UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

Facultad de Química

DISEÑO E INSTALACION DE UNA SALA DE COMPUTO PARA SERVICIOS DE INFORMACION QUIMICA

TESIS
Que para obtener el título de
INGENIERO QUIMICO
presenta

JOEL IVAN CORDERO CHAVEZ

México, D. F.

2003

PAGINACION

DISCONTINUA

Jurado asignado:

Presidente	**Prof. Rafael Moreno Esparza**
Vocal	**Prof. Carlos Galdeano Bienzobas**
Secretario	**Prof. Imelda Velázquez Montes**
1er. Suplente	**Prof. Sergio Álvarez Navarro**
2°. Suplente	**Prof. Francisco Rojo Callejas**

Coordinación de Sistemas de Información Digital (COSID)
Anexo Biblioteca, Facultad de Química.

M. en C. Imelda Velázquez Montes

Joel Iván Cordero Chávez

A mi Papá ✞, que le hubiera gustado estar presente en estos momentos.

A mi Mamá, que siempre me ha apoyado en todo momento.

A la Maestra Imelda Velázquez que me impulsó, y me soportó para completar este proyecto.

Agradecimientos

A la Maestra Imelda Velázquez, que me brindó su tiempo y su conocimiento. A mi Mamá por haberme apoyado en TODO momento, física y espiritualmente. A todos mis Amigos, que me aguantaron durante toda la carrera y en especial al George que si no fuera en gran medida por él, este proyecto todavía no estaría terminado. A la Facultad de Química de la UNAM, que me dió la oportunidad de realizar mis estudios. A los miembros del jurado que me brindaron parte de su tiempo para evaluar este trabajo.

CONTENIDO

Justificación

En la actualidad la información que se genera en las ciencias químicas es de naturaleza muy extensa así como compleja; por ello, los profesionales de ellas, para mantener un grado competitivo, deben contar con los conocimientos adecuados en el momento que se requieran, pues resulta impráctico y casi imposible tratar de concentrar toda la información existente en un lugar o persona, para esto se recurre a las herramientas que brinda la última tecnología, los llamados sistemas de información digital.

Las fuentes de información tradicionales son, por ejemplo, medios impresos (libros, revistas y publicaciones en general), las bases de datos en CD-ROMS y los programas interactivos. Pero lo que todas estas fuentes de información tradicionales tienen en común es que resulta problemático o costoso mantener dicha información actualizada.

Actualmente para resolver dicho problema se cuenta con nueva tecnología, por medio de Internet se tiene un acceso cada vez más fácil a un mundo de información al alcance; en él se puede acceder a bases de datos en línea, revistas electrónicas, foros de discusión, correo electrónico y páginas web, así como otros servicios.

El almacenamiento y el análisis de la información han sido de los grandes problemas a los que se ha enfrentado el hombre desde que se inventó la escritura. No es sino en la segunda mitad del siglo XX que, gracias a la invención de la computadora, el hombre ha podido resolver parcialmente este problema. [1]

En la década de los cincuentas, el hombre dio un gran salto al inventar la computadora electrónica; la información ya podía ser enviada en grandes cantidades a un lugar central donde se realizaba su procesamiento. Ahora el problema era que esta información tenía que ser "acarreada" al departamento de proceso de datos. [9]

Con la aparición de las terminales en la década de los sesentas, se logró la comunicación directa entre los usuarios y la unidad central de procesos, y con ello una comunicación más rápida y eficiente; pero se encontró un obstáculo, entre más periféricos y terminales se agregaban al computador central: la velocidad de comunicación decaía. [9]

Las necesidades de información de los usuarios también han cambiado con el tiempo por la aparición de las nuevas tecnologías de comunicación, que han influido en el trabajo de la investigación, docencia, etc. Los profesionales ahora requieren mayor velocidad para presentar sus resultados que antes de que estas tecnologías hicieran su aparición.

Las universidades y los centros de investigación necesitan acceder a la información generada en otras partes del mundo, casi en el momento en que aparece, para que su trabajo sea reconocido y para mantenerse en la frontera de la investigación. Por eso se justifica la creación de centros de información científica de punta dentro de dichos ámbitos.
Por lo planteado, en el presente trabajo se incluye la propuesta para diseñar e instalar un sitio con las condiciones apropiadas de infraestructura necesaria para ofrecer servicios de información digital a los usuarios de un centro de trabajo, como lo es la Facultad de Química de la UNAM.

Introducción

A partir del año 1975, la refinada tecnología del silicón y la integración en miniatura permitieron a los fabricantes de computadoras construir máquinas con gran capacidad de procesamiento y almacenamiento pero más pequeñas, llamadas microcomputadoras; descongestionaron las viejas máquinas centrales y permitieron que cada usuario tuviera su propia microcomputadora. [3]

En 1982, las microcomputadoras habían revolucionado por completo el concepto de *computación electrónica* así como sus aplicaciones y mercados. Los gerentes de los departamentos de informática fueron perdiendo el control de la información ya que ahora el proceso de la información no estaba centralizado. Esta época se podría denominar como la "era del *floppy disk*". Los vendedores de microcomputadoras proclamaban: "en estos 30 disquetes usted podrá almacenar la información de todos sus archivos". Sin embargo, de algún modo se había retrocedido en la manera de procesar la información, pues ahora había que "acarrear" la almacenada en los disquetes de una microcomputadora hacia otra, además la poca capacidad de éstos hacía difícil el manejo de grandes cantidades de información. [3]

Con la llegada de la tecnología Winchester (la cual permite el almacenamiento de información en discos duros), se lograron dispositivos que podrían almacenar grandes cantidades de información. Una desventaja de esta tecnología era el alto costo de dichos dispositivos. Entonces nació la idea que permitiría a múltiples usuarios compartir los costos y beneficios de un disco Winchester: las Redes de Área Local (LAN, *Local Area Network*) habían nacido. [4]

En un principio, las redes de microcomputadoras se formaron por simples conexiones que permitían a un usuario acceder a recursos residentes en otras microcomputadoras, tales como discos duros, impresoras, cd-rom's, etc. Estos equipos permitían a cada usuario el mismo acceso a todas las partes del disco duro, lo que causaba obvios problemas de seguridad (acceso de lectura y escritura a cualquier usuario) y de integración en los datos.

Hacia 1983, la compañía Novell, Inc. fue la primera en introducir el concepto de "servidores de archivos", en el que todos los usuarios pueden tener acceso a la misma información, compartir archivos y contar con niveles de seguridad (limitando el permiso a los usuarios de sólo lectura a los datos vitales del sistema). [4]

Historia de Internet

Es importante conocer la historia de Internet con el fin de comprender porque se ha convertido en el instrumento de comunicación del futuro en el que muchos de sus servicios son gratuitos. [8]

1957. Se creó ARPA (*Advanced Research Project Agency*, Agencia de Proyecto para la Búsqueda Avanzada) administrado por el Ejército de los Estados Unidos en respuesta al lanzamiento del Sputnik (primer satélite artificial en orbitar la tierra). Al iniciar Estados Unidos la carrera espacial de manera tardía, se creó la ARPA para buscar alternativas de comunicación de voz y datos vía terrestre. En años siguientes, se creó una red llamada ARPANET, que enlazaba los organismos militares estadounidenses. ARPANET fue conocida como la "red apocalíptica".

1969. Se creó una red entre UCLA (Universidad de California) y ARPANET. UCLA es una de las universidades que trabajan con el gobierno. Para tal efecto, se estableció una conexión fuera de ARPANET que permitía a los investigadores de UCLA estar en contacto con los equipos de cómputo de ARPANET.

1971. ARPANET contaba con 15 nodos y 23 servidores. Nació el correo electrónico. ARPANET se convirtió en un instrumento de suma utilidad para efectos militares. Se desarrollaron los primeros programas de correo electrónico que trabajaban en equipos de IBM 370.

1973. Se establecieron conexiones a Inglaterra y Noruega. ARPANET estableció las primeras conexiones interoceánicas con sus aliados.

1976. Surgió Usenet (servidores de grupos de noticias, *Newsgroups*) entre las universidades de DUKE y UNC. Nació Usenet como la derivación del correo electrónico. Su propósito inicial era compartir información tematizada entre los investigadores.

1982. Se estableció el TCP/IP como protocolo estándar dentro de Internet. Al establecer como estándar al TCP/IP, Internet inició su camino hacia la globalización por medio de un lenguaje de comunicación que puede usar todo tipo de computadoras.

1984. La Universidad de Berkeley liberó UNIX 4.2. Ya existían 500 servidores. UNIX 4.2 se convirtió en el estándar mundial en sistemas operativos multiusuario. La mayoría de las versiones actuales de UNIX usaban las librerías de Berkeley como estándar.

1986. La NSF (*National Software Foundation,* Fundación Nacional de Software*)* estableció cinco Centros de Súper Cómputo. Velocidad de transmisión: 56 kbps (kilobauds por segundo). La NFS comenzó a jugar un papel muy importante en la administración de Internet.

1987. Se fundó la ANS (*Advanced Network & Services*, Red Avanzada y Servicios*)* para evitar monopolios. Las empresas Merrit, IBM y MCI fundaron la ANS para que Internet se convirtiera en una identidad jurídica separada de cualquier empresa privada.

1988. Internet cuenta ya con 20,000 servidores. Apareció el gusano de Internet. El gusano de Internet infectó a casi la mitad de dichos servidores. Se tuvieron que crear sistemas de seguridad que no permitieran este tipo de programas dañinos.

1989. La velocidad de conexión llegó a 1.544 mbps. Las redes digitales invadieron Internet.

1990. *Compuserve* se conectó a Internet. *El cual* usó el *backbone* (línea principal de la red) de Internet para sus servicios.

1991. Internet ya cuenta con un total de 617,000 servidores. La Universidad de Minessota liberó el servicio *Gopher*, que permitía organizar información jerárquicamente dentro de los servidores. Se facilitó la búsqueda de información por parte de los usuarios.

1992. Se creó el servicio WWW (*World Wide Web*). Internet operaba a una velocidad de 44.736 mbps. Se cuenta con alrededor de 1,000,000 de servidores. Internet desarrolló su *backbone* actual a una velocidad de más de 44 millones de bauds por segundo. Empezó el crecimiento exponencial de Internet.

1994. Ahora se cuenta con alrededor de 3,000,000 de servidores. *Mosaic* apareció para Windows 3.1 y se convirtió en el detonante que faltaba en los servidores WWW. *Mosaic* contaba con capacidad de acceder automáticamente a los servidores *Gopher*, FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos) y Telnet.

1995. Se cuenta con casi 4,000,000 de servidores. *Netscape* desplazó a *Mosaic* como herramienta de navegación en Internet. En ese momento, *Netscape* contaba con un 70% del mercado a menos de un año de haber liberado su versión 1.0.

1996. *Microsoft* inició su aventura dentro de Internet. El cual lanzó al mercado *Explorer*, herramienta para navegación de Internet, cuyo fácil manejo desplazó rápidamente a *Mosaic* y empezó a competir contra el navegador más utilizado, *Netscape*.

1997. Se inició una batalla por el control de las herramientas de la red. *Microsoft* enfrentó una cerrada lucha contra *Netscape* por el dominio de la visualización de Internet; los dos liberaron sus respectivas versiones 3.0 al principio del año (enero) y se esperaba para finales del verano que ambos estuvieran listos para la versión 4.0. *Microsoft* designó una gran cantidad de dinero para desarrollar aplicaciones para Internet. *Sun Microsystems* liberó un lenguaje muy poderoso conocido como Java; también participó con aplicaciones poderosas hacia Internet. Las páginas HTML (*Hyper Text Markup Language*) comenzaron a ser parte de la

historia y VRML (*Virtual Reality Markup Language*) se empezó a conocer como el formato ideal parea diseño de páginas en la red. [8]

En la actualidad es posible mantener al día la información disponible en Internet, sólo resta encontrar una forma práctica de acceder a ella. Dentro del presente trabajo, se proponen las opciones básicas para diseñar, instalar y configurar una sala de cómputo que ofrezca servicios de información química.

En el primer capítulo se hace una breve introducción a la teoría involucrada en el funcionamiento de una red de computadoras, su definición, así como sus necesidades físicas para funcionar; se describe el *hardware* mínimo básico, se explican las posibles configuraciones y se nombran las más comunes.

El segundo capítulo explica paso a paso cómo configurar una red punto a punto dentro de Windows 95/98 con opción de un servidor Windows NT, asignando las direcciones IP a cada equipo, así como los pasos para compartir recursos bajo dicha red, tales como impresoras, archivos, carpetas, etc.

Dentro del tercer capítulo se muestra un ejemplo de configuración de la red de una sala para servicios de información química, desde la selección del tipo de cable más conveniente para objetivos particulares, la topología de red por usar, hasta las instrucciones generales para poner en funcionamiento la sala de servicios de información química.

También se menciona una opción extra con la que se puede complementar dicha sala, la instalación de un servidor *Linux* para servicios como correo electrónico, servidor de páginas WWW, grupos de discusión, compartir archivos vía Internet (FTP), etc., igualmente, en este capítulo se presenta de manera resumida la forma para instalar, configurar y administrar dicho servidor.

En el cuarto capítulo se enumeran los alcances de este trabajo, sus limitaciones en cuanto a la naturaleza del tema, así como sus posibles proyecciones a futuro (complementos de este trabajo).

