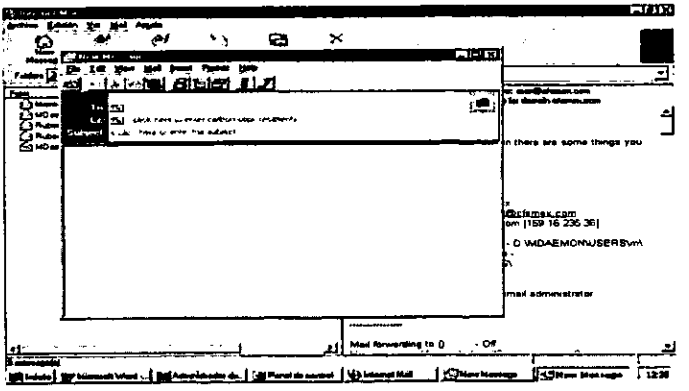


Fig. 4.26 Envio de correo electrónico.

En el apartado **To** deberá indicar el destinatario o destinatarios del mensaje. Puede tomar las direcciones que tenga guardadas en el libro de direcciones dando un click con el mouse

en la etiqueta que esta delante del **To** y mostrará las direcciones que tiene actualmente o crear nuevas tarjetas con las direcciones de las personas con las que intercambia constantemente información pulsando el botón de nuevos contactos y agregar la información de correo del nuevo contacto, pulsar el botón Add y se agregará la nueva dirección a su lista (Fig. 4.27). Seleccione la cuenta de correo y presione To->, se agrega la dirección a donde se enviara el mensaje, presionar Ok y aparecerá en el **To.**

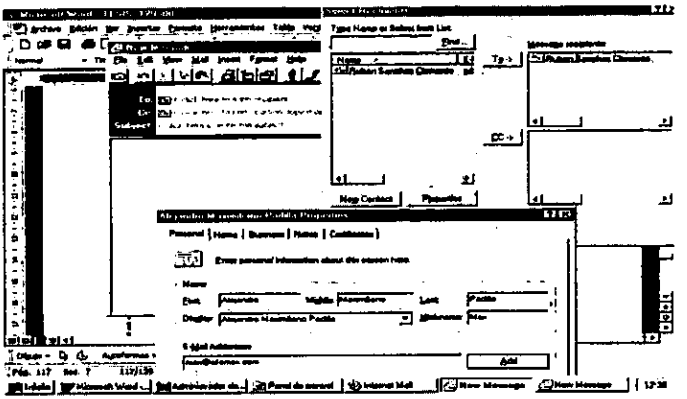


Fig. 4.27 Creación de nuevos contactos de correo.

En el apartado Cc (con copia) indicará el usuario o los usuarios a los que, aunque no sean receptores del mensaje, desea enviárselo para que tengan conocimiento de su envío (siguiendo el mismo proceso indicado en el párrafo anterior pero marcando Cc en lugar de **To**).

En el apartado **Asunto** deberá indicar el titulo que desea dar al correo que va a enviar.

En el cuerpo central deberá escribir el texto que desea que incorpore el correo.

Puede insertar un archivo. Para ello presione el icono con un dibujo de un clip, indique el nombre del archivo que desea enviar y marque **Aceptar** (si abre el menú Insert, podrá insertar también mensajes y objetos. Entre estos últimos se encuentran: archivos de sonido, imágenes, documentos, etc.).

Para enviar el correo, marque el primer icono de la izquierda y volverá a la bandeja de entrada, el mensaje tardara en entregarse el tiempo que este indicado en la configuración del servidor de correo). Le mandará un mensaje de que se enviará hasta que pulse el botón Send and Receive.

4.9.4. LECTURA DE CORREO RECIBIDO

Para leer el correo recibido, deberá estar situado en la Bandeja de entrada. Una vez situado en ella, verá la lista de los mensajes recibidos.

Si se sitúa sobre uno de ellos y pulsa una vez el botón izquierdo del ratón, verá la pantalla donde se muestran los datos del mensaje recibido.

Si dentro del cuerpo del mensaje ve un icono con un nombre debajo, indica que tiene insertado un objeto. Si se sitúa sobre dicho objeto y pulsa el botón derecho del ratón, verá su menú contextual. Podrá abrirlo, imprimirlo, hacer una revisión rápida, guardarlo en un directorio (con el mismo o con otro nombre) o cambiar su nombre dentro del mensaje.

4.9.5. AGENDA DE DIRECCIONES

Para introducir nuevos miembros en la agenda presionar nuevo mensaje y seleccionar el sexto botón de izquierda a derecha, aquí se pueden editar o crear nuevos contactos de correo (Fig. 4.28).

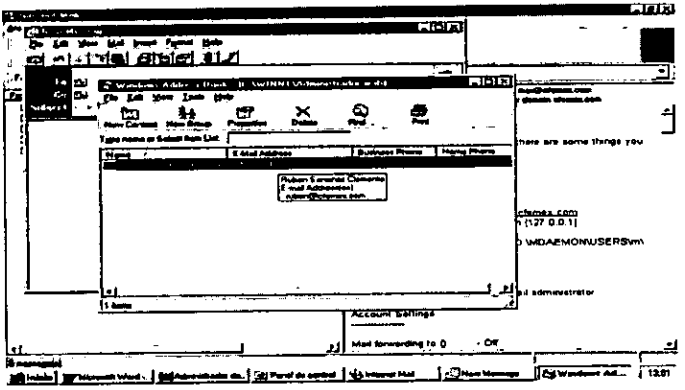


Fig. 4.28 Agenda de direcciones.

4.10 SERVIDOR PROXY

CONCEPTOS SOBRE MICROSOFT PROXY SERVER.

Se entiende por servidor proxy (apoderado) A una computadora que se configura como servidor y actúa como apoderado o proxy para otros clientes en Internet.

Microsoft Proxy Server es una manera fácil y asegura de proporcionar acceso a Internet a cada estación, permitiendo un control de acceso que se encuentra en manos del administrador de la red.

Proporciona soporte a todos los protocolos de Internet incluyendo los siguientes:

- HTTP
- FTP
- TCP/P
- IRC
- MAIL
- NEWS

Incorpora los tres servicios siguientes:

- Web Proxy
- WinSock Proxy
- Socks Proxy

Respecto a su funcionamiento, el usuario no percibe ninguna diferencia entre llamar directamente a Internet o llamar a través de un servidor proxy. De la misma manera, un servidor Web de Internet no sabe si es llamado desde un cliente o un servidor proxy.

Entre los beneficios de su utilización se encuentran:

- Protege contra el acceso de usuarios no controlados.
- Oculta la identidad real del usuario.
- Es fácil de administrar y configurar.
- No requiere el uso de direcciones validas de Internet para cada estación.
- Es mas barato que otros firewalls basados en hardware.
- Permite monitorear la utilización de la red.

Entre sus inconvenientes se encuentran:

- Es necesario realizar una administración adicional.
- Requiere algún aprendizaje para el usuario final.
- Es necesario utilizar software que pueda llamar al servidor proxy.
- No proporciona protección contra ataques de usuarios internos de la red.

4.10.1. SEGURIDAD

Normalmente, un servidor proxy debe tener dos tarjetas de red:

- La primera es una tarjeta con una dirección real y legal de Internet que es la que le proporciona el acceso al exterior.

- La segunda es una tarjeta con una dirección interna que no proporciona acceso a Internet y es la que se comunica con la red interna.

Dentro de la clase A están reservadas las direcciones que van desde 10.0.0.0 hasta 10.255.255.255 y que no pueden usarse para acceder a Internet.

Dentro de la clase B están reservadas las direcciones que van desde 172.16.0.0 hasta 172.31.255.255 y que no pueden usarse para acceder a Internet.

Dentro de la clase C están reservadas las direcciones que van desde 192.168.0.0 hasta 192.168.255.255 y que no pueden usarse para acceder a Internet.

Pero no hay ningún problema para que dichos rangos de direcciones de las clases A,B Y C que están reservadas puedan utilizarse para asignarlas a estaciones de redes internas sin acceso a Internet.

Cada cliente necesite un acceso a Internet, enviara un requerimiento al servidor proxy que comprobara la dirección IP interna. Si es valida, enviara dicho requerimiento a Internet con su dirección IP externa.

Cuando reciba contestación, la dirigirá a la estación que la había solicitado.

Desde esta manera se establece una barra de seguridad (firewall) entre su red e Internet, pudiendo controlar tanto las estaciones que van a realizar acceso al exterior como los usuarios autorizados a ello.

De la misma manera, se bloqueara el acceso a la red interna a todas las direcciones IP externas que no estén autorizadas en el servidor proxy.

4.10.2. ADMINISTRACION

Microsoft Proxy Server proporciona los siguientes aspectos para su administración:

- Se administra con el Internet Service Manager que permite tener un único punto de administración del servidor proxy para toda la red interna.

- Las cuentas de los usuarios no deben volver a crearse una vez instalado el servidor proxy, pero deberá asignar limitaciones de acceso a Internet para aquellos usuarios que lo desee, asignando permisos.

- Incorpora Auto-Dial para poder realizar conexiones telefónicas (módem o RDSI) para acceder a Internet.
- Incorpora un monitor de rendimiento del servidor proxy (Monitor Microsoft Proxy Server Perfomance) para monitorear el estado del servidor proxy de la red.
- Genera mensajes de alerta cuando se produce un intento de acceso no autorizado.
- Puede examinarse el estado actual del servidor proxy utilizando una consola SNMP.

4.10.3. INSTALACION DEL SERVIDOR PROXY

Para llevar a cabo la instalación, siga los pasos siguientes:

1. Ejecute el archivo comprimido (**msp2i.exe**).
2. Le preguntará si desea instalar Microsoft Proxy Server 2.0 Version en su sistema **Conteste SI**.
3. Le mostrará la licencia de uso. Proceda a su lectura y **marque Yes** para aceptarla.
4. Procederá a la descompresión de los archivos y le mostrará una pantalla de bienvenida. **Marque Continue**. Fig. 4.30.

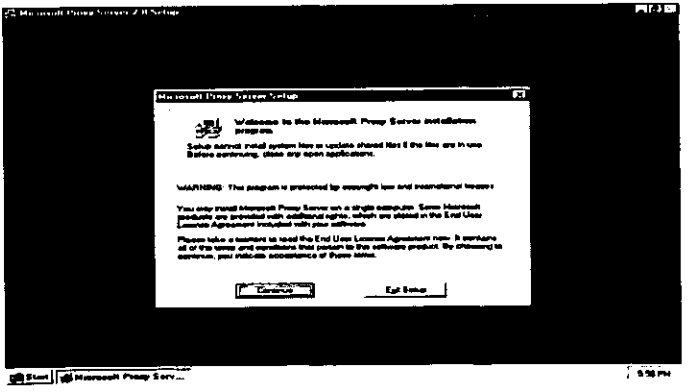


Fig. 4.30 Instalación del Proxy Server 2.0.

5. Le pedirá que introduzca la clave que se encuentra en el. Escríbalos y **marque OK**. Fig. 4.31.

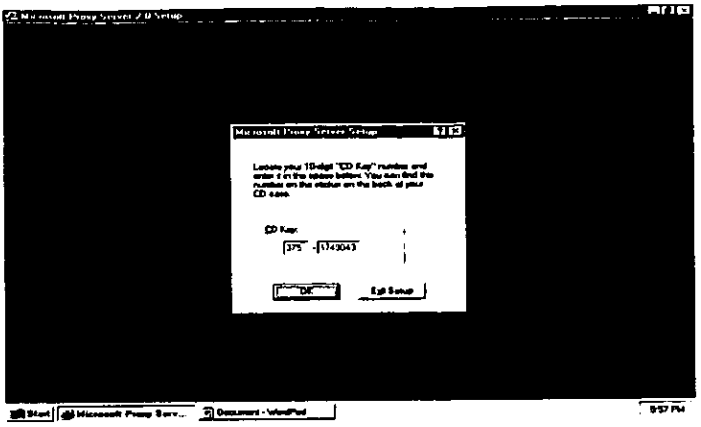


Fig. 4.31 N° de licencia.

6. Le mostrará el número de identificación del producto que deberá apuntarlo por si desea llamar al servicio de soporte técnico de Microsoft. Anote el número y **marque OK**.

7. En la pantalla que aparece puede cambiar la carpeta donde se va a instalar el producto, marcando **Change Folder**, indicando la deseada y **marcando OK**.

Cuando desee continuar con la instalación, marque Instalation Options.

8. Puede seleccionar las opciones que desea instalar (por defecto son todas). **Marque Continue.** Fig. 4.31.

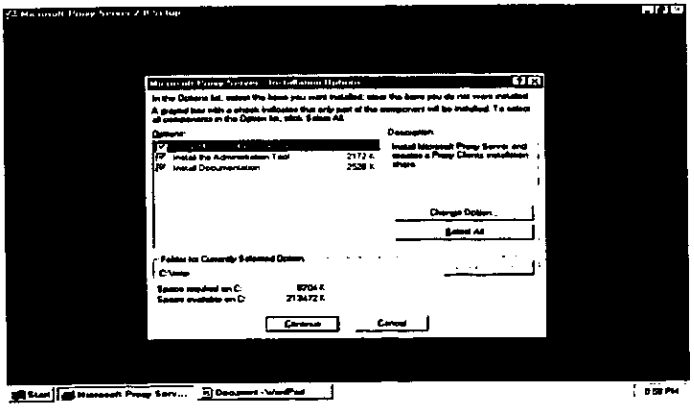


Fig. 4.31 Opciones de instalación.

9. Si no ha instalado una partición NTFS en la computadora, le mostrará un mensaje indicándole que no puede habilitar el uso de cache. Marque Aceptar.

10. Le mostrará una pantalla donde podrá habilitar el uso de cache (recuerde que solo puede hacerlo si tiene una partición NTFS) si marca Enable Caching. En este caso, deberá indicar el tamaño máximo que desea utilizar en Maximum Size (este valor debe ser como mínimo de 100 MB mas medio MB por cada servicio cliente proxy). Fig. 4.32.

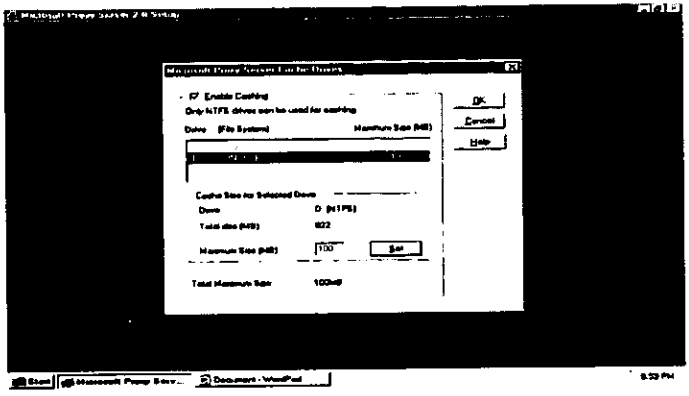


Fig. 4.32 Tamaño del cache para los servicios de la Intranet.

11. Cuando haya finalizado, **marque OK**. Le mostrará la siguiente pantalla.Fig. 4.33.

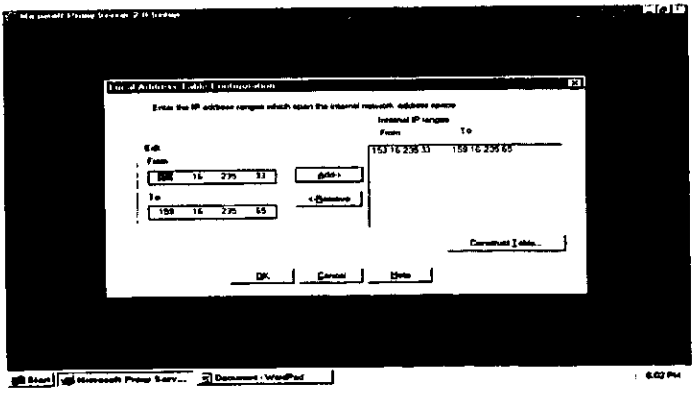


Fig. 4.33 Identificación de IP's internos.