Objetivos

En este trabajo se hace una propuesta práctica y resumida de los componentes básicos suficientes para diseñar e instalar una sala que proporcione servicios de información química en donde sea requerida, tanto dentro de alguna pequeña o mediana empresa como de alguna institución educativa, por ejemplo la Facultad de Química.

Los objetivos específicos de este estudio se pueden enumerar de la siguiente manera:

- Proporcionar la teoría básica del funcionamiento de redes para entender su "lógica" de configuración, así como de los protocolos que comúnmente se manejan.
- Configurar y ordenar una red local de computadoras para la sala de servicios de información química.
- Enumerar los pasos para compartir recursos bajo una red en entorno Windows 95/98, tales como impresoras o archivos.
- Proporcionar una lista de pasos básicos para instalar un servidor *Linux* para complementar los servicios de dicha sala de información química.
- Finalmente, poner en funcionamiento la sala de cómputo de servicios de información química.

Capítulo I

REDES Y REQUERIMIENTOS FÍSICOS

Capítulo I: Redes y requerimientos físicos

Para poder ensamblar una sala de cómputo, es importante contar con los antecedentes de los conocimientos de su definición, estructura, composición, funcionamiento además de saber con cuantas opciones se cuenta para poder cumplir con el objetivo principal del presente trabajo. Dentro de este primer capítulo se analizan estos pilares del conocimiento sobre redes de computadoras.

¿Qué es una red? [4]

Una red consiste en dos o más computadoras unidas que comparten recursos (ya sea archivos, CD-ROM´s o impresoras) y que son capaces de realizar comunicaciones electrónicas. Las redes pueden estar unidas por cable, líneas de teléfono, ondas de radio, satélites, etc...

La clasificación básica de redes es: Red de Área Local, Red de Área Metropolitana, Red de Área Extensa.

Red de área Local / *Local Area Network* (LAN) [4]

Se trata de una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos computadoras que disten entre sí más de un kilómetro.

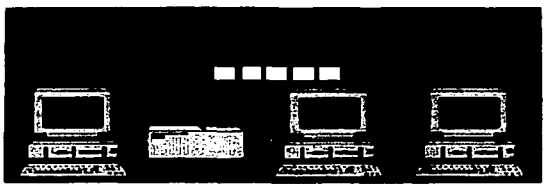

Figura 1. Red de área local

Una configuración típica en una red de área local es tener una computadora llamada servidor de archivos en la que se almacena todo el software de control de la red así como el software que se comparte con las demás computadoras de la red. Las computadoras que no son servidores de archivos reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y suelen tener software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

Red de área Metropolitana / *Metropolitan Area Network* (MAN) [9]

Las redes de área metropolitana cubren extensiones mayores como puede ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuye la información a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

Figura 2. Red de área metropolitana

Redes de área Extensa / Wide Area Network (WAN) [9]

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cable transoceánico o satélites se utilizan para enlazar puntos que se encuentran a grandes distancias entre sí.

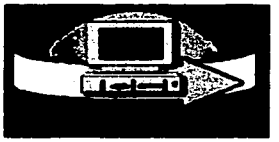

Figura 3. Red de área extensa

Con el uso de una WAN se puede contactar desde México con Japón sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada. Se utilizan multiplexores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problemas. El mejor ejemplo de una red de área extensa es Internet.

El Cableado de la red [12]

El cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN. Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Estos son los tipos de cable más utilizados en redes LAN:

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

Este tipo de cable es el más utilizado. Tiene una variante con blindaje pero la variante sin blindaje suele ser la mejor opción para una PYME (Pequeña Y Mediana Empresa).

Figura 4. Cable de par trenzado sin blindar (UTP)

La calidad del cable y consecuentemente la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable. Las categorías van desde el cable de teléfono, que esta limitado únicamente a transmitir voz hasta el cable de categoría 5 capaz de transferir 100Megabytes por segundo.

Tabla 1.- Categorías UTP

Tipo	Uso
Categoría 1	Voz (Cable de teléfono)
Categoría 2	Datos a 4 Mbps (LocalTalk)
Categoría 3	Datos a 10 Mbps (*Ethernet*)
Categoría 4	Datos a 20 Mbps/16 Mbps *Token Ring*
Categoría 5	Datos a 100 Mbps (*Fast Ethernet*)

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas). Es conveniente sin embargo utilizar cables de categoría 5 ya que estos permitirán migraciones de tecnologías 10Mb a tecnología 100 Mb.

Conector UTP

El estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. Las siglas RJ se refieren al estándar *Registered Jack* (Conector Registrado) creado por la industria telefónica. Este estándar define la colocación de los cables en su pin correspondiente.

Figura 5. Conector RJ-45

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

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este problema existe un tipo de cable UTP que lleva blindaje, esto es, protección contra interferencias eléctricas. Este tipo de cable se utiliza con frecuencia en redes con topología *Token Ring*.

Cable Coaxial

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un blindaje metálico con forma de rejilla que aísla el cable de posibles interferencias externas.

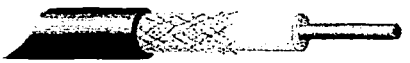

Figura 6. Cable Coaxial

Aunque la instalación del cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias. Por otra parte también es posible conectar distancias mayores que con los cables de par trenzado. Existen dos tipos de cable coaxial, el fino y el grueso conocidos como *thin* (delgado) coaxial y *thick* (grueso) coaxial.

Con frecuencia se pueden escuchar referencias al cable coaxial fino como *thinnet* o 10Base2. Esto hace referencia a una red de tipo *Ethernet* con un cableado coaxial fino, donde el 2 significa que el mayor segmento posible es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología de BUS (la cual se define en páginas siguientes).

Con frecuencia se pueden escuchar referencias al cable coaxial grueso como *thicknet* o 10Base5. Esto hace referencia a una red de tipo *Ethernet* con un cableado coaxial grueso, donde el 5 significa que el mayor segmento posible es de 500 metros. El cable coaxial es muy popular en las redes con topología de BUS. El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace de este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar.

Conector para cable coaxial

El más usado es el conector BNC. BNC son las siglas de Bayone-Neill-Concelman. Los conectores BNC pueden ser de tres tipos: normal, terminadores y conectores en T.

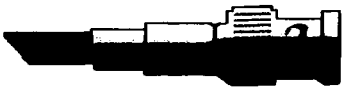

Figura 7. Conector BNC

Cable de fibra óptica

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar.

Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencia o servicios interactivos. El coste es similar al cable coaxial o al cable UTP pero las dificultades de instalación y modificación son mayores. En algunas ocasiones se escuchará 10BaseF como referencia a este tipo de cableado. En realidad estas siglas hablan de una red *Ethernet* con cableado de fibra óptica.

Figura 8. Cable de fibra óptica

Características:

- El aislante exterior está hecho de teflón o PVC.
- Fibras Kevlar ayudan a dar fuerza al cable y hacer más difícil su ruptura.
- Se utiliza un recubrimiento de plástico para albergar a la fibra central.
- El centro del cable está hecho de cristal o de fibras plásticas.

Conectores para fibra óptica

El conector de fibra óptica más utilizado es el conector ST. Tiene una apariencia similar a los conectores BNC.

Tabla 2.- Resumen de tipos de cables empleados

Especificación***	Tipo de Cable	Longitud Máxima
10BaseT	U T P	100 metros
10Base2	Thin Coaxial	185 metros
10Base5	Thick Coaxial	500 metros
10BaseF	Fibra Óptica	2000 metros

***NOTA: Para asignarle un nombre a una red se sigue el siguiente formato: v tipo l. Donde v significa velocidad de transmisión en Mbps; tipo significa tipo de señalización, que puede ser BASE para Baseband o BROAD para Broadband; l es longitud máxima de cable en múltiplos de 100 metros, a excepción de 10BASE-T, donde T significa cable de par trenzado (twisted-pair wire).

Redes LAN sin cableado [22]

No todas las redes se implementan sobre un cableado. Existen redes que utilizan señales de radio de alta frecuencia o haces infrarrojos para comunicarse. Cada punto de la red tiene una antena desde la que emite y recibe. Para largas distancias se pueden utilizar teléfonos móviles o satélites.

Este tipo de conexión está especialmente indicada para su uso con portátiles o para edificios viejos en los que es imposible instalar un cableado.

Las desventajas de este tipo de redes son sus altos costos, su susceptibilidad a las interferencias electromagnéticas y la baja seguridad que ofrecen. Además son más lentas que las redes que utilizan cableado.

Principales tipos de topologías físicas [19]:

Topología de Bus / *Linear Bus*

Consiste en un cable con un terminador en cada extremo del que se conectan todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable. Este cable recibe el nombre de *Backbone Cable* (cable central de conexión de red). Tanto *Ethernet* como *LocalTalk* pueden utilizar esta topología.

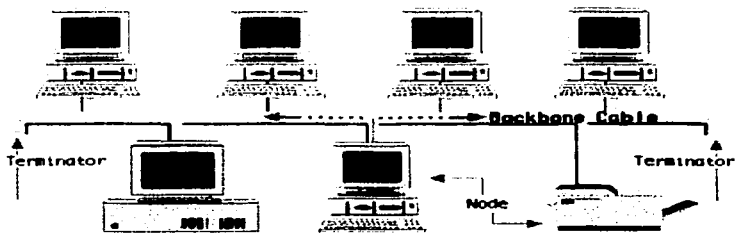

Figura 9. Topología de Bus

Ventajas de la topología de Bus:

- Es fácil conectar nuevos nodos a la red.
- Requiere menos cable que una topología estrella (se hablará de esta topología en paginas posteriores).

Desventajas de la topología de Bus:

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requieren terminadores.
- Es difícil detectar el origen de un problema cuando toda la red "cae".
- No se debe utilizar como única solución en edificios grandes.

Topología de estrella / *Star*

En una topología estrella todos y cada uno de los nodos de la red se conectan a un concentrador o *hub*.

Los datos en estas redes fluyen desde una computadora hacia el concentrador. Este controla realiza todas las funciones de red además de actuar como amplificador de los datos. Esta configuración se suele utilizar con cables de par trenzado aunque también es posible llevarla a cabo con cable coaxial o fibra óptica.

Tanto *Ethernet* como *LocalTalk* utilizan este tipo de topología.

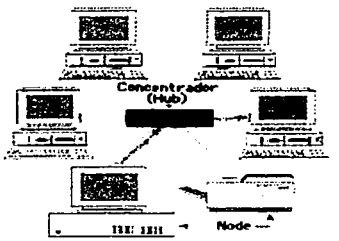

Figura 10. Topología estrella

Ventajas de la topología de estrella:

- Gran facilidad de instalación.
- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y su reparación.

Inconvenientes de la topología de estrella:

- Requiere más cable que la topología de bus.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
- Se han de comprar *hubs* o concentradores.

Topología de Estrella cableada / *Star-Wired Ring*

Físicamente parece una topología estrella pero el tipo de concentrador utilizado, la MAU (*Multi-station Access Unit*, Unidad de Acceso Multiestación) se encarga de interconectar internamente la red en forma de anillo.

Esta topología es la que se utiliza en redes *Token-Ring* (este protocolo se define más adelante en el presente capítulo).

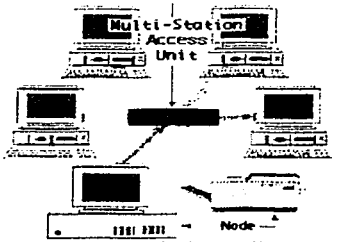

Figura 11. Topología de estrella cableada

Topología de Árbol / *Tree*

La topología de árbol combina características de la topología de estrella con la de *bus*. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red.

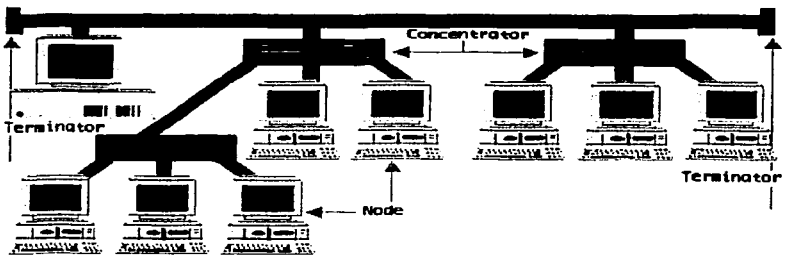

Figura 12. Topología de árbol.

Ventajas de la topología de árbol:

- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Inconvenientes de la topología de árbol:

- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo.
- Es más difícil de configurar.

Tabla 3.- Resumen de topologías físicas de redes

Topología	Cableado	Protocolo
Bus	Coaxial Par Trenzado Fibra óptica	*Ethernet* *LocalTalk*
Estrella	Par trenzado Fibra óptica	*Ethernet* *LocalTalk*
Estrella en Anillo	Par trenzado	*Token Ring*
Arbol	Coaxial Par trenzado Fibra óptica	*Ethernet*

Protocolos Redes LAN [6]

Un protocolo es un conjunto de normas que rigen la comunicación entre las computadoras de una red. Estas normas especifican que tipo de cables se utilizarán, que topología tendrá la red, que velocidad tendrán las comunicaciones y de que forma se accederá al canal de transmisión.

Los estándares más populares son: *Ethernet*, *Localtalk*, *Token ring*, FDDI (*Fiber Distributed Data Interface*).

Ethernet

Ethernet es hoy en día el estándar para las redes de área local. Tanto *Ethernet* (Versión 2) como el muy similar estándar IEEE802.3 definen un modo de acceso múltiple y de detección de colisiones, es el conocido *carrier sense multiple access/collision detection (CSMA/CD)*. Cuando una estación quiere acceder a la red escucha si hay alguna transmisión en curso y si no es así transmite. En el caso de que dos redes detecten probabilidad de emitir y emitan al mismo tiempo se producirá una colisión pero esto queda resuelto con los sensores de colisión que detectan esto y fuerzan una retransmisión de la información.

Tabla 4.- Velocidades de transmisión (Cableados)

Tipo de *Ethernet*	Velocidad (Mbps)	Distancia (m)	Media
10Base5 (IEEE 802.3)	10	500	Coaxial Grueso
10Base2 (IEEE 802.3)	10	185	Coaxial Fino
10BaseT (IEEE 802.3)	10	100	UTP
10BaseF (IEEE 802.3)	10	2000	Fibra Óptica

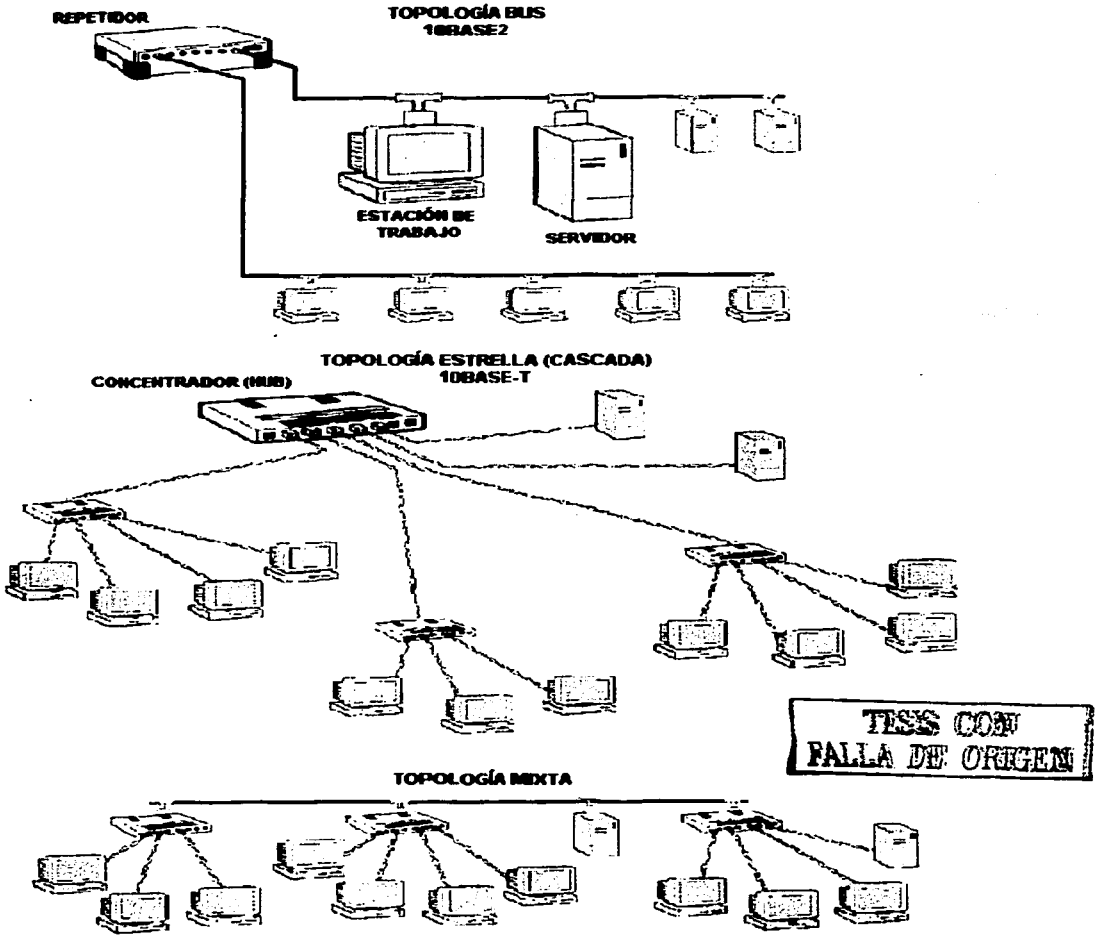

Figura 13. Diferentes topologías de red

Formatos de Trama (paquetes de comunicación)

Formatos de trama *Ethernet* IEEE 802.3

Ethernet define de qué manera se introducirán los datos en la red. Donde se indicará el receptor, el emisor donde irán los datos, donde irá el *checksum* (comprobación de datos), etc. Esto se define en la trama *Ethernet*. En la figura superior se puede ver la distribución de la información en cada paquete enviado. Se comienza con un preámbulo que termina al que sigue la trama en sí. El inicio de la trama es la información de la dirección de destino seguido de la dirección de procedencia a lo que sigue el tipo o la longitud de la información los datos y el *checksum* de la trama. El *checksum* (*Frame Check Sequence* FCS) se comprueba en la llegada para asegurarse de la correcta recepción de la información.

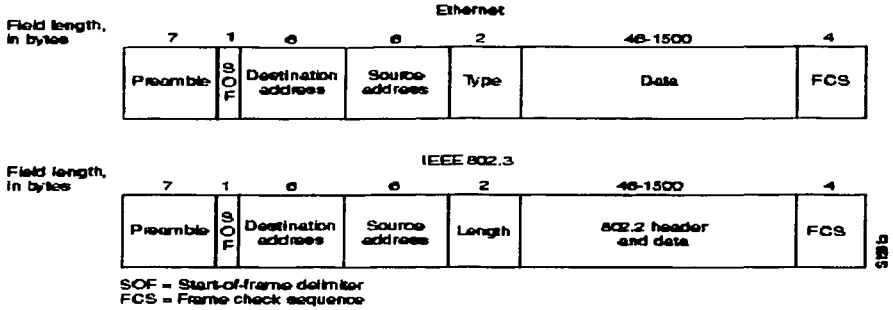

Figura 14. Formatos de trama

Para aumentar la velocidad de la red de 10Mbs a 100Mbs se han definido nuevos estándares de *Ethernet* denominados en conjunto *FastEthernet* (IEE802.3u).Tres nuevos tipos de redes *Ethernet* han visto la luz, como se muestra en la tabla 5. Estas únicamente pueden funcionar bajo la topología estrella.

Tabla 5.- Diferente Medio de *Fast Ethernet*

Tipo de *Ethernet*	Velocidad (Mbps)	Medio
100BaseTX (IEEE 802.3u)	100	UTP de categoría 5
100BaseFX (IEEE 802.3u)	100	Fibra óptica
100BaseT4 (IEEE 802.3u)	100	UTP de categoría 3 modificado *

* Se añaden dos líneas al cable UTP de categoría 3.

LocalTalk

El protocolo *LocalTalk* fue desarrollado por Apple Computer, Inc. para computadoras Macintosh. El método de acceso al medio es el CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*, Sensor de transporte de múltiple acceso con prevención de colisiones). Este método, similar al de *Ethernet* (CSMA/CD) se diferencia en que la computadora anuncia su transmisión antes de realizarla. Mediante el uso de adaptadores *LocalTalk* y cables UTP especiales se puede crear una red de computadoras Mac a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional aunque se puede crear una red cliente servidor con el sofware *AppleShare*.

Con el protocolo *LocalTalk* se pueden utilizar topologías bus, estrella o árbol usando cable UTP pero la velocidad de transmisión es muy inferior a la de *Ethernet*.

Token Ring

El protocolo *Token Ring* fue desarrollado por IBM a mediados de los 80. El modo de acceso al medio esta basado en el traspaso del testigo (*token passing*). En una red *Token Ring* las computadoras se conectan formando un anillo. Un testigo (*token*) electrónico pasa de una computadora a otra. Cuando se recibe este testigo se está en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes *Token Ring* se montan sobre una topología estrella cableada (*star-wired*) con par trenzado o fibra óptica. Se puede transmitir información a 4 o 16 Mbs. Cabe decir que el auge de *Ethernet* está causando un descenso cada vez mayor del uso de esta tecnología.

Tramas en *Token Ring*

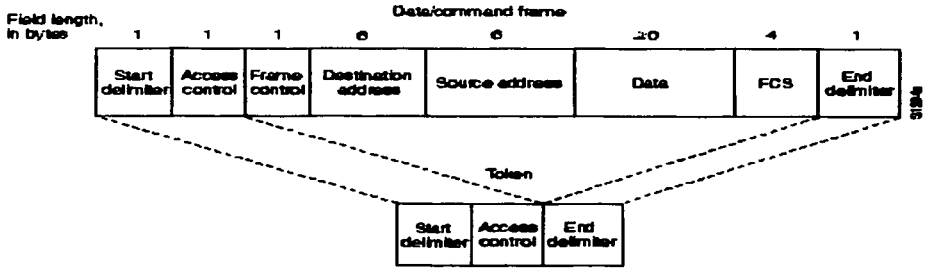

Figura 15. Trama de *token ring*

Como se puede ver, la trama de *Token Ring* es similar a la de *Ethernet*, la principal diferencia consiste en que a los datos se le agrega un *Token*, que es el que marca la prioridad de transmisión.

Propiedades:

- Arquitectura full-duplex y manipulación a nivel de bit.
- El Token se envía solo después de que la dirección origen ha regresado.
- El tráfico es regulado a través de bits de reserva y paridad de cada paquete.
- Usa códigos diferenciales
- Control centralizado con un reloj monitor activo,permitiendo paquetes muy largos.
- Medio: par trenzado.

Fiber Distributed Data Interface (FDDI)

FDDI son las siglas de *Fiber Distributed Data Interface* (interfase de datos de fibra distribuida). Este protocolo de red se utiliza principalmente para interconectar dos o más redes locales que con frecuencia distan grandes distancias.

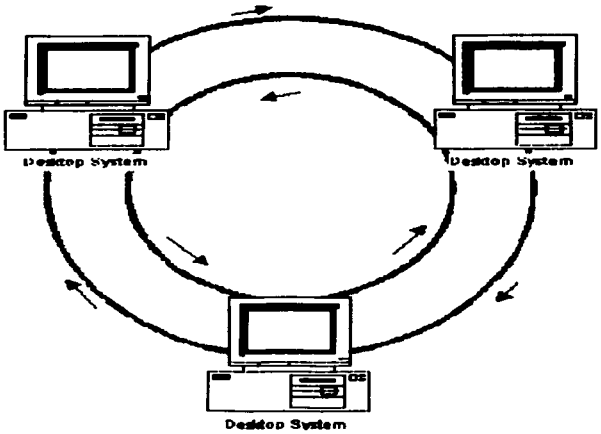

Figura 16. *Fiber Distributed Data Interface* (FDDI)

El método de acceso al medio utilizado por FDDI está basado también en el paso de testigo (*Token*). La diferencia es que en este tipo de redes la topología es de anillo dual (ver figura 16). La transmisión se da en uno de los anillos pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión (ver figura 17). Se monta sobre cables de fibra óptica y se pueden alcanzar velocidades de 100 Mbps.

Propiedades:

- Provee mayor ancho de banda que *Ethernet*.
- Utiliza fibra óptica para transferir datos codificados en pulsos de luz.
- 100 Mbps.
- Tolerancia a fallas.
- Tecnología *Token Ring*.
- Distancia de hasta 200 Kms.
- Hasta 100 estaciones conectadas.

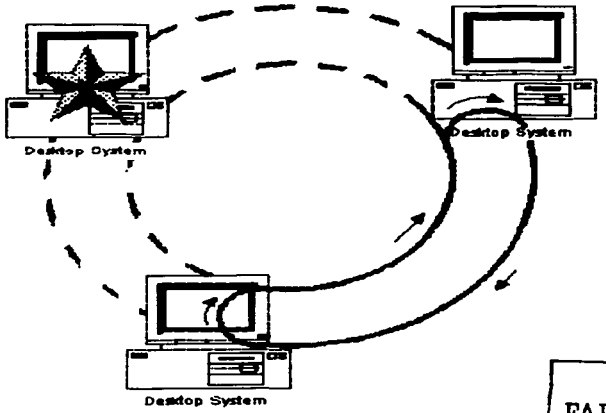

Figura 17. *Fiber Distributed Data Interface* (FDDI)

Tabla 6.- Resumen de Protocolos

Protocolo	Cable	Velocidad	Topología
Ethernet	Par trenzado, coaxial, fibra óptica	10 Mbps	Bus Linear, Estrella, Árbol
Fast Ethernet	Par trenzado, fibra óptica	100 Mbps	Estrella
LocalTalk	Par trenzado	23 Mbps	Bus Linear o Estrella
Token Ring	Par trenzado	4 Mbps - 16 Mbps	Anillo Cableado en estrella
FDDI	Fibra óptica	100 Mbps	Anillo dual

Principales componentes de las redes informáticas [10]

Las redes de computadoras se montan con una serie de componentes de uso común y que en mayor o menor medida siempre aparecerán en cualquier instalación.

Servidores

Los servidores de archivos conforman el corazón de la mayoría de las redes. Se trata de computadoras con mucha memoria RAM (1 Gigabytes), un enorme disco duro (160+ Gigabytes) y una rápida tarjeta de red (10/100). El sistema operativo de red se ejecuta sobre estos servidores así como las aplicaciones compartidas.

Un servidor de impresión se encargará de controlar gran parte del tráfico de red ya que será el que acceda a las demandas de las estaciones de trabajo, y el que les proporcione los servicios que pidan, impresión,

archivos, Internet, comunicarse entre si, etc. Está claro que se necesita una computadora con capacidad de guardar información de forma muy rápida y de compartirla con la misma velocidad.