En ella puede identificar las direcciones IP internas y excluir direcciones IP externas de su red. Esta información se mantiene en una Tabla de direcciones locales (LAT) que es usada por clientes WinSock Proxy, Web Proxy y Socks Proxy.

En el bloque **Edit**, hay las siguientes opciones:

- **From.** Indica la primera dirección IP interna que desea añadir.
- **To.** Indica la última dirección IP interna que desea añadir.

Cuando haya escrito ambas, marque **Add** y se añadirán a la lista de **Internal IP Ranges**. Puede volver a repetir el proceso si hay más intervalos (en el caso de indicar una única dirección, escriba la misma dirección en **From** y **To**, marque **Add**).

Si desea quitar una dirección interna, selecciónela de la lista de **Internal IP Ranges** y marque **Remove**. Cuando haya finalizado marque **Construct Table** verá la siguiente pantalla. Fig. 4.34.

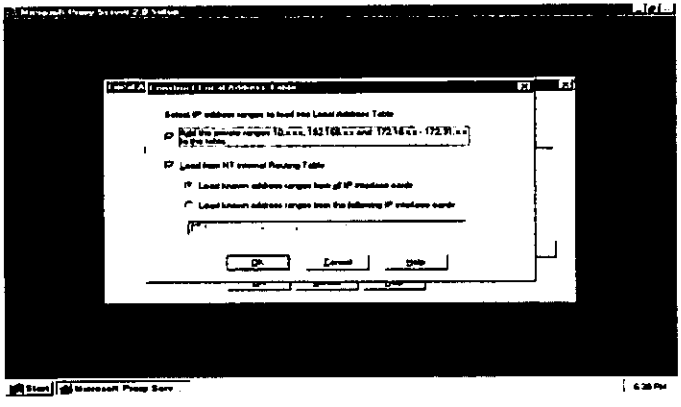


Fig. 4.34 Construcción de tablas de direcciones locales.

- **Add the private ranges...** Si marca esta opción puede añadir a la tabla tres rangos de direcciones IP definidas como privadas que pueden ser usadas en una red privada que no esta conectada a Internet.

- **Load from NT internal...** Si marca esta opción, especificara cuando cargara las direcciones IP a través las tarjetas de red del servidor. Deberá indicar una de las dos opciones siguientes:

- **Load Known address ranges from all IP...** Marque esta opción si no conoce que tarjetas de red están conectadas a la red interna y cuales lo están a Internet.

- **Load Snown address ranges from the following**... Marque esta opción si conoce que tarjetas de red estan conectadas a la red interna. Debera eliminar las tarjetas que aparecen en la parte inferior que estan conectadas a Internet y por tanto, no pertenecen a a la red privada.

Cuando haya finalizado, **Marque OK**.

12. Le mostrará un aviso indicándole que ya se han cargado los rangos de direcciones **IP** en la **LAT.** Marque **OK**.

13. Verá que en función de las opciones indicadas en la construcción de la tabla se han ampliado las direcciones indicadas en **Internal IP Ranges**. Cuando desee, marque **OK**. Verá una pantalla parecida a la siguiente. Fig. 4.35.

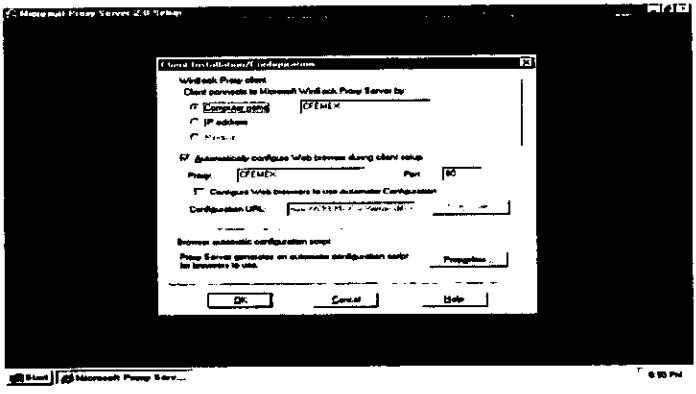


Fig. 4.35 Configuración del Winsock Proxy Client.

En ella puede ver las siguientes opciones:

En el bloque WinSock Proxy client se indica como se van a conectar al servidor WinSock Proxy los clientes WinSock Proxy. Pueden hacerlo de tres maneras:

- **Computer name**. Acceder por medio del nombre de la computadora.
- **IP adrdress**. Acceder por medio de la dirección IP.
- **Manual**. Indica que no se sobrescriba el archivo mspclnt.ini. En este caso, deberá editar manualmente el archivo e indicar el dato en la sección correspondiente.

- **Automatically configure Web browser during client setup**. Si marca esta opcion, esta indicando que realice automáticamente la configuración del navegador Web de los clientes proxies haciéndole que apunte al servidor proxy. En este caso deberá indicar el nombre del computador que actua como servidor proxy y el número de puerto que utiliza el cliente para conectarse con el.

- **Configure Web browsers to use Automatic Configuration**. Si marca esta opción, tendrá que indicar el valor que va a utilizar para configurar el navegador Web usando una especificación Javascript (en este caso, deberá indicar la ubicación de dicha especificación).

Browser automatic configuration script. Si marca **Properties**, deberá indicar como se va a actualizar el navegador **Web** de los clientes **proxies**. Cuando haya finalizado, marque OK.

14. Verá la siguiente pantalla (Fig. 4.36):

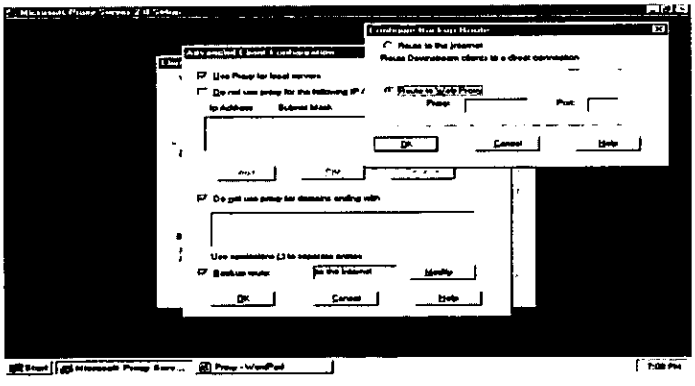


Fig. 4.36 Uso del servidor proxy.

En ella se ven las siguientes opciones:

- **Use Proxy for local servers**. Si marca esta opción, indica que el navegador de los clientes proxies deberá utilizar el servidor proxy para comunicarse con los sitios Web internos (un sitio Web se considera interno cuando en su dirección no figura ningún punto, por ejemplo http://cfemex/.

- **Do not use proxy from the**... Si marca esta opción, deberá indicar las direcciones IP de los clientes que no van a utilizar el servidor proxy para comunicarse con los sitios Web internos. En este caso, deberá indicar su dirección IP y sus mascaras de subred. Para ello, marque Add, escriba ambos datos, marque OK y se añadirá a la ventana inferior. Repita el proceso con cada una de las direcciones IP que desee. Si selecciona una dirección y marca Remove, la eliminara; y si marca Edit, podrá modificarla.

- **Do not use proxy for domains ending with**. Si marca esta opción indicará que no usaran el servidor proxy aquellos dominios TCP/IP que acaben en un valor que deberá especificar en la ventana inferior (si desea especificar varios, deberán ir separados por punto y coma).

- **Backup route**. Si marca esta opción, indica que ruta alternativa van a utilizar los clientes proxies si el servidor proxy no esta disponible. En este caso, marcando Modify, podrá seleccionar entre encaminarse directamente a Internet o utilizar otro servidor proxy. Cuando haya finalizado, marque OK para volver a la pantalla Advanced Client Configuration.