Estaciones de trabajo

Son las computadoras conectadas al servidor. Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesitan una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Una estación de trabajo puede carecer de disquetera y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier computadora puede actuar como una estación de trabajo.

Tarjeta de Red

La tarjeta de red (NIC, *Network Interfase Card*, tarjeta de interfase de red) es la que conecta físicamente la computadora a la red. Son tarjetas que se conectan en la computadora como si se tratara de una tarjeta de video o cualquier otra tarjeta. Puesto que todos los accesos a red se realizan a través de ellas se deben utilizar tarjetas rápidas si se quiere comunicaciones fluidas.

Las tarjetas de red más populares son por supuesto las tarjetas *Ethernet*, existen también conectores *LocalTalk* así como tarjetas *TokenRing*.

Tarjetas *Ethernet*

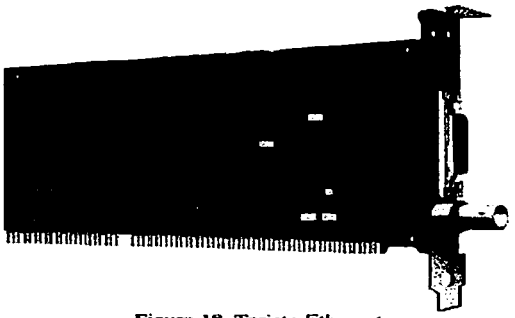

Figura 18. Tarjeta *Ethernet* con conector RJ-45, AUI, BNC

Conectores *LocalTalk*

Se utilizan para computadoras Mac, conectándose al puerto paralelo. En comparación con *Ethernet* la velocidad es muy baja, de 230KB frente a los 10 o 100 MB de la primera.

Tarjetas *Token Ring*

Son similares a las tarjetas *Ethernet* aunque el conector es diferente. Suele ser un DIN (conector redondo) de nueve pines.

Concentradores o *Hubs*

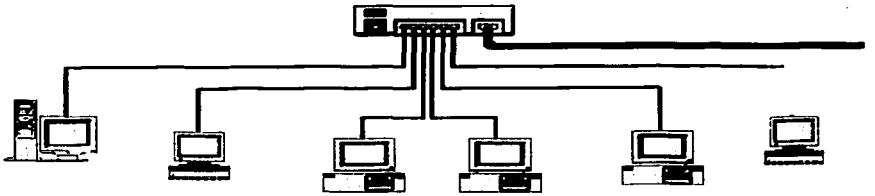

Figura 19. Concentrador

Un concentrador o *Hub* es un elemento que provee una conexión central para todos los cables de la red. Los *hubs* son "cajas" con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red. Los hay de tipo inteligente (*Switch*) que envían la información solo a quien ha de llegar mientras que los normales envían la información a todos los puntos de la red siendo las estaciones de trabajo las que decidirán si se quedan o no con esa información. Están provistos de salidas especiales para conectar otro *Hub* a uno de los conectores permitiendo así ampliaciones de la red.

Repetidores

Figura 20. Repetidor

Cuando una señal viaja a lo largo de un cable va perdiendo intensidad a medida que avanza. Esta pérdida de fuerza puede desembocar en una pérdida de información. Los repetidores amplifican la señal que reciben permitiendo así que la distancia entre dos puntos de la red sea mayor que la que un cable solo permite.

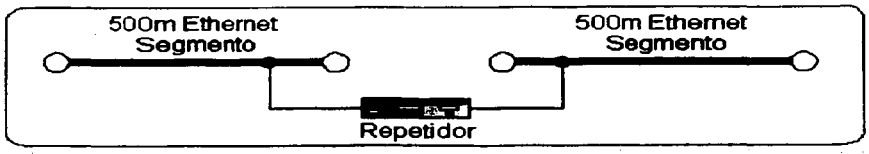

Figura 21. Repetidor

Puentes o *Bridges*

Los puentes se utilizan para segmentar redes grandes en redes más pequeñas. De esta forma solo saldrá de la red pequeña el tráfico destinado a otra red pequeña diferente mientras que todo el tráfico interno seguirá en la misma red. Con esto se consigue una reducción del tráfico de red.

Ruteador o *Routers*

Un ruteador dirige tráfico de una red a otra, se podría decir que es un puente superinteligente ya que es capaz de calcular cual será el camino más rápido para hacer llegar la información de un punto a otro. Es capaz también de asignar diferentes preferencias a los mensajes que fluyen por la red y dirigir unos por caminos más cortos que otros así como de buscar soluciones alternativas cuando un camino está muy cargado.

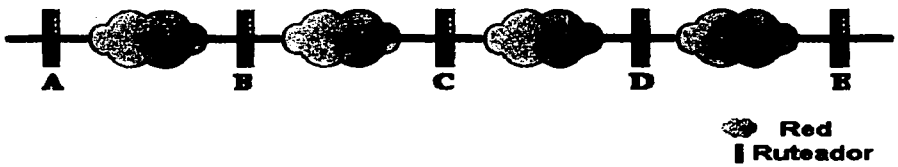

Figura 22. Ejemplo de uso en la configuración simple de Ruteadores

Mientras un puente conoce la dirección de las computadoras a cada uno de sus extremos un ruteador conoce la dirección tanto de las computadoras como de otros ruteadores y puentes y es capaz de buscar y analizar toda la red para encontrar el camino menos congestionado.

Firewalls

Los *firewalls* son barreras creadas entres redes privadas y redes públicas como por ejemplo Internet. Originalmente, fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. En la actualidad, los sistemas de seguridad proporcionados por terceras empresas, son la solución más escogida. Los *firewalls* son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado. Se definen entonces ciertas políticas de seguridad las que son implementadas a través de reglas en el *firewall* donde estas políticas típicamente se diseñan de forma que todo lo que no es expresamente autorizado, es prohibido por defecto. Un *firewall* protege la red interna de una

organización, de los usuarios que residen en redes externas, permite el paso entre las dos redes a sólo los paquetes de información autorizados y puede ser usado internamente, para formar una barrera de seguridad entre diferentes partes de una organización, como por ejemplo a estudiantes y usuarios administrativos de una universidad. Un *firewall* de nivel de red permite un control de acceso básico y poco flexible, pues permite aceptar o denegar el acceso a un nodo basándose sólo en la información que conoce a nivel de red. Es decir, se permite el acceso desde o hacia un nodo en forma total o simplemente no se permite. Por ejemplo, si una máquina es un servidor Web y a la vez servidor FTP, entonces puede resultar conveniente que sólo algunos clientes tengan acceso al servicio FTP, y que todos tengan acceso al servicio Web. Este tipo de control no es posible con un *firewall* de nivel de red, pues no existe forma de hacer la diferenciación de servicios que existen en una misma máquina que, por lo tanto, tendrá una misma dirección de red. La solución a este problema se hace filtrando a niveles superiores al de red, con lo que se obtiene un *firewall* flexible y eficiente, pero como desventaja se tiene un mayor consumo de procesador debido a la mayor cantidad de información que es necesario analizar.

Modelo OSI

En 1977, la Organización Internacional de Estándares (*Internacional Standard Organization, ISO*), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

Como se mencionó anteriormente, OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

Estos equipos presentan diferencias en:

- Procesador Central.
- Velocidad.
- Memoria.
- Dispositivos de Almacenamiento.
- Interfaces para Comunicaciones.
- Códigos de caracteres.
- Sistemas Operativos.

Estas diferencias propician que el problema de comunicación entre computadoras no tenga una solución simple.

Dividiendo el problema general de la comunicación, en problemas específicos, facilitamos la obtención de una solución a dicho problema.

Esta estrategia establece dos importantes beneficios:

Mayor comprensión del problema.

La solución de cada problema específico puede ser optimizada individualmente. Este modelo persigue un objetivo claro y bien definido:

Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independientemente del:

- Fabricante.
- Arquitectura.
- Localización.
- Sistema Operativo.

Este objetivo tiene las siguientes aplicaciones:

Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APLIACION.

Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones específicas diseñadas para atender el protocolo del nivel superior.

No especificar detalles de cada protocolo.

Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada nivel.

Estructura del Modelo OSI de ISO

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

Estructura multinivel: Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

Unidades de información: En cada nivel, la unidad de información tiene diferente nombre y estructura:

Niveles del Modelo OSI.

Aplicación.

Presentación.

Sesión.

Transporte.

Red.

Enlace de datos.

Físico.

La descripción de los 7 niveles es la siguiente:

Nivel Físico: Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

Definir conexiones físicas entre computadoras.

Describir el aspecto mecánico de la interfase física.

Describir el aspecto eléctrico de la interfase física.

Describir el aspecto funcional de la interfase física.

Definir la Técnica de Transmisión.

Definir el Tipo de Transmisión.

Definir la Codificación de Línea.

Definir la Velocidad de Transmisión.

Definir el Modo de Operación de la Línea de Datos.

Nivel Enlace de Datos: Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

Detectar errores en el nivel físico.

Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.

Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.

Enviar bloques de datos con el control necesario para la sincronía.

En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

Nivel de Red: Este nivel define el enrutamiento y el envío de paquetes entre redes.

Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.

Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).

Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.

Define el estado de los mensajes que se envían a nodos de la red.

Nivel de Transporte: Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento. Además, garantiza una entrega confiable de la información.

Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

Este nivel define como direccionar la localidad física de los dispositivos de la red.

Asigna una dirección única de transporte a cada usuario.

Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.

Define la manera de habilitar y deshabilitar las conexiones entre los nodos.

Determina el protocolo que garantiza el envío del mensaje.

Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

Nivel Sesión: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

Establece el inicio y termino de la sesión.

Recuperación de la sesión.

Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.

Referencia a los dispositivos por nombre y no por dirección.

Permite escribir programas que correrán en cualquier instalación de red.

Nivel Presentación: Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.

Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.

Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.

Opera el intercambio.

Opera la visualización.

Nivel Aplicación: Proporciona servicios al usuario del Modelo OSI.

Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.

Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (FTP), etc.

Capítulo II

CONFIGURACIÓN (SOFTWARE, WINDOWS)

Capítulo II: Configuración (Software, Windows)

Contando con los conocimientos presentados en el capítulo anterior, se puede ahora comprender mucho mejor la lógica de funcionamiento de lo relacionado a la teoría de redes (básica), tanto dispositivos físicos (*hardware*) como los recursos no tangibles (*software*), ahora bien, estos recursos de redes necesitan una configuración para que se pueda aprovechar la función para lo cual están diseñados. Dentro del presente capítulo se presenta una manera paso a paso y de manera ilustrada, la forma para poner a funcionar una red bajo Windows95/98.

Configuración de una red punto a punto en Win95/98 [19]

Para configurar el sistema operativo de forma que se pueda trabajar en red lo primero desde luego será comprar el cableado necesario e instalar la tarjeta de red. La tarjeta de red se instala como cualquier otra tarjeta que se instale en la computadora. Si esta es *Plug & Play* (lo más habitual hoy en día), no se tendrá más que enchufar la tarjeta, reiniciar la computadora y seguir los pasos que nos indica el asistente. Si no es así se deberá instalar la tarjeta a través del asistente "Agregar nuevo hardware" que se encuentra en el panel de control. Una vez instalada esta tarjeta ya se puede entrar en lo que es la auténtica configuración de red.

Para llevar a cabo cualquier configuración de red siempre se ha de seguir el mismo camino. Configuración, Panel de Control, Red. Con esto se despliega el siguiente cuadro.

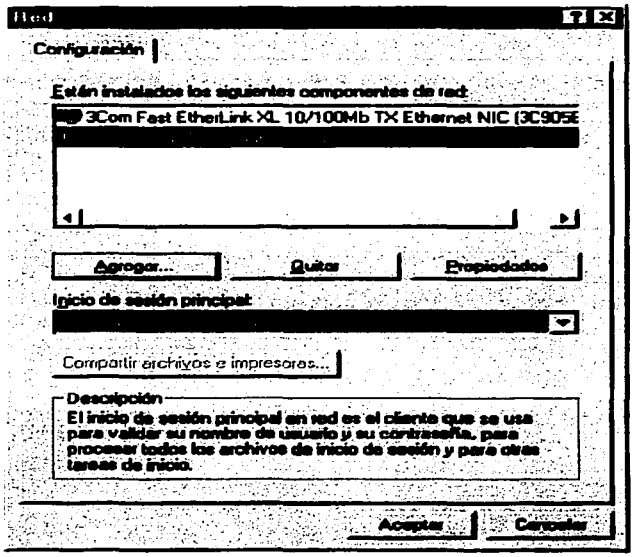

Figura 23. Propiedades de red

Se observa que aparece la tarjeta de red y debajo un icono con la leyenda "3Com TCAATDI Diagnostic TDI" (el cual solo aparece para tarjetas 3com, lo cual no afecta para la configuración de la red), esto es lo que aparece cuando se instala la tarjeta de red, es decir, todo esto llega aquí automáticamente.¿Qué es lo que se ha de añadir? Para trabajar en red se necesita en primer lugar una conexión física, como se muestra esto ya está, por lo tanto el siguiente paso es la instalación de los protocolos. En este caso se instalará el protocolo TCP/IP, para así ver su configuración, de todas formas, la instalación de otro protocolo sería idéntica a esta. Para instalar un protocolo se ha de pulsar el botón "Agregar".