15. Marque OK para volver a la pantalla Client Installation/Configuration.

16. Cuando haya finalizado, marque OK y verá la siguiente pantalla (Fig. 4.37):

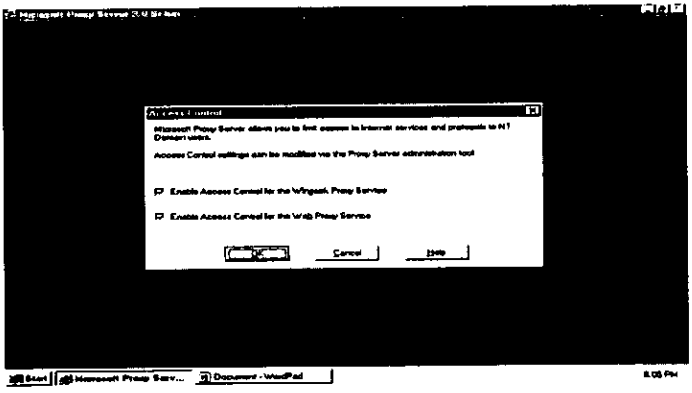


Fig. 4.37 Habilitando el control de acceso.

En ella se ven las siguientes opciones:

- **Enable Acces Control for the Winsock Proxy Service**. Si marca esta opción, únicamente podrán utilizar ese servicio los clientes que tienen otorgados permisos.

- **Enable Acces Control for the Proxy Service**. Si marca esta opción, únicamente podrán utilizar ese servicio los clientes que tienen otorgados permisos.

Cuando haya finalizado, **marque OK**.

17. Se procederá al copiado de los archivos y a su instalación.

18. Le mostrará un mensaje diciéndole que puede utilizar las herramientas de administración para poner en funcionamiento los filtros de seguridad. Cuando lo haya leído, **marque OK**.

19. Al cabo de un momento le mostrará un aviso indicándole que ha finalizado el proceso de instalación. **Marque OK** y compruebe en el menú Programas del botón Inicio, que hay una nueva opción llamada Microsoft Proxy Server.

20. Si ejecuta la utilidad Administrador de servicios Internet, que esta incluida dentro de Microsoft Internet Server (Común), que forma parte del menú Programas del botón Inicio, verá que, además de los servicios que tenia desde que instalo IIS, se encuentran tres servicios nuevos:

    - Socks Proxy
    - WinSock Proxy
    - Web Proxy

21. A esta misma pantalla puede llegar desde utilidad **Internet Service Manager**, que esta incluida dentro de **Microsoft Proxy Server (común)**, que forma parte del menú Programas del botón Inicio.

4.11. CONFIGURACION DE MICROSOFT INTERNET EXPLORER

Para configurar Microsoft Internet Explorer de manera que los usuarios se conecten a nuestra Intranet se deberá ir al **Menú Principal** y seleccionar la opción de **View → Option → Connection** y nos aparecerá la pantalla mostrada a continuación (Fig. 4.38):

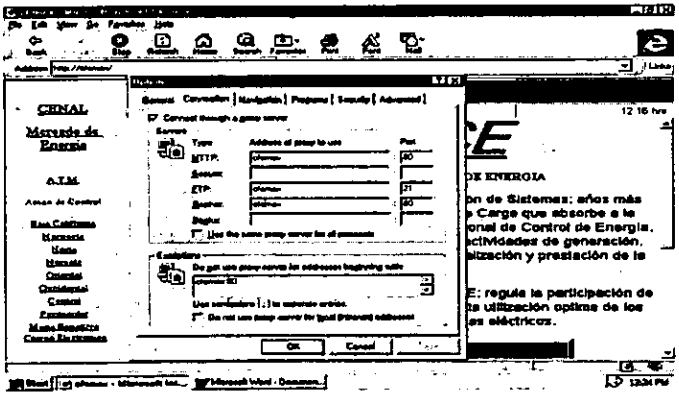


Fig. 4.38 Configuración del Internet Explorer 3.02.

Aquí se deberá especificar la dirección o alias del servidor donde se encuentra alojada la pagina principal de nuestra Intranet y el número de puerto correspondiente al servicio de HTTP, de igual forma se configurará la opción del servicio FTP y GOPHER.

En el **Menú Principal →View → Option → Navigation** se deberá configurar en el campo de **Address** (como se ve en la Fig. 4.39) el nombre de la pagina Principal o Home de nuestra Intranet (*http://cfemex*), de tal forma que los usuarios al entrar a Microsoft Internet Explorer entren siempre a la página principal de la Intranet (previamente configurada en el WWW del IIS), haciendo con esto mas eficiente y rápido el acceso a la información que nos interesa consultar.

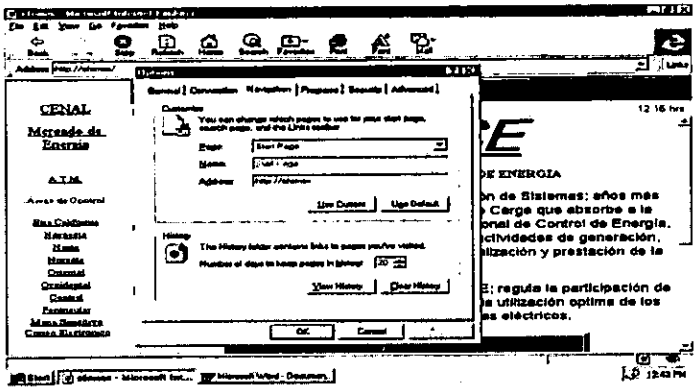


Fig. 4.39 Configuración de la pagina delnicio.

4.12. PRESENTACION DE LOS SERVICIOS EN LA INTRANET

Servicio WWW

Es el servicio que nos permite configurar la Página Principal (Fig 4.40), a través de la cual se tiene acceso a la información general del Centro Nacional de Control de Energía, este se encarga de coordinar las actividades de Generación, Conducción, Transformación, Distribución, Comercialización y Prestación de la Energía Eléctrica, además de regular la participación de cada una de las unidades generadoras y permite la optimización de los recursos de que disponen los sistemas eléctricos.

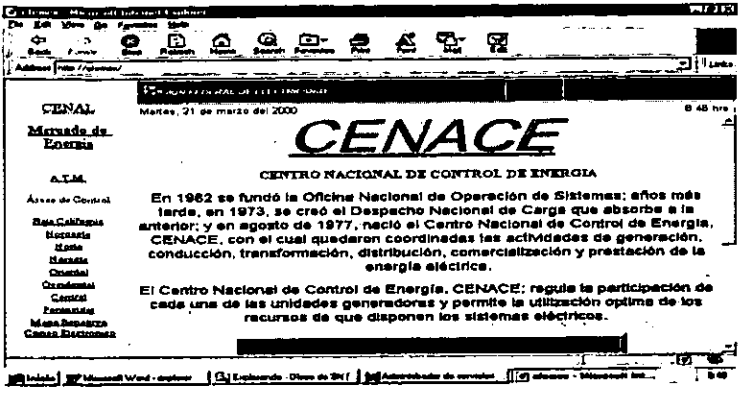


Fig. 4.40 Página Principal de la Intranet.

Servicio FTP

El objetivo de este servicio es facilitar el intercambio de información a través de las diferentes áreas de la empresa, esto se hace conectándose utilizando el Microsoft Internet Explorer, para ello en el apartado de **Address** introducir ftp://cfemex, esto hace que se despliegue la pantalla siguiente (Fig. 4.41).

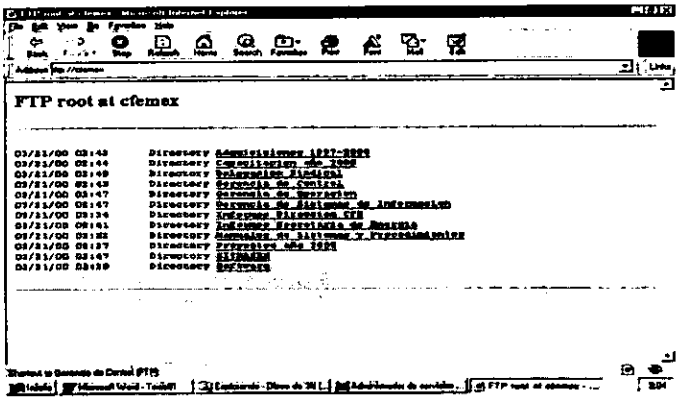


Fig. 4.41 Información disponible en FTP.

Se observa que existen varios directorios, los cuales contienen la información que se puede bajar vía ftp desde cualquier punto de la Intranet, evitando así hacer uso de otros recursos para obtener esta información.

De esta forma quedan en funcionamiento los servicios necesarios en la Intranet, la cual ya se encontrará lista para dar servicio a los usuarios del CENACE.

Capítulo V

ANALISIS DE COSTOS Y BENEFICIOS

ANÁLISIS DE COSTOS Y BENEFICIOS

5.1. RENDIMIENTO A LA INVERSIÓN PARA INTRANETS

Los medios han dejado a las pequeñas y grandes compañías creer que desarrollar Intranet es bastante fácil y barato. En su mayor parte, las declaraciones de los medios son correctas, sin embargo eventualmente las compañías deben de agregar aplicaciones Intranet avanzadas que requieren de una planeación cuidadosa y la disponibilidad de recursos y fondos.

En general, los costos de inicio de los sistemas Intranet son altos. Sin embargo, mientras añada una variedad de aplicaciones avanzadas (cosa que necesitará), la compañía podría enfrentar rápidamente costos de miles de dólares en las compras iniciales y después de esos costos continuos dar soporte de aplicaciones. Para obtener la aprobación de la administración superior para comprar aplicaciones de software costosas, debe mostrar los costos y beneficios que estos servicios proporcionan a la compañía a través del tiempo.

Para analizar el rendimiento de la inversión de una Intranet, debe hacerse un inventario de todas las actividades que se piense que se afectaran el desarrollo de la Intranet. Debe entenderse el costo asociado con la distribución de información a través de elementos tradicionales (tales como memos, catálogos y manuales), su búsqueda de información sobre el costo podría llevarlo a un territorio poco amistoso.

5.2. EL RENDIMIENTO DE LA INVERSION (ROI)

Para realizar un análisis ROI para una Intranet primero se debe evaluar los factores que afecten el ROI de cualquier inversión. Un ROI es un porcentaje de los beneficios que una inversión genera. En pocas palabras, calcula estos beneficios al dividir los ahorros en costos y ganancias generadas por la inversión, entre el costo de la inversión. La fórmula del ROI es la siguiente:

$$\frac{Ahorros + Ganancias}{Costo} = ROI$$

Costo de inversión : Cuanto dinero debe de invertir
Ahorros: Cuanto dinero ahorrará después de la inversión
Ingresos: Cuanto dinero generará la inversión

5.3. CAPITALIZACIÓN O DEPRECIACIÓN DE LOS COSTOS DE INVERSIÓN

Para entender el ROI, primero deben de entenderse los costos de inversión. El desarrollo inicial de una pieza de maquinaría, por ejemplo, obviamente es un costo de inversión. En la mayoría de los casos proyectará que la inversión durará para un número específico de años. Por esto, puede amortizar el costo de estos años al sustraer un cantidad llamada depreciación. Por ejemplo, se sabe que un automóvil de 5 cinco años vale menos que su precio original de compra, su propietario a consumido algo de la vida útil del automóvil, el automóvil ahora se ha depreciado. Hay muchos métodos disponibles para que se calcule la depreciación, tales como el de línea directa acelerado, y la suma de dígitos a través de los años.

Otro concepto importante que se necesita considerar al invertir en equipos es la capitalización. Puede capitalizar gastos que extienden la vida útil de una inversión. Capitalizar estos nuevos costos (nuevas inversiones) significa agregar a los costos al denominador de la fórmula ROI.

Debido a que la capitalización de gastos de una compañía afecta sus obligaciones fiscales, es recomendable consultar un contador público certificado o u otro profesional fiscal para realizar estos puntos. Todas las compañías deben de actualizar el hardware, tal como discos duros, memoria y varias aplicaciones de software, el concepto de capitalización afectará el costo de mantenimiento de la Intranet.

5.4. MEDICIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Es apropiado hablar acerca de algunos de los objetivos y términos que se involucran en la medición de la tecnología de la información. Debido a que las primeras formas de la tecnologías de la información fueron utilizadas para automatizar los procesos, era relativamente sencillo calcular los beneficios financieros. Por ejemplo, una compañía podía tener instalado un dispositivo electrónico para ejecutar en forma remota una máquina, o podría tener instalada una PC para reemplazar el diario de un libro contable. Hoy en día, la tecnología de la información proporciona administración con datos que puede usar para tomar decisiones estratégicas. Estos beneficios no solo son más avanzados, sino que también son más difíciles de establecer.

Debido a que la inversión financiera de una compañía para una herramienta de tecnología de la información puede ser alta, realizar un análisis de costo beneficio es importante. Las razones por las cuales las compañía fallan en su intento para medir las herramientas de la tecnología de la información influye:

- La estimación exacta de los costos y los beneficios es difícil.
- Los costos verdaderos y beneficios del sistema podrían no ser claros por algún tiempo.La evaluación del sistema podría requerir meses o años de estudios cuidadosos después de la implementación inicial

- Los costos por no proceder por una inversión en tecnología de la información son igualmente difíciles de estimar.

5.5. CONCEPTOS Y TERMINOLOGIA

Hablando matemáticamente, calcular un ROI es sencillo, sin embargo el proceso de identificar costos y beneficios es difícil después de conocer sus costos y beneficios, calcular un ROI involucra más que simples sumas, restas y divisiones. Para su mayor entendimiento se mencionarán algunas definiciones como son costos inflexibles, costos flexibles y beneficios.

Costos inflexibles

Para una Intranet sus costos inflexibles incluyen hardware y software. Los costos inflexibles son fáciles de entender y establecer. Son estimaciones predecibles de costos fáciles de detectar. Cualquier nombre de fabricantes puede anotar el precio de venta de cualquier pieza de equipo de computo o software. Los costos para instalar software y hardware son también costos inflexibles.

Costos flexibles

Los costos flexibles son costos de objetos intangibles tales como la capacitación o la ineficacia durante el periodo de aprendizaje del usuario. Los costos flexibles pueden ser fáciles de entender pero es difícil establecerlos. Por ejemplo, es complicado estimar cuanto tiempo tomara a los empleados aprender una tecnología nueva o llegar a ser tan eficientes como lo son con la tecnología existente. Tal tiempo de aprendizaje no solo le cuesta a la compañía una proporción de los salarios individuales, sino que también, afecta temporalmente todas las salidas de datos de la organización.

Beneficios

Para determinar el ROI de una tecnología de información primero debemos entender los tipos de beneficios que una empresa podría obtener al hacer uso de dichas tecnologías. La siguiente tabla se definen los diferentes tipos de beneficios.

TIPOS DE BENEFICIOS	DESCRIPCIÓN
Tangibles	Beneficios tangibles son aquellos que afectan directamente el balance final de la compañía. Puede decir objetivamente que esos beneficios generan ganancias.
Intangibles	Beneficios intangibles son aquellos que afectan de manera indirecta el balance final de la compañía. Pueden o no generar ganancias.
Cuantificables	Beneficios que pueden medirse o cuantificarse fácilmente.
No cuantificables	Beneficios que no se pueden medir o cuantificar con facilidad.

Beneficios de Intranet (El numerador ROI): Para calcular el numerador ROI debe definir los beneficos que una Intranet ofrece. Estos beneficios tienen dos formas: ahorros de costos evitados y rendimiento de la eficiencia creada. Los costos evitados son muy obvios. Si un costo ya no es necesario debido a la implementación de una Intranet, la compañía habrá ahorrado dinero y se puede anotar el costo como un beneficio de la Intranet. De igual forma, si un trabajo puede ser determinado con mayor rapidez debido a la implantación de una Intranet, la compañía ha ahorrado dinero que también podrá anotar como un beneficio de la Intranet. Los rendimientos por la eficiencias creadas son las ganancias que la compañía puede ver si da buen uso al tiempo ahorrado.

Costos evitados

Muchas de las ventajas que una Intranet proporcionan están en forma de edición electrónica. Una compañía puede colocar virtualmente cualquier cosa que imprima y distribuya en papel dentro de los sitios web internos de la compañía y, a su vez, reducir costo de impresión. Además utilizar documentos electrónicos, los lectores pueden terminar y recuperar electrónicamente materiales que requieren respuesta.