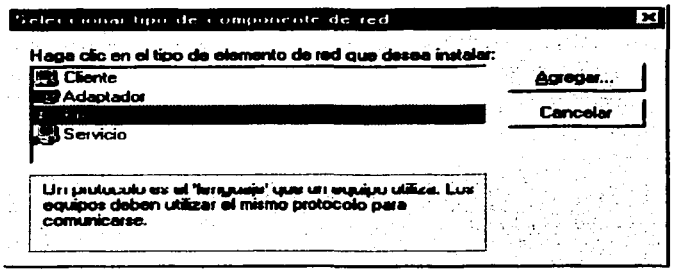

Figura 24. Instalando un protocolo

Aparecen cuatro opciones, agregar un cliente, agregar un Adaptador, agregar un Protocolo o agregar un Servicio. Agregar un adaptador instala una nueva tarjeta de red, agregar un protocolo instala un protocolo, lo mismo para servicio. Si se agrega un cliente se instalarán una serie de funciones que el sistema operativo necesita como funciones para trabajar con servidores Novell, o funciones para trabajar con servidores NT, es decir, se instalarán las funciones adicionales que el sistema operativo necesita para trabajar con otros servidores. Se dice que un cliente siempre necesitará que existan protocolos instalados, por ejemplo, el cliente para trabajar con servidores Novell exige que se haya instalado el protocolo IPX/SPX, de todas formas Windows se encargará de instalar automáticamente todos los protocolos necesarios por lo que no se debe preocupar por esto. Lo mismo ocurre con los servicios, los servicios son porciones del sistema operativo que permiten a la computadora llevar a cabo funciones de red como compartir archivos, impresoras, etc... Si un servicio requiere protocolos determinados el sistema se encargará de instalarlos automáticamente. En este caso se va a construir la casa desde los cimientos, una vez instalada la tarjeta, se instalará el protocolo TCP/IP.

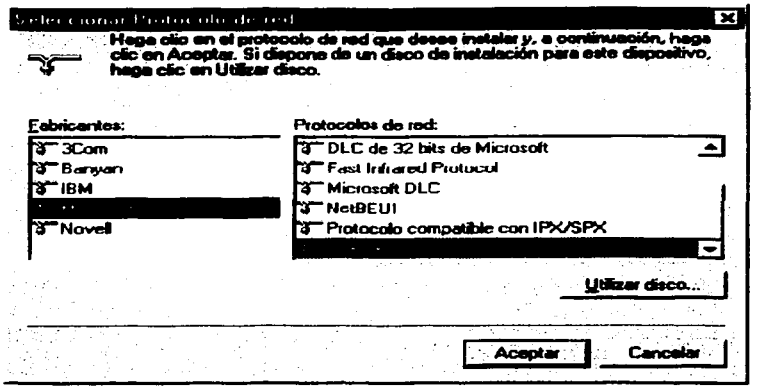

Figura 25. Protocolo TCP/IP

De todos los protocolos posibles se escogen los de Microsoft, y dentro de los de Microsoft TCP/IP.

Como se puede ver, aparte de TCP/IP ha aparecido el Cliente para redes Microsoft. Esto es porque Windows entiende que si se está instalando TCP/IP es por que se va a trabajar en red y para ello se necesitan ciertos añadidos sobre el sistema operativo, así que automáticamente se instala el Cliente para redes Microsoft. Más adelante habrá que configurar este cliente para redes. De momento se configura el protocolo instalado. Simplemente se tiene que señalar este protocolo y hacer click en "Propiedades", lo cual da como resultado la presentación de la ventana representada en la figura 26.

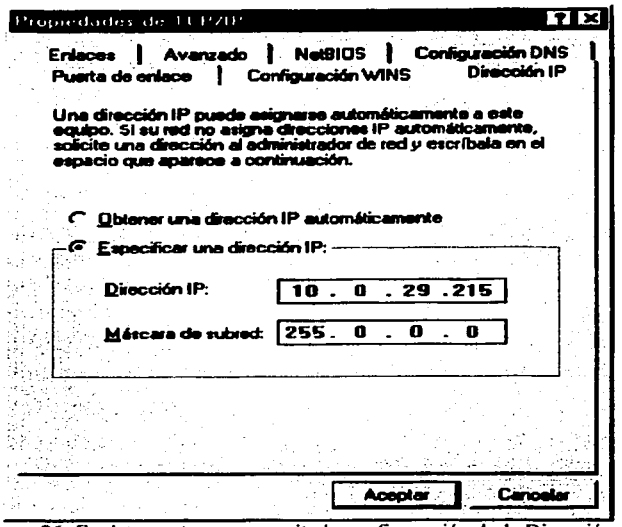

Figura 26. En ésta ventana se permite la configuración de la Dirección IP

Métodos de comunicación [10]

Direcciones MAC (*Media Access Control*, Control de Acceso de Medios)

Todos los equipos compatibles *Ethernet* poseen una **dirección MAC** única en el mundo, de 48 bits de longitud. Cada fabricante de equipos *Ethernet* tiene asignado un **segmento de direcciones**, y es responsabilidad de este asignar una dirección distinta a cada equipo. Las direcciones MAC están almacenadas en una pequeña memoria que poseen las tarjetas de red. Las direcciones MAC se representan en hexadecimal con el siguiente formato: **XX:XX:XX:XX:XX:XX**.

La información es enviada al bus agrupada en forma de **tramas o paquetes**. Estos paquetes contienen la dirección MAC de destino, la de origen, el tipo de datos, los datos a transmitir y un checksum de comprobación. En condiciones normales, una tarjeta *Ethernet* solo es capaz de "oír" los paquetes destinados a su dirección MAC o los destinados a todo el mundo (*BROADCAST*). La dirección MAC de *BROADCAST* es FF:FF:FF:FF:FF:FF

Protocolos IP y ARP

El protocolo IP (*Internet Protocol*, Protocolo de Internet), es un protocolo de red con direcciones de 32 bits, bajo el conocido formato **aaa.bbb.ccc.ddd, formando 4 grupos de 8 bits. La dirección de red IP puede ser dividida en dos partes, la dirección de red y la dirección de equipo. Si se está en una red conectada a Internet,**

la dirección de red será única en Internet, y la dirección de equipo será única en la red local, formando así una dirección IP única a nivel global.

Se mostrará un caso de conectividad entre máquinas de propia red IP, funcionando sobre un medio físico *Ethernet*.

Para enviar un paquete IP desde una estación 192.168.1.1 hacia la estación 192.168.1.2, es necesario conocer la dirección MAC de la estación de destino. Se podría solucionar con un archivo de configuración, asignando a cada dirección IP de la red, la correspondiente dirección MAC asociada a cada IP, pero sería poco práctico. Para solucionar este problema se desarrolló el protocolo ARP (*Address Resolution Protocol*, Protocolo de resolución de dirección). Cuando un equipo desea conocer la dirección MAC correspondiente a una IP, emite un paquete *BROADCAST* preguntando "¿Quien es el propietario de 192.168.1.2?". Todos los equipos de la red escuchan la petición, pero solo responde el destinatario: "aquí está 192.168.1.2 desde la dirección MAC xx:xx:xx:xx:xx:xx". Esta respuesta se almacena en el caché ARP del peticionario para usos posteriores, y procede a enviar el paquete al destinatario

Configuración [19]

A no ser que se esté en una red en la que haya un servidor (pueden ser Unix, NT, Linux, etc...) que se encargue de asignar **direcciones IP** automáticamente, a todos los equipos se les ha de otorgar una dirección IP. Aparte de esto se tendrá que asignar también una máscara de red. La dirección IP son cuatro dígitos separados por puntos al igual que la máscara de red. De estos cuatro números unos indican el número de red y otros el número de equipo dentro de la red. ¿Qué dígitos son la red y cuales son el equipo? Depende de la máscara de red. Lo que hay "encima" del 255 es número de red y lo que hay encima del "0" es el número de equipo. En este caso se ubica la PC en la red 10 y es el equipo 0.29.215. ¿Qué números utilizar para la máscaras y para la dirección IP? Para la dirección IP se pueden utilizar número entre 0 y 255. Para la máscara como sigue...

Los pares dirección Máscara de subred pueden ser de tres tipos

Tipo A:
Dirección IP: **1-126 . 0-255 . 0-255 . 0-255**
Máscara de subred: **255 . 0 . 0 . 0**

Tipo B:
Dirección IP: **128-191 . 0-255 . 0-255 . 0-255**
Máscara de subred: **255 . 255. 0 . 0**

Tipo C:
Dirección IP: **192-223 . 0-255 . 0-255 . 0-255**
Máscara de subred: **255 . 255.255 . 0**

Para redes internas se utilizan direcciones Tipo A con el primer dígito (el de red) un 10. Así pues, se pondrá una dirección como la de arriba. Con esto ya se ha configurado la parte más importante del protocolo TCP/IP.

Configuración de la Puerta de enlace (*Gateway*)

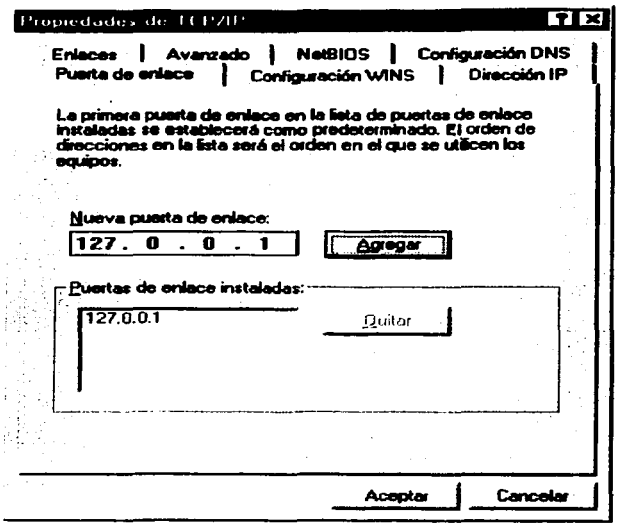

Figura 27. Puerta de enlace

De acuerdo con lo mencionado, una dirección IP hace referencia a una red y a un equipo dentro de la red. En este caso se está en la red 10 y se es el equipo 0.29.25. Si se quisiera conectar con un equipo de la red 11 se debería hacerlo a través de una puerta de enlace, esto es, un equipo que está en la red 10 y en la red 11 al mismo tiempo (esto se consigue con un servidor NT o Unix con dos tarjetas de red, cada una con una dirección). Aquí se dirá quien es ese equipo. Si no existen dos redes el concepto de gateway no tiene sentido por lo que este campo se puede dejar en blanco o se puede poner la dirección que arriba se observa. Esta dirección en lenguaje TCP/IP significa la propia computadora, es decir en este caso sería lo mismo poner 127.0.0.1 que 10.0.29.215. Así mismo la puerta de enlace es también la dirección IP de la máquina que puede permitir una salida del equipo de la red local a la red global llamada Internet.

Configuración del Servidor de Nombres de Dominio (*Domain Name Server*, DNS)

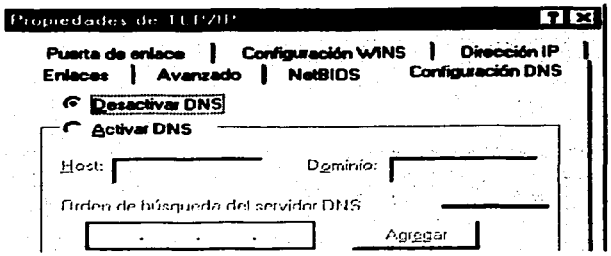

Figura 28. DNS

DNS (*Domain Name Server*) es una computadora en el que se almacena todas las direcciones de los equipos de red. A cada dirección se le asigna un nombre, por ejemplo a la dirección 10.0.29.215 se le asigna el nombre PC_Amiga. Cualquier llamada futura que se quiera hacer a esta computadora se puede hacer llamando a la computadora 10.0.29.215 o a la computadora PC_Amiga. Si en esta red no existe una de estas computadoras (habitualmente un servidor con NT, Unix o parecido) se desactivará esta opción.

Configuración de Enlaces

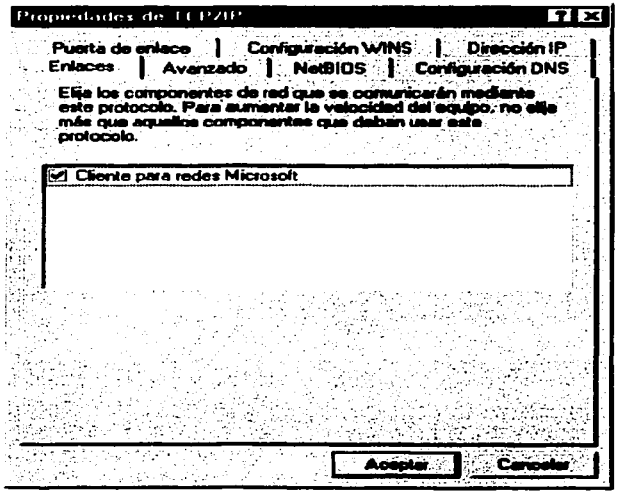

Figura 29. Enlaces

Esta configuración aparece en todos los protocolos. Indica que servicios o clientes van a utilizar este protocolo. En este caso se observa que aparece el único cliente que se tiene instalado. Como era de esperar, teniendo únicamente un protocolo y un cliente, el cliente llevará a cabo sus funciones mediante el uso de este protocolo. En caso de tener otros protocolos instalados se podría decidir si un cliente va a utilizar este protocolo o va a utilizar otro, y lo mismo para los servicios.