Costos de impresión

Cualquiera con acceso a una computadora, puede obtener y enviar información en forma electrónica evitando los costos de copia. Los costos más obvios son papel y tinta. Reducir la cantidad de dinero que se gasta en papel y tinta para uso interno, es una forma de abatir costos sin reducir el costo al cliente.

Además, la edición electrónica proporciona otros ahorros en costos. Cuando las compañías imprimen grandes cantidades de materiales costosos tales como un beneficios para n empleados, a menudo ordenan copias extra debido a que volver a imprimir pequeñas cantidades es costoso. Cuando una compañía utiliza edición Intranet, esta puede crear un número exacto de copias, sin desperdicio.

Otros costos

Cuando las copias llegan a la oficina de alguien también deben almacenarse y archivarse al almacenar información en línea puede reducir requerimientos de espacio para suministros y archivos además, se debe de considerar los gastos de distribución (correo, embarque y costos de mensajería que pueden ser significativos). Como se sabe, las máquinas de fax casi han terminado con la necesidad de enviar pequeños documentos por correo así mismo, una Intranet le permite enviar cualquier longitud de documento a cualquiera en unos cuantos segundos.

Creación de eficiencias

Mientras la ventaja más importante de una Intranet es su capacidad para distribuir información a través de varias plataformas, la segunda ventaja con mayor importancia de la Intranet es la facilidad con la cual los usuarios pueden acceder a la información. Los

empleados pueden encontrar información dentro de una Intranet casi al instante. Una Intranet hace que encontrar información sea una tarea rápida e intuitiva.

Por ejemplo, la página principal del departamento de recursos humanos es el lugar obvio en la que un empleado puede encontrar información sobre beneficios. Las hiperligas hacen que encontrar un documento o reporte sea una operación sencilla al dar un click con el ratón. Los usuarios pueden examinar listas y categoría de datos con sus sublistas y subcategorías en minutos. Si los usuarios no saben donde empezar a buscar información pueden emplear un mecanismos de búsqueda para localizar con exactitud los datos.

Cada minuto que una Intranet ahorra a un empleado contribuye a engrandecer las productividad del empleado. Cuando los empleados no pueden encontrar los datos por si mismos usualmente recurren a otros para obtener ayuda. Este trastorno eleva el precio que las empresas pagan por la obtención de información. La Intranet es una solución de tecnología de información que no sólo acorta el tiempo entre la información solicitada y su entrega, sino que reduce el número de personas que se involucran para entregar la información.

Cuando se considera el ROI para la implantación de una Intranet es importante tomar en cuenta cual valioso es ahorrar tiempo. En el pasado una búsqueda de información especializada requería que los empleados inspeccionarán documentos, hicieran preguntas a los autores del documento, visitaran la biblioteca de la compañía y posiblemente intercambiaran varios memos o faxes. Con un mecanismo de búsqueda de Intranet, un empleado puede buscar información sobre un tema en segundos.

Eficiencia para un buen uso

Utilizando el tiempo que ahorran los empleados pueden por lo menos, iniciar su próxima tarea; poco a poco, mientras la Intranet acelera más tarea los empleados encontraran tiempo extra al dar buen uso a este tiempo, aun si solo son 15 minutos la compañía se coloca en la posición de ver resultados extraordinarios.

Costos acarreados

Otro paso a ejecutar para definir los ingresos netos para la formula ROI es calcular los diferentes gastos que debe acarrear regularmente para operar la Intranet. Los gastos más comunes para el desarrollo de una Intranet incluye lo siguiente:

- *Personal de sistemas*: Una administrador de sistemas mantiene en funcionamiento a la Intranet, instala un nuevo equipo, actualiza las computadoras de escritorios, y mantienen la seguridad del sistema. Mientras que el personal actual puede estar capacitado para absorber estas responsabilidades, un nuevo empleado puede hacer necesario para instalaciones más grandes. Conforme los trabajadores de una organización incrementan su uso de la Intranet, pronto podrían ver la necesidades de software o aplicaciones personalizadas. Un administrador de aplicaciones tienen una asignación muy parecida a la de un administrador de sistemas, excepto porque el administrador de aplicaciones se enfoca al software. Además de manejar el software

existe el administrador de aplicaciones podría necesitar escribir aplicaciones personalizadas.

- *Capacitación*: Los administradores de sistemas y aplicaciones deben asistir a clase y programas de certificación para mantenerse en lo más alto de la tecnología. Y, aunque las Intranet son fáciles de instalar e instintivas en su diseño, deben proporcionarle a sus usuarios instrucciones sobre la marcha acerca de las formas en que se pueden maximizar los beneficios del sistema. Tal capacitación al usuario puede ocurrir utilizando a su personal como entrenadores o contratando entrenadores externos. En ambos casos, la compañía incurriría en costos de capacitación.

- *Planear después de la instalación*: Debido a que una Intranet es un sistema envolvente, la compañía debe colocar un equipo multifucional que continuamente guíe el desarrollo de la Intranet. Debe de anotar un costo, basado en los salarios de estos empleados como un gasto.

- *Autoría*: Una Intranet es tan útil como su información este disponible. La compañía debe impulsar a cada empleado a colocar información en el Web interno. Cuando los empleados crean tal información, no están realizando sus labores normales. Debe contar un costo, basado en el salario de los empleados como un gasto.

- *Hardware y Software misceláneo*: Durante cada año debe de tener una tolerancia en el presupuesto para gastos en el Hardware y Software anticipados e inesperados.

Inversión Intranet: El denominador ROI

Una inversión Intranet consiste principalmente en Hardware y Software. Esta discusión asume que la compañía tiene una red existente. Mientras que pueda haber un debate para decidir si cada pieza de Hardware es necesaria si el Software es suficiente, su objetivo es incluir todo lo que sea razonable con el fin de determinar el ROI más confiable. Cada compañía tiene una situación diferente. De hecho, algunas compañías tienen suficiente equipo para iniciar una pequeña Intranet sin costos de Hardware entonces pueden bajar Software gratuito de sitios Intranet.

Los costos de inversión para una Intranet incluyen:

- *Planear antes de la instalación*: La compañía debe de formular un equipo que realice varias funciones para diseñar la Intranet y sus usos. Mientras los miembros de este equipo definen los planes de la Intranet, no ejecutan sus tareas regulares. Debe contar un costo, basado en el salario de cada empleado, como un gasto.

- *Hardware* : La Intranet requerirá al menos una computadora servidor con espacio de disco duro adecuado y velocidad para alojar los sitios Web. Los servidores necesitarán ser reemplazados o expandidos durante la vida de la Intranet. Además, puede requerir servidores adicionales que sirven como estructura de seguridad.

- *Software*: La Intranet requerirá Software servidor así como Software cliente (visualizadores), Software Firewall(de seguridad), herramientas de autoría HTML, un sistema de administración de documentos, mecanismos de búsqueda y más, dependiendo de las necesidades de la compañía.

- *Instalación*: La compañía debe configurar físicamente el servidor cada servidor e instalar el Software adecuado. Así mismo, la compañía podría necesitar software en cada sistema de usuario, lo que conlleva un costo.

- *Depreciación*: Como se ha dicho debe restar una cantidad de depreciación de la inversión de cada año.

CONCLUSIONES

La comunicación en la actualidad gira entorno a la tecnología Internet/Intranet Diversas organizaciones están implementando ya esta tecnología buscando en ella la solución a sus problemas de integración tecnológica y humana. Por lo tanto, todas las organizaciones que deseen sobrevivir en este mundo globalizado, deberán elegir alguna solución tecnológica

Las Intranets están revolucionando los sistemas empresariales de información, constituyen potentes herramientas competitivas que permiten aumentar la productividad y generar mayores ingresos a la vez que reducir costes; prácticamente cualquier aspecto de trabajo de una empresa puede mejorarse gracias a una Intranet. Las Intranets representan la evolución natural de los sistemas de información actuales, que permiten:

- Crear un sistema de información flexible que se adapte a las necesidades.
- Ser independiente de los proveedores.
- Ser independiente de la arquitectura material.
- Desarrollar una aplicación una sola vez y desplegarla inmediatamente por todo el sistema de información.
- Reducir los costes de adquisición, operativos de desarrollo y administración.

Una Intranet es una herramienta extremadamente útil para las empresas. Mientras se mueven las industrias ventajas de competitividad sustanciales a través del control de recurso y la administración de información, la Intranet sigue siendo una solución de tecnología de información efectiva en costo. Cualquier empresa que considera varias tecnologías para incrementar la conectividad interna debe considerar la Intranet como una empresa de bajo costo con un potencial de alto rendimiento.

En la implementación de la Intranet a la Secretaría de Relaciones Exteriores, podemos citar algunos beneficios de ésta:

- La Intranet mejora la arquitectura computacional existente, permitiendo a la red de área local desenvolverse mejor que antes.

- La Intranet reduce costos, mejora la productividad y promueve el intercambio de información.

- La Intranet resulta ser una herramienta valiosa para el Centro Nacional de Control de Energía y continuará haciéndolo en el futuro por las aplicaciones que ésta sustenta.

- Permite involucrar a los empleados, manteniéndoles informado y solicitándoles retroalimentación.

- Agilizar la comunicación de datos e información para distribuir y actualizar software y documentación electrónica.

- Proporcionar una forma de debates, para ofrecer un curso en línea.

La seguridad en la red local del Centro Nacional de Control de Energía. es muy importante ya que finalmente esta dependerá del éxito o fracaso de la Intranet. La cual es la referencia requerida para las computadoras y otros equipos que actúan directa o indirectamente con el servidor Web, esta referencia se encuentra protegida por el servidor Proxy 2.0. El cual tiene como objetivo conservar la integridad de la información contenida dentro de la Intranet.

El servidor Proxy es el encargado de controlar el uso tanto de los recursos de Internet como los de la Intranet, restringiendo el acceso a sitios no permitidos, también es utilizado para almacenar los sitios o páginas más visitados , de la manera que los usuarios tengan el acceso más rápido a esos sitios cada vez que ellos requieran visitarlos.

GLOSARIO DE TERMINOS

Ancho de Banda. El término se refiere a cuanta cantidad de información se puede enviar a través de una conexión. Usualmente se mide en bits-por-segundo. Por ejemplo una página completa de texto son aproximadamente 16,000 bits. Un módem rápido puede mover aproximadamente 52,000 bits en un segundo. Movimiento en vídeo completo (full-screen) requeriría aproximadamente 10,000,000 bits por segundo dependiendo de la compresión.

ANSI (Instituto Nacional de Estándares de Estados Unidos). La principal organización de desarrollo de estándares en Estados Unidos. El organismo que representa a Estados Unidos ante la ISO, ANSI es un organismo independiente y sin fines de lucro que está apoyado por organizaciones del ramo, sociedades profesionales y la industria.

ATM (Modo de Transferencia Asíncrona). Tecnología de punta de transmisión y conmutación a grandes velocidades por medio del movimiento asíncrono de paquetes con una velocidad de 155 Mbps o más, también se conoce como CELL RELAY, se considera la siguiente generación en arquitectura de redes.

AUI (Interfaz de unidad de aditamento). El cable entre el transceptor y la tarjeta de interfaz de red en una Pc o en otro nodo de la red.

Backbone. Una línea ó series de líneas de conexión de alta velocidad que forman una ruta principal con una red. Es la parte de la red que lleva el tráfico mas pesado.

Blindaje. El proceso de proteger un cable con un metal aterrizado, de tal forma que las señales eléctricas no pueden interferir con la transmisión dentro del cable.

Bps (Bits Por Segundo). Una unidad de medida de que tan rápido los datos son movidos de un lugar a otro. Un modem de 28.8 puede mover 28,800 bits por segundo.

Bridge (Puente). Dispositivo de red que conecta dos redes LAN y transmiten o filtran paquetes entre ellos, el destino de direcciones se basa en un puenteo que opera en la capa de nivel de datos o MAC del modelo OSI.

Bus. Un trayecto de transmisión o canal; una conexión eléctrica, con uno o mas conductores por la cuál todos los dispositivos conectados reciben todas las transmisiones al mismo tiempo; una configuración lineal de red de área local, tal como la utilizada en Ethernet y en Token Bus.

Browser o Navegador. Un programa cliente (software) que es usado para visualizar varios tipos de recursos de Internet.

Cliente. Un programa software que es usado para contactar y obtener información de un programa servidor en otra computadora comúnmente a gran distancia. Cada programa cliente es diseñado para trabajar con uno o más tipos específicos de programa servidor y cada servidor requiere un tipo específico de Cliente por ejemplo un Web Browser es un tipo de cliente específico.

Concentrador. Dispositivo usado para la conexión de los cables de los nodos de una red dispuesta en topología física de estrella, este dispositivo se asocia con una red Ethernet 10BaseT.

Conector. Un dispositivo que mantiene juntas dos partes de un circuito, de manera que puedan hacer contacto eléctrico.

CSMA (Sensor de Portadora de Accesos Múltiples). Método de contención para compartir un canal. Antes de transmitir la información la estación emisora comprueba si el canal esta libre, y si no detecta ninguna señal comienza a transmitir. Técnica de contención que permite que solo una de entre varias estaciones tengan acceso al canal de transmisión.

CSMA/CD (Sensor de Portadora de Accesos Múltiples con Detección de Colisión). Es un protocolo utilizado para enviar señales dentro de una red local. Cuando la tarjeta detecta solo la portadora empieza a transmitir, pero debe seguir escuchando por si ocurre una colisión. De ser así requerirá hacer una retransmisión esto evitara las colisiones de datos.

DIMM. : Más alargados (unos 13 cm), con 168 contactos y en zócalos generalmente negros; llevan dos muescas para facilitar su correcta colocación. Pueden manejar 64 bits de una vez, por lo que pueden usarse de 1 en 1 en los Pentium, K6 y superiores. Existen para voltaje estándar (5 voltios) o reducido (3.3 V).

Dominio. Término que hace referencia a un grupo de computadoras de una red, las que son administradas como un grupo relacionado o como una sola entidad.

E-mail o Correo Electrónico. Mensajes, usualmente texto, enviado de una persona a otra vía computadora, un correo puede ser enviado automáticamente a un gran numero de direcciones o destinos.

Estación de Trabajo. Computadora que accede a los recursos compartidos en otras computadoras pero no comparte sus recursos con las demás. También se llama cliente. El termino estación de trabajo suele hacer referencia a un a computadora aislada.

Ethernet. La más popular tecnología LAN usada. El estándar IEEE802.3 que define las reglas para configurar una red Ethernet. Define una velocidad de 10 Mbps utilizando protocolo CSMA/CD.

FDDI . Interface de datos distribuida por fibra, interfaz para cableado de fibra óptica capaz de conseguir una velocidad de transmisión de 100 Mbps. Originalmente especificada para líneas de fibra, aunque también puede operar sobre par trenzado para distancias cortas.

Fibra Óptica. Un medio de transmisión de datos que consiste en una fibra de vidrio (o de plástico). Una fuente luminosa (LED o lasser emite un haz de luz que se va reflejando dentro del cable gracias a los diferentes grados de refracción entre el material de la fibra y una cubierta de un metal similar). Aunque el costo de la fibra ha bajado, todavía resulta costoso y complejo instalar fibra óptica en redes locales.
Frecuencia. Número de ciclos por unidad de tiempo. Normalmente medida en Hertz (Hz), que son ciclos por segundo.

Gateway (Puerta de Enlace). Dispositivo para interconectar dos o más redes distintas. Este puede traducir todos los niveles de protocolo de la capa física sobre el modelo OSI.

Host. Generalmente identificado como un nodo en la red.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos, Organización profesional dedicada al avance de la ingeniería eléctrica, la electrónica y aspectos afines de la ingeniería y la ciencia. También la IEEE registra y define estándares industriales, es miembro de ANSI e ISO.