Una vez que se tiene instalado el protocolo se añade un servicio que sirve para compartir archivos e impresoras entre computadoras. Para añadirlo se elige añadir servicio...

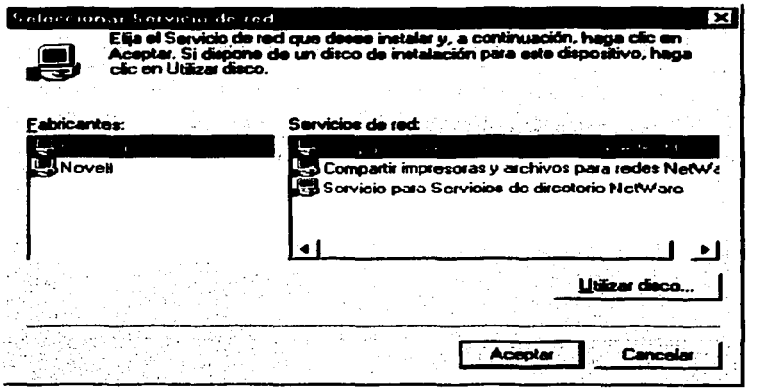

Figura 30. Servicios de red

Se elige este servicio y se verá que en la pantalla de configuración de red aparece un nuevo servicio.

Compartir archivos e impresoras

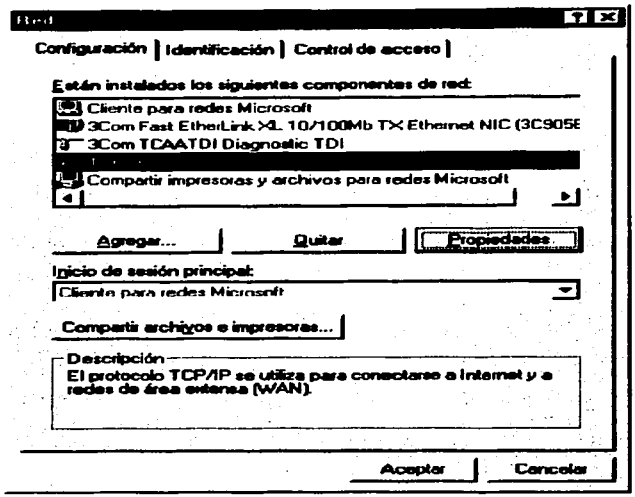

Figura 31. Propiedades de red

Un nuevo servicio llamado compartir impresoras y archivos para redes Microsoft ha aparecido. Si ahora se da doble click en Compartir archivos e impresoras se podrá decidir si se va a compartir archivos, impresoras, ambos o ninguno.

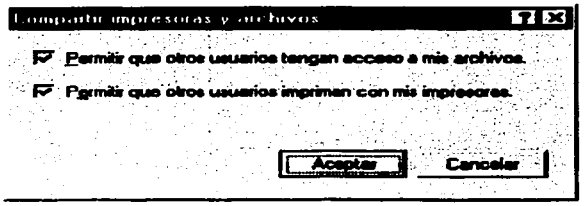

Figura 32. Compartir recursos

A partir de ahora se podrá compartir impresoras y archivos utilizando el servicio instalado que a su vez utilizará al protocolo TCP/IP, el cual utilizará a la tarjeta de red instalada.

Cliente para redes Microsoft

Se sigue con la configuración de la red. Ya se ha instalado la tarjeta, se ha añadido el protocolo TCP/IP y el servicio para compartir archivos e impresoras. Se ha configurado los dos últimos. Ahora se configurará el Cliente para redes Microsoft y se terminará la configuración general de red.

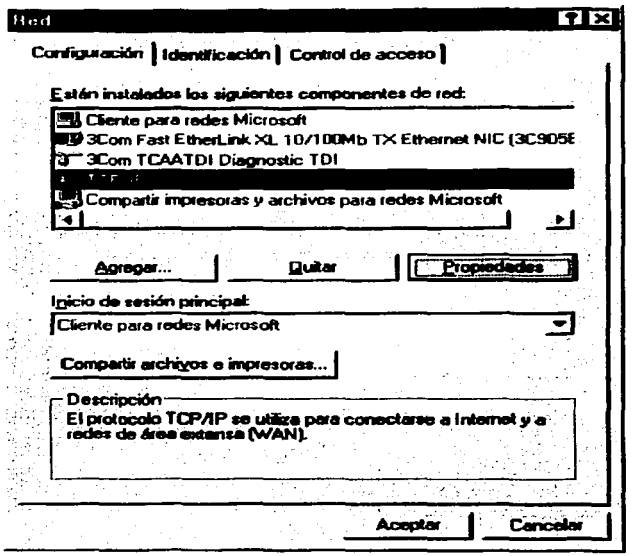

Figura 33. Cliente para redes Microsoft

Se selecciona Cliente para redes Microsoft y se pulsa "Propiedades". Esto es lo que aparecerá:

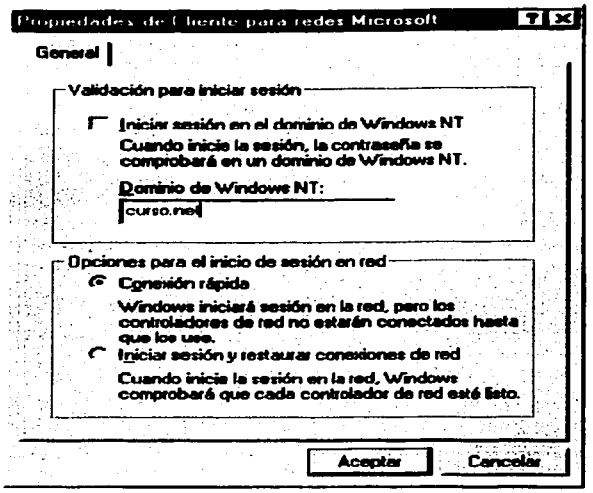

Figura 34. Propiedades de cliente para redes Microsoft

La primera opción que se tiene es iniciar una sesión en el dominio de Windows NT. Si en esta red existe un servidor NT y se utilizan recursos de este se deberá activar esa opción para que el servidor reconozca como usuarios y ofrezca sus servicios. Si se encuentra activa, pedirá un nombre de dominio, esto no es más que el nombre que Windows NT le da a la red, en este caso **curso.net**.

Otra opción que aparece es la conexión rápida o el Inicio de sesión y la restauración de conexiones, si se elige el primero no se cargarán en memoria los elementos necesarios para trabajar en red hasta que el usuario realice una operación de red, si se elige el segundo se cargarán todos los elementos necesarios para el trabajo en red tan pronto como se inicia la computadora.

Con esto finaliza la configuración del Cliente para redes Microsoft.

Grupos de Trabajo

El siguiente paso es terminar con la configuración general de red. Para ello en propiedades de red se debe señalar la pestaña de Identificación.

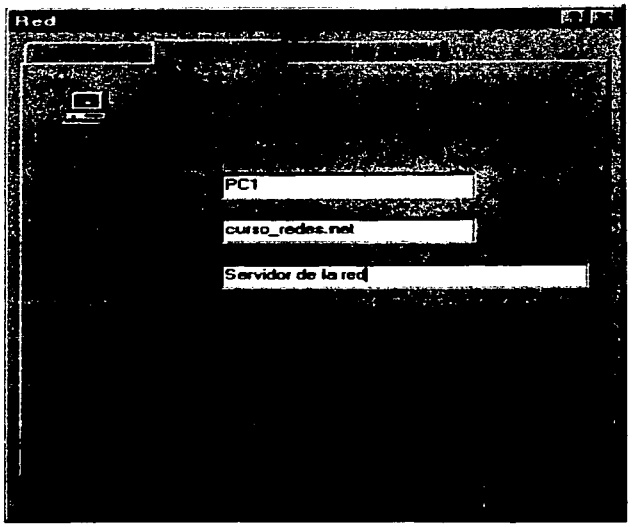

Figura 35. Identificación de la máquina

En esta ventana se otorga un nombre a la PC, se puede poner el que se desee. Este será el nombre con el que se verá a dicho equipo en la red más adelante. También se puede introducir un comentario, este comentario será el que aparezca en la ventana de entorno de red cuando se seleccione la PC.

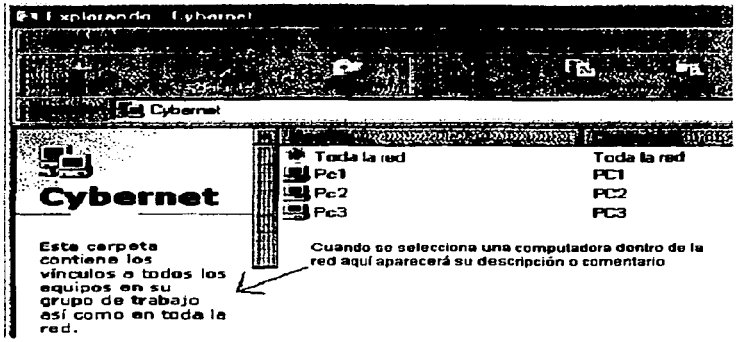

Figura 36. Entorno de red

Un concepto importante que también aparece es el de grupo de trabajo. Se recuerda que NT daba un nombre a la red, y ese nombre es conocido como el dominio. En caso de que no se tenga más que una red punto a punto el concepto de dominio desaparece pues no se tiene servidores NT, sin embargo, y siguiendo la misma filosofía el conjunto de la red recibe un nombre que es el de **Grupo de trabajo**. Todas las computadoras de dicha red deben pertenecer al mismo grupo de trabajo o no será posible localizarlas mediante la ventana de entorno de red. En este ejemplo las tres computadoras que se tienen están en el grupo de trabajo curso_redes.net. Podría haber más computadoras en la misma red (conectados físicamente) pero si no se especifica en la configuración de red de estas computadoras que el grupo de trabajo al que están adscritos es curso_redes.net no se podrán comunicar entre ellas.

Con esto solo queda configurar el Control de Acceso para acabar con la configuración de red general.

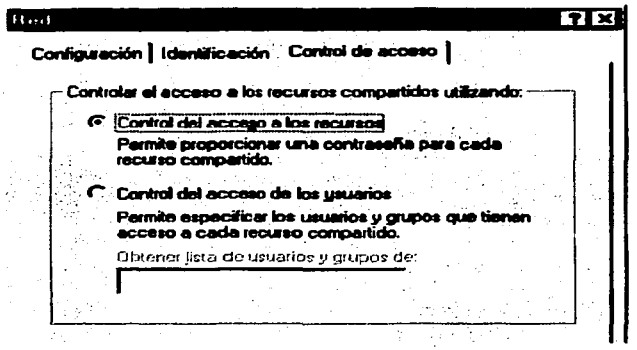

Figura 37. Control de acceso

Este es el último paso. Si se decide compartir archivos o impresoras de la propia computadora se puede especificar una contraseña para cada elemento compartido. Esta sería la primera opción. Sin embargo, si se está en una red con un servidor NT, este tendrá una lista de todos los usuarios existentes y los permisos de uso que estos usuarios tienen en la red. Activando la segunda opción se puede utilizar la lista del servidor NT, solo habrá que especificar cual es el dominio de dicho servidor.

Capítulo III

APLICACIÓN E INSTALACIÓN

Capítulo III: Aplicación e instalación

Uno de los objetivos es compartir recursos, como por ejemplo impresoras a través de la red, esto es, imprimir desde un equipo en la impresora que se instaló físicamente en otro equipo. Para ello parece evidente que se han de conectar físicamente las dos computadoras. De las múltiples soluciones que existen para conectar equipos físicamente en red (*Ethernet* 10base2, 10baseT, 100baseTX, TokenRing, etc...) se debe escoger una cualquiera. En este caso se escogió la solución más habitual, una red ***Ethernet* 10baseT**. Sobre *Ethernet* 10baseT se deben instalar unos protocolos que permitan la comunicación entre computadoras. Se han escogido el conjunto de protocolos **TCP/IP** como se podrían haber escogido otros protocolos de red (NetBeui, IPX/SPX, etc.). Una vez instalados los protocolos se necesitan instalar aplicaciones de red y esto se ha hecho instalando el **Servicio para compartir Archivos e Impresoras**. Todo esto se ha llevado a cabo sobre Windows 98. Se podría haber optado por soluciones diferentes. Se podría haber escogido una red 100baseTX, el protocolo IPX/SPX y el sistema operativo de red Novell o se podría haber utilizado una red *TokenRing*, con protocolos TCP/IP y sistema operativo Unix. La decisión siempre es la misma, elegir un tipo de red, elegir los protocolos a utilizar y elegir el sistema operativo de red. De hecho, esto se suele simplificar a elegir un tipo de red y un sistema operativo de red pues los protocolos y aplicaciones necesarios para el trabajo en red siempre irán incluidos en este.

Cuando se este pensando en conectar en red una impresora, el proceso de razonamiento a seguir es el mismo. En primer lugar se ha de saber a que tipo de redes se puede conectar a la máquina, esto depende en gran medida de los conectores de la tarjeta de red de ésta. Una impresora de hoy día podrá utilizarse seguramente en una red *Ethernet* 10base2, 10baseT, 100baseT, o *TokenRing*, este tipo de datos siempre aparece en la documentación de la impresora los mismo pasa con los protocolos soportados y servicios de red soportados.

A partir de este punto ya se cuenta con las bases teóricas para poder instalar una red local contando con ello recursos compartidos, ahora para complementar los servicios que brindará esta sala de servicios de información química, se propone la instalación de un servidor Linux para servicios específicos tales como correo electrónico, servidor de paginas WWW (*World Wide Web*), grupos de discusión, compartir archivos vía Internet (FTP: *File Transfer Protocol*), etc.

Preparativos para instalar Linux [18]

Uno de los puntos más importantes para instalar Linux es tener listo el disco duro. Parece un tanto raro el comentario pero ciertamente es donde más de un usuario se pierde, especialmente cuando tienen que particionar y cosas así, por lo que lo se explica brevemente.

Dado que actualmente la mayoría de las PC llegan con Windows preinstalado (¿la mayoría?, más bien todas), los usuarios no se preocupan por mucho más que sólo prenderla y cuando llega el caso, reinstalar con un CD, pero cuando tiene que hacer que el disco duro contenga otro sistema operativo (incluso otra versión de Windows), necesitar partir (particionar) el disco duro. Y aquí se empieza con los problemas.

En el caso que se tenga la posibilidad de adquir otro disco duro para instalar Linux, es mejor hacerlo y se ahorrará todo lo relativo a particionamiento de ésta sección, pero en caso contrario, se procederá a particionar el disco.

Un disco duro se consta, físicamente, en cilindros y cada uno de estos se divide en sectores, regularmente de 512 bytes y es en este espacio donde la información es grabada. En el momento que se indica que un disco se divida en varias unidades, se realiza el proceso llamado particionamiento, en el que se le asigna un espacio específico a cada partición.

Verificando el hardware

Un elemento que regularmente los usuarios novatos pasan por alto es el relativo a verificar la compatibilidad y estado de su hardware, lo que puede traer como consecuencia que el sistema no quede bien instalado, sea inestable o de plano no funcione por completo el instalador, por lo que se deben verificar los siguientes puntos:

- Revisar que el hardware esté soportado por la distribución que se va a utilizar.
- Revisar que funcionen correctamente las tarjetas (red, sonido, módem).
- Revisar que el disco duro no tenga sectores dañados (ejecutar el scandisk).
- Si se tienen problemas con Windows (lo que no es raro), como que se congele la máquina o no termine de encender, se recomienda mandarla a un servicio técnico para que revisen la tarjeta madre o el estado del RAM (*Random Access Memory*, memoria de acceso aleatorio).

Las revisiones de compatibilidad de hardware, es decir podemos saber por adelantado antes de instalar Linux si este va a funcionar sin problemas en la máquina elegida, se pueden buscar en:

- Red Hat: http://hardware.redhat.com/hcl/
- Mandrake: http://www.linux-mandrake.com/en/hardware.php3
- SuSe: http://hardwaredb.suse.de/index.php
- Debian: http://www.debian.org/
- Slackwave: http://www.slackware.com

Para otras distribuciones de Linux se deberá revisar la página Web del proveedor.

En los casos de hardware desconocido o no compatible (caso clásico son los winmódems y softmódems) o que se tenga dañada alguna tarjeta, lo más recomendable es adquirir uno nuevo. Para el caso concreto de los módems, casi cualquier externo por hardware funciona, ya que estos cuentan con todas las funciones necesarias directamente en sus circuitos y no dependen del sistema operativo dentro del cual funcione.

Linux no soporta ciertos dispositivos y tarjetas debido a que los controladores los hacen los mismos miembros de la comunidad Linux y esto es posible sólo cuando el fabricante libera las especificaciones de su hardware, por eso siempre hay un cierto período desde que un nuevo dispositivo es lanzado, hasta que lo soporte este sistema operativo; caso contrario a Windows/Macintosh, ya que los fabricantes mismos son quienes desarrollan y prueban los controladores. El caso de los módems por software (winmódem/softmódem) es especial, ya que diversas funciones que debería manejar el hardware se le relega a que las maneje Windows directamente, lo que es una ventaja para los fabricantes al ser muy baratos de producir, pero que imposibilita su uso fuera del sistema operativo de las ventanas.

Una revisión previa es importante, ya que es frecuente que un usuario incauto simplemente no pueda configurar su móden, tarjeta de red o de sonido y le eche la culpa al sistema operativo, o peor aún cuando un hardware dañado interrumpa la instalación, lo que los lleva a decir "Linux no sirve". El caso es sencillo, es el hardware, no el software. Si aparentemente todo está bien, se puede iniciar la instalación.

Antes que nada, se respalda

Se recomienda mucho respaldar la información del disco duro; para lo cual existen diversas opciones, tanto diferentes dispositivos externos creados específicamente para ello, así también se puede usar alguna unidad en red para guardar la información importante que exista en el disco duro antes de iniciar la instalación de Linux, también se puede utilizar alguna herramienta para generar una imagen del disco, como:

- Partition Image for Linux (http://www.partimage.org)
- Norton Ghost (http://www.symantec.com/sabu/ghost/ghost_personal)
- PowerQuest Drive Image (http://www.powerquest.com/driveimage)

¿Para que se particiona?

Los motivos para particionar son varios e incluso es aconsejable aún cuando no se vaya a instalar otro sistema operativo, porque:

- Permite las partes donde se guarda la información y donde se guardan los programas, de manera que si se corrompe una unidad, no se pierde todo. Útil también con muchos virus que atacan la unidad C de una PC.
- Mejora el desempeño del disco duro, al tener que leer sectores más pequeños de disco duro y no toda la unidad.
- Limita el tamaño al que pueden crecer las carpetas de diversos usuarios (en ambientes de redes), para evitar que saturen el disco duro y el sistema operativo ya no pueda operar.

¿Con que se particiona?

Desde DOS se puede utilizar una muy confiable pero limitada herramienta llamada *fdisk*, la cual puede eliminar y crear nuevas particiones, sin embargo el contenido del disco duro se pierde y no hay manera de recuperarlo. Para activarlo simplemente es necesario, desde el prompt de DOS, teclear fdisk, eliminar todas las particiones existentes y luego crear las nuevas, después de salir de fdisk se debe formater las unidades ya que se pierde absolutamente todo. **Nota**: esta utilería no puede funcionar desde Windows, es necesario iniciar una sesión de DOS para ello.

Para particionar mediante fdisk se puede leer en este COMO (*HOWTO*) de Linuxdoc:
http://www.linuxdoc.org/HOWTO/mini/Partition/partition-5.html.

OK, era un susto, si se pueden recuperar particiones creadas con fdisk, pero mejor ser cuidadoso y ahorrar el problema, para esto se puede consultar este manual para soporte:
http://www.linuxdoc.org/HOWTO/mini/Partition/recovering.html.

Otras opciones para crear particiones son:

- FIPS. Legendaria herramienta libre que se ditribuye con Red Hat y otras distribuiciones de Linux desde hace tiempo, pero que tiene varias limitaciones, es software libre (http://www.igd.fhg.de/~aschaefe/fips).
- parted: Particionador del proyecto GNU, es software libre (http://www.gnu.org/software/parted/parted.html).
- Partition Magic: Permite crear, eliminar, mover y modificar las particiones desde un entorno gráfico, es software comercial - $70 USD - (http://www.powerquest.com/partitionmagic/index.html)
- Disk Drake: Script en Perl/Gtk para crear, modificar y eliminar particiones que se distribuye principalmente con Mandrake, es software libre (http://www.linux-mandrake.com/diskdrake)
- Disk Druid: Es el particionador por defecto de la instalación de Red Hat, software libre.
- Ranish Partition Manager: tiene un sistema de arranque compatible con Windows 9x/NT/2000 y Linux, es software libre (http://www.ranish.com/part/)
- The Partition Resizer v. 1.3.4: permite mover y modificar pariciones existentes, freeware (http://www.utilitygeek.com/cgi-bin/download.pl?http://members.nbci.com/Zeleps/Files/PRESZ134.ZIP)

¿Cómo dividir el disco duro?

El tamaño de las particiones dependen del tamaño del disco duro, es lógico que mientras más grande es éste, más espacio se puede dejar a Windows por un lado y Linux por el otro, pero...

Cuidado. Un aspecto muy importante es el hecho que muchos BIOS (*Basic Input Output System*, sistema básico de entrada salida) , incluyendo los de algunas computadoras nuevas (contra lo que dicen los fabricantes), no pueden iniciar un sistema operativo que se encuentre después del cilindro 1024 (equivalente aproximadamente a 7,168 MB), por lo que al determinar el tamaño se debe tener cuidado donde colocar la partición de Linux, es decir si se instalan dos sistemas operativos en dos particiones diferentes dentro de un mismo disco duro, el sistema operativo que quede físicamente grabado después del cilindro que corresponde a los 7,168 MB no podrá ser reconocido por el sistema (*hardware*) y por lo tanto será inoperable.

En principio, a cada sistema operativo habrá que dejarle el espacio suficiente para que trabaje, lo cual es variable, por ejemplo, Windows 95 ó 98 pueden funcionar dentro de particiones de 3 GB, con espacio para las aplicaciones y archivos, pero Windows 2000 necesita de al menos 8 GB para trabajar bien como estación de trabajo (*workstation*, como servervidor es mucho más); Red Hat necesita al menos de 600 MB para una instalación mínima, aparte va el espacio para usuarios, archivos de log y demás; es cosa de acomodar lo que se vaya a cargar para determinar cuanto espacio necesitan.

Otro comentario es que, regularmente, Windows debe ir en la primera partición y que este sistema operativo es el "propietario" del *Master Boot Record* (MBR), que se ubica en el sector 0 del disco y que tiene la información para el arranque de (los) sistema(s) operativo(s). En el caso de que no se pueda instalar el arranque de Linux antes del cilindro 1024 y que no quiera iniciar después de instalarlo, es posible que sea más fácil utilizar un disco de arranque en vez de luchar en un reacomodo del la información del disco duro, que posiblemente no funcione.

Se puede obtener más información en:

- http://sdb.suse.de/sdb/en/html/1024_Zylinder.html
- http://www.linuxdoc.org/HOWTO/mini/Linux+Win95/

¿Cómo identificar la unidad donde se va a instalar Linux?

Cuando se observa un disco duro o unidades dentro de Windows, se presentan como letras del abecedario (C, D, E, etc.) pero dentro de Linux, es bastante diferente, ya que su estructura semeja un árbol donde cada partición y dispositivo de lectura / escritura se representa como un directorio, los nombres de las unidades de disco duro son:

- hda: disco duro principal
- hdb: disco duro secundario
- hda1: primera partición del disco duro principal.
- hdb2: segunda partición del disco secundario

Ahora, para ejemplificar todo este proceso, suponer que se tiene un disco duro de 20 GB y generar dos particiones, una de 5 GB para Windows y el resto para Linux, entonces es **hda1** (Windows) y **hda2** (Linux), siendo en este último donde se crearían las particiones del sistema.

¿Qué particiones se necesitan para Linux?

OJO. Estas particiones se crean al momento de instalar, no de dividir el disco duro para varios sistemas operativos, pero es importante conocerlas de antemano.

En principio sólo se pueden montar tres y es suficiente para que funcione:

- swap. Espacio físico para la memoria virtual del sistema, tradicionalmente debe ser del doble del tamaño de la memoria RAM total del sistema.
- /boot. Es la partición donde se leen los parámetros para iniciar el sistema (kernel) y que preferentemente debe ir antes del cilindro 1024 y debe ser de al menos 16 MB. El resto de la instalación puede estar en cualquier otro lado.
- / (RAIZ). Si, no es un error, es un "slash" o diagonal, es donde se coloca el sistema operativo, carpetas de temporales e información de usuarios.

Pero otras particiones son:

- /var. Contiene el spool (cola de proceso) de mail e impresión, los archivos de log y archivos similares.
- /usr. Contiene la mayoría de los binarios (ejecutables), bibliotecas compartidas, manuales, datos de aplicaciones e imágenes que utiliza el sistema, cabeceras de desarrollo, el árbol del kernel y documentación.
- /tmp. Archivos temporales que generan los programas.
- /home. Donde se colocan las carpetas de cada usuario con los perfiles de cada cuenta.

Por costumbre (y experiencia) se recomienda crear particiones independientes para /boot, / (raíz), /home, /var y swap. También es aconsejable una para /usr.

Seleccionar una distribución

A diferencia de Windows o MacOS, Linux tiene muchos fabricantes (se calcula que son aproximadamente 250 diferentes) y que soportan una amplia gama de arquitecturas (tipos de procesadores y por tanto funcionamiento), como es PowerPC, MIPS, RISC y otras excentricidades, pero la más común es para Intel de la serie x86 (80386, 80486, Pentium, AMD K5, AMD K7, Athlon, etc.), siendo ésta la base de este trabajo.

Elegir la distribución puede no ser, de todas formas, muy difícil, ya que más bien depende del nivel de conocimientos y en ocasiones, del bolsillo. Esto último es un poco engañoso, pero luego se comentará al respecto.

Existen distribuciones muy sólidas y confiables, como Slackwave o Debian, pero que no están tan acercadas a los usuarios novatos, lo que desde la instalación podría representar un problema; otras más buscan un acercamiento comercial como es SuSe o Caldera, lo que implica que existe un costo, por obtenerlas; en otras opciones se encuentra Red Hat o Mandrake que están en un punto intermedio, donde se acercan bastante al usuario medio pero que tienen una gran cantidad de aplicaciones para servidores y *workstations* (estaciones de trabajo), de hecho Red Hat es virtualmente el líder del mercado, aunque a Mandrake se le reconoce como una de las distribuciones más sencillas de instalar y personalizar; también hay casos especiales que buscan ofrecer el acceso de Linux desde Windows, como es Winlinux, pero antes de que se empiece a descargarlo (de algun sitio público de la red), se advierte que la versión completa, sin soporte técnico, cuesta $20 USD.

Respecto al costo, se recuerda que la traducción REAL de "*Free Software*" es Software LIBRE, no GRATUITO. Aquí no se debe confundir la libertad con el precio que se cobra por la obtención del cd que contiene la instalación de Linux, porque si bien este tipo de aplicaciones reducen el costo de propiedad al no pagar licencias, se debe hacer una inversión en capacitación, soporte técnico y hasta en hardware, así que si se está en esto porque no se tiene dinero para pagar el MS Office, mejor pensarlo dos veces, ya que no el no contar con recursos económicos no es razón suficiente para elegir la instalación de Linux.

Disco de arranque para la instalación

Luego de tener Windows en la computadora (no afecta si se configuran todos los parámetros de red y dispositivos o no), se puede comenzar a instalar Linux. El primer paso es obtener un disco de inicio de la instalación de la distribución de Linux (en caso que la PC no pueda iniciar desde el CD-ROM), que se genera de la siguiente forma:

1. Se inserta un disquete nuevo en la unidad correspondiente.
2. Se inserta el primer CD de Linux.
3. Se localiza en el CD la carpeta "dosutils" (regularmente en su raíz). Se recomienda leer el archivo "README" para tener un poco más de información.
4. Ejecutar el programa "rawrite.exe".
5. A continuación se le preguntará por la "imagen" que se utilizará, se teclea: D:\images\boot.img (o la unidad del CD-ROM).
6. En seguida se le preguntará por la unidad en donde se instalará esta "imagen". En este caso se refiere al floppy de 3½ pulgadas, así que se teclea "a" o bien "b", según corresponda.
7. Después de algunos segundos, el disquete que se introdujo, estará listo.

En un momento determinado del procedimiento, se nos preguntará si se desea instalar **Lilo** (Linux Loader) o **Grub** (este puede no existir en ciertas distribuciones o versiones) para iniciar Linux. Se debe verificar que se reconozca la partición de Windows. En el caso de que se instale cualquiera de los dos en hda1 (unidad C en Windoows y MS-DOS) o en la partición donde se encuentra Linux. Este pequeño programa permite arrancar distintos sistemas operativos en una misma PC si los hubiese. De forma predeterminada, si se tiene instalado Windows o MS-DOS en la unidad C del disco duro, al reiniciar el sistema podrá acceder a uno de estos sistemas operativos tecleando "dos" en el prompt de Lilo o a Linux con solo presionar la tecla ENTER. Si por alguna razón se desea desinstalar Lilo del disco duro, se utiliza fdisk de MS-DOS o Windows y se utiliza el siguiente comando en el símbolo de sistema de MS-DOS:

```
fdisk /mbr
```

Si la instalación de Linux no queda antes del cilindro 1024, será recomendable que se le inicie mediante un disquete de arranque, mismo que se podrá crear al terminar la instalación.

Inicio dual con Windows NT/2000/XP [17]

Las versiones de Windows 95/98/Me pueden ser inicializadas con el procedimiento anterior, pero para las versiones de Windows a 32 bits, como Windows NT/2000/XP, es necesario utilizar el siguiente procedimiento:

1. Se instala Windows en una partición.
2. Se instala Linux en otra.
3. Se inicia Linux desde un disquete de arranque.
4. En el prompt se teclea "cp /dosc/bootsect.dos /dosc/bootsect.lnx".
5. Se hace una copia de el kernel en /dosc/linux/vmlinux. El kernel se encuentra en la partición /boot.
6. Utilizando un editor de texto (por ejemplo: vi, emacs o pico), se edita el archivo "/dosc/boot.ini" y se modifica para que se vea así:

```
[boot loader]
timeout=30
default=c:\bootsect.lnx
[operating systems]
c:\bootsect.lnx="Linux"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation
Version 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation
Version 4.00 [VGA mode]" /basevideo /sos
C:\="Microsoft Windows"
```

7. De la misma forma, hay que modificar el archivo /etc/lilo.conf de la siguiente forma

```
boot=/dosc/bootsect.lnx
map=/boot/map.lnx
install=/boot/boot.b
image=/dosc/linux/vmlinux
          label=linux
          root=/dev/hdb2
          read-only
```

8. Se guardan los cambios de lilo.conf y desde el prompt se ejecuta "lilo" (sin comillas) para que se tomen los cambios en el arranque.
9. Cuando se reinicie la máquina, el arranque de NT deberá presentar la entrada "linux", la que al ser seleccionada, deberá iniciar el arranque de Linux.

Cómo configurar correctamente los parámetros de red

Configurar los parámetros de red en una estación de trabajo Linux o un servidor no es realmente complicado. Solamente requerirá de algunos conocimientos básicos sobre redes y cualquier editor de texto.

Procedimientos

La marca es lo que menos interesa, lo que es importante es que se determine con exactitud que chipset utiliza la tarjeta de red. Esto puede determinarse examinando físicamente la tarjeta de red o bien examinando a detalle la salida en pantalla que se obtiene al ejecutar el siguiente comando:

```
less /proc/pci | grep  Ethernet
```

Lo cual devuelve una salida similar a la siguiente (en el caso de una tarjeta 3Com 905 C)

```
Ethernet controller: 3Com Corporation 3c905C-TX [Fast Etherlink] (rev 120).
```

Debe editarse con un procesador de texto /etc/modules.conf o conf.modules y debe verificarse que el módulo de su tarjeta de red realmente este especificado correctamente. Ejemplo:

```
alias eth0 3c905C-TX
```

Si se realizó alguna edición de este archivo, se deberá ejecutarse el siguiente comando, a fin de actualizar dependencias:

```
/sbin/depmod -a
```

Nota importante Si se utiliza kernel 2.4.x (como serían Red Hat Linux 7.1 y 7.2, Mandrake 8.x), la lista de módulos existentes en el equipo que puede utilizar para distintos chipsets de distintas tarjetas de red se puede obtener listando el contenido del directorio /lib/modules/[versión del kernel]/kernel/drivers/net/. Ejemplo:

```
ls /lib/modules/2.4.9-ac10/kernel/drivers/net/
```

Si se utiliza kernel 2.2.x (como serían Red Hat Linux 6.x y 7.0, Mandrake 6.x y 7.x), la lista de módulos existentes en el equipo que puede utilizar para distintos chipsets de distintas tarjetas de red se puede obtener listanto el contenido del directorio /lib/modules/[versión de su kernel]/net/. Ejemplo:

```
ls /lib/modules/2.2.16-3/net/
```

Debe editarse con un procesador de textos /etc/sysconfig/network y en este establece la puerta de enlace (Gateway) y su nombre de máquina. Ejemplo:

```
NETWORKING=yes
HOSTNAME=su_máquina.su_dominio.com
GATEWAY=192.168.1.254
```

Nota importante: Si se está utilizando Red Hat Linux6.x, LinuxPPP 6.x o Mandrake Linux 7.x, IP versión 4 se habilita añadiendo en /etc/sysconfig/network:

```
FORWARD_IPV4=true
```

Si se utiliza RedHat 7.1 o Mandrake Linux 8.0, IP versión 4 se habilita en /etc/sysctl.conf añadiendo en éste:

```
net.ipv4.ip_forward = 1
```

Debe editarse con un procesador de textos /etc/sysconfig/network-scripts/ifcfg-eth0 y debe verificarse que los parámetros de red sean los correctos. Ejemplo:

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.1.50
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
```

Los parámetros anteriores son proporcionados por el administrador de la red local en donde se localice la máquina que está siendo configurada. El administrador de la red deberá proporcionar una dirección IP (IPADDR), una máscara de la subred (NETMASK), dirección IP de la red (NETWORK) y el Broadcast (BROADCAST).

Debe editarse con un procesador de textos /etc/hosts, y debe verificarse que esté diferenciado el loopback del nombre de la máquina. Ejemplo:

```
192.168.1.50        su_máquina.su_dominio.com    su_máquina
127.0.0.1  localhost.localdomain        localhost
```

Debe editarse con un procesador de textos /etc/resolv.conf y deben establecerse en éste los servidores de resolución de nombres de dominio (DNS). Ejemplo:

```
nameserver 192.168.1.254
nameserver 192.168.1.1
```

Después de hacer todo lo anterior, solo deberá de ser reiniciado el servicio de red. Debe ejecutarse el siguiente comando:

```
/etc/rc.d/init.d/network restart
```

Basta solamente comprobar si hay realmente conectividad. Puede ejecutarse el comando ping hacia cualquier dirección de la red local para tal fin.

```
ping 192.168.1.254
```

Cómo configurar una red con un firewall[17]

Breve historia sobre Firewall y Enmascaramiento de direcciones

No hace mucho tiempo una red de cómputo era algo que no muchas empresas o escuelas tenían en su centro de cómputo. La gran mayoría de estas computadoras se encontraban aisladas una de la otra aunque se encontraran en el mismo cuarto o salón de cómputo. Únicamente grandes empresas, Instituciones Gubernamentales o Universidades tenían este recurso. Eso a cambiado con el paso del tiempo, hoy en día es común encontrar computadoras conectadas a en red y obtener información de ella o brindar servicios (tal es el caso de Internet o una intranet en una oficina u hogar), y es común el uso de ellas, como por ejemplo enviar y recibir correo electrónico, entre muchos servicios más.

El gran desarrollo de estas redes no ha sido del todo positivo en varios aspectos. Uno de ellos es la disponibilidad de Direcciones IP, que esta limitado a 4,300 millones de direcciones IP válidas aproximadamente. Esta cantidad de direcciones puede ser a primera vista muchísimas direcciones, pero direcciones válidas libres en internet son actualmente muy pocas, por lo que cada vez es más difícil poder obtener una dirección válida en internet. Con la llegada de la versión 6 del protocolo IP se espera poder extender este rango de direcciones en un par de millones más. Pero como ésta nueva versión aun no se encuentra disponible se debe de trabajar con la actual (IPv4) y por ende se debe administrar mejor el uso de este tipo de direcciones. Una forma de administrar mejor esto, es escondiendo computadoras con direcciones no válidas dentro de una red, detrás de una dirección IP válida. A esta técnica se le conoce como enmascaramiento de direcciones.

Existe otro problema que no es técnico sino social. Cada día existen más computadoras y personas que acceden a Internet. La necesidad de proteger los sistemas conectados a una red de usuarios no deseados es cada vez más común y se vuelve más importante día a día.

Instalar un firewall es en buena medida una buena solución para protegerse de ataques a una red interna o de usuarios no deseados. Actualmente, el Kernel de Linux (Por ejemplo LinuxPPP 6.2, RedHat 6.2) soporta filtrado de paquetes, que puede ser utilizado para implementar un sencillo firewall.

El filtrado de paquetes

Actualmente linux soporta el filtrado de paquetes. La versión de Kernel 2.2 de Linux contiene cambios significativos en su estructura para brindar este servicio.

Existen cadenas o reglas que los paquetes IP deben de igualar para que estos puedan ser aceptados. Si llega algún paquete al equipo, una regla decide que hacer con él. Este paquete puede ser aceptado, negado, rechazado, enmascarado o enviado a otra regla.

Con este mecanismo es fácil construir reglas sencillas para el filtrado de paquetes con un firewall. Esto quiere decir que todos lo paquetes que lleguen a la máquina, independientemente si son TCP o UDP, serán primero filtrados antes de ser enviados a su destino.

Linux soporta un gran número de características para las reglas de un firewall y el enmascaramineto de paquetes.

Cadenas IP

Las cadenas de un firewall no son más que reglas que se utilizan para que el paquete cumpla con alguna de ellas y en un cierto orden. Esto quiere decir que el paquete debe de cumplir con alguna regla. La regla determina que es lo que va a suceder con el paquete que ha sido recibido. Si el paquete no coincide la próxima regla determinará que hacer con el. Si llega al final de ésta regla se utilizará la política que se encuentra por omisión.

Existen tres tipos de reglas por omisión que se utilizan:

INPUT
: Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisados por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.

OUTPUT
: Esta regla define los permisos para enviar paquetes IP. Todos los paquetes que se encuentran listos para ser enviados a una de las interfaces de la red local y son revisados por la regla de salida. Si el paquete no coincide con alguna de las reglas el paquete es rechazado.

FORWARD
: Esta regla define los permisos para el envío del paquete a otro sitio. Todos los paquetes que se envían a un equipo remoto, nuevamente, si el paquete no coincide con alguna de las reglas este paquete es rechazado.

Si se observa como la máquina puede funcionar como ruteador, se observará que existen tres tipos de tráfico. Los paquetes enviados a esta máquina, los paquetes originados por la máquina y los paquetes ruteados a través de la máquina. La tabla 8 muestra como estos paquetes son ruteados a través de las reglas.

Tabla 7.- Cadenas y paquetes IP

	To local host	*To remote host*
From local host		*Output*
From remote host	*Input*	*Input -> froward -> Ouput*

Como se muestra en la tabla 8 sólo aquellos paquetes que provienen de un host y se dirigen a otros host tienen todo el acceso de las tres cadenas, los paquetes de entrada a la red local podrán solo entrar a través de la cadena o regla de entrada y los paquetes originados desde una máquina local solo podrán salir a través de la cadena o regla de salida. Con este esquema de niveles se puede tener una gran flexibilidad para instalar reglas para diferente tipo de tráfico.

En la versión del kernel 2.2 hay un grupo de reglas predefinidas. Estas están integradas dentro de las reglas de entrada