Internet. Es una serie de interconexiones de redes local, regional, nacional e internacional inmensa usando TCP/IP. Internet une gobiernos, universidades y muchos mas sitios en el mundo. Provee de e-mail, conexiones remotas y servicio de transferencia de archivos

Intranet. Es una red que existe exclusivamente dentro de una organización y que esta basada en la tecnología de Internet. Distribuye los recursos de información de la organización al escritorio de cada miembro de manera rápida y económica y, al mismo tiempo, protege la información frente accesos no autorizados.

IPX. Intercambio de paquetes entre redes, un protocolo de comunicación de Netware de Novell que crea, mantiene y termina conexiones entre dispositivos de una red, tales como estaciones de trabajo y servidores

ISO (Organización de Estándares Internacional). Modelo referencial de capas que se basan en normas para las comunicaciones. Este modelo se basa en siete capas: Físico, Datos, Red, Transporte, Presentación y Aplicación. Cada capa provee de servicios.

LAN (Red de área local). Tecnología para conectar varias computadoras que estén a unos cuantos cientos de metros de distancia entre sí. Grupo de computadoras y/o terminales inteligentes o no inteligentes, conectadas entre sí de forma que pueden compartir periféricos e información, o que se encuentran dentro de un área reducida, como por ejemplo un edificio o una oficina. sistema de transmisión de datos que permite compartir recursos e información por medio de computadoras o redes de computadoras.

MAC (Control de Acceso al Medio). Mecanismo a través del cual los dispositivos conectados a una red local, conducen el medio de transmisión. El MAC combina algunas funciones de los niveles físico y de datos del modelo OSI.

Mainframe. Un computador en gran escala que puede alojar software completo y varios equipos periféricos , y también manejar muchos usuarios, generalmente cientos de ellos.

Mbps. Mega bits por segundo

Modem. Un dispositivo modulador - demodulador que transforma una señal digital de una computadora en forma analógica adecuada para transmitirse a través de líneas telefónicas comunes. El módem convierte una señal en dos niveles en una secuencia de señales de dos frecuencias (tonos de pulso de audio), los tonos vienen a través de la línea entran al módem y transforman de nuevo en código digital para comunicarse con una computadora.

Multiusuarios. El poder dar soporte a mas de un usuario a la vez. Una aplicación multiusuarios permite que más de una persona use la aplicación al mismo tiempo.

Netware. Un desarrollo de Novell como sistema operativo de red (NOS) que provee de un servicio de archivos que se comparten además de un servicio de impresión de información entre redes de computadoras.

NIC Son las siglas de Network Interface Card. Tarjeta de Red

Nodo. Estación en una red. El nodo puede ser una computadora o una terminal. Estas terminales proporcionan puntos de captación/salida de datos en redes de computadoras y también pueden computar o procesar datos.

Nombre de Dominio. Es un texto relacionado a un texto de computadoras, es una forma de identificación única a través de Internet.

NOS. Es el sistema operativo de red, un software que corre dentro de un servidor para que tengan acceso al servicio de archivos y otros recursos. Por ejemplo, Novell, Unix, etc.

Paquete. Serie de bits, información en una red que consiste de datos e información de control y que incluye el destino pretendido del paquete.

PPP. Protocolo punto a punto, el sucesor de SLIP, provee ruteadores-a-ruteadores y host-a-red.

Protocolo. Reglas que van a definir la manera en como se da la comunicación en la red

Punto a Punto. Tipo de red en la cual cada nodo es capaz de compartir sus recursos y usar los recursos compartidos de todos los demás nodos de la red.

Red. Un sistema de interconexión de computadoras, este puede comunicarse con otras y compartir archivos, datos y recursos.

Repetidor. Dispositivo usado en las redes locales para amplificar y retransmitir una señal a fin de evitar su degradación.

RJ-45. Conector para cable de par trenzado (UTP y STP)

Ruteador. Dispositivo que conecta redes que utilizan la misma capa de protocolo de red (nivel 3), como TCP/IP o IPX. Los ruteadores tienen la capacidad de conectar redes que usan diferentes topologías lógicas, como Ethernet y Token Ring.
Servidor. Se encarga del control de cada una de las terminales que se encuentran enlazadas a él. Dispositivo con capacidad de procesos que proporcionan un servicio especifico a la red.

Servidor de Archivos. Computadora cuyo propósito principal es compartir archivos con otros nodos en la red. Algunas veces se usa de forma intercambiable servidor de archivos y servidor.

SIMM. (Single in line Memory Module), Modulo de Memoria en una Sola línea. Se trata de tarjetas longitudinales en las que ya están integrados y soldados los nueve chips, aunque también existen módulos que sólo poseen tres chips. Tiene la desventaja que en ciertas tarjetas madre se debe instalar las tarjetas de memoria en pares de iguales características de tamaño y velocidad. Este es el caso de los procesadores Pentium y similares. En el mercado se pueden encontrar dos tipos de tarjetas de memoria SIMM:
Sin paridad, es la memoria RAM normal ,es la más barata y es la que usa la mayoría de la gente y se consigue en varias velocidades, tienen un número par de chips típicamente ocho.
Con paridad, es un poco más cara y no presenta mejoría de rendimiento alguno, pero algunos computadores requieren memoria Con paridad, y no funcionan con la Sin paridad. La paridad es una característica de corrección de errores que tiene este tipo de memoria.

SLIP. Protocolo de Interedes de línea serial , un protocolo antiguo para conexiones con IP sobre líneas telefónicas. Esta siendo reemplazado por el protocolo punto a punto (PPP).

SPX. Intercambio secuencial de paquetes, protocolo de Novell para permitir que dos estaciones de trabajo se comuniquen a través de una red, los datos son transferidos en secuencia y revisa que lleguen a su destino final

Switch. Dispositivo multipuerto Ethernet diseñado para incrementar la capacidad de la red

TCP/IP. Protocolo de Control de transmisión y Protocolo de Internet siempre van juntos y son los protocolos de red en la norma de ambiente UNIX.

Token Ring. Una topología de red en donde se pasa un token (señal) entre computadoras que están conectadas en anillo. Cuando una computadora esta en posesión del token, puede transmitir datos por la red. Cuando termina, el token pasa a la siguiente computadora y así sucesivamente.

Topología. Arreglo lógico o físico de las terminales sobre una red en relación a otra. Configuración de la red ya sea centralizada o distibuida. Las estaciones conectadas a una línea común de comunicaciones.

UTP. Par de conductores retorcidos sin blindaje. Cable de par retorcido sin blindaje o con blindaje o conjunta

Windows NT Server. El NOS de Microsoft de 32 bits y de multitareas.

BIBLIOGRAFÍA

- **BAKER**, Richard H.
  Networking the Enterprise. MC Graw Hill

- **BLACK**, Uyless
  Redes de Computadoras, Protocolos, Normas e Interfases. Macrobit 1990

- **BRONSON**, Purdy.
  Implementación de Redes de Area Local. Tecnology Training S. De R.L. de C.V.

- **GONZALEZ** Sainz, Nestor
  Comunicaciones y Procesamiento de Datos. Mc Graw Hill

- **HALSAL**, Fred
  Data Comunications Computer Networks and Open systems. Addison – Wesley

- **HOPPER / TEMPLE / WILLIAMSON**
  Diseño de redes Locales. Addison-Wesley Iberoamericana. 1991

- **MADRON** Wm, Thomas.
  Local Area Networks In Large Organizations. Hayden

- **SCATT**, Stan.
  A Fondo: Redes de Area Local. Anaya Multimedia

- **STOLTZ,** Kevin.
  Todo Acerca de las Redes de Computadoras. Prentice Hall Mexico 1995

- http://nti.educa.rcanaria.es/conocemos_mejor/apuntes/paginas/ethernet.htm
  Información general de redes ethernet, características de cables, etc.

- http://tiny.uasnet.mx/prof/cln/ccu/mario/REDES/node20.html
  Información de dispositivos usados en las redes ethernet.

- http://www.map.es/csi/silice/defglosario.html
  Definiciones de redes y comunicaciones.

- http://www.microsoft.com/msdownload/PROXY/00000.HTM
  Proxy Server 2.0 for Windows NT(i386) - US English Version

- http://www.it.uc3m.es/~prometeo/comdat/apuntes/tema1/tema1.htm
  Información general de redes de comunicación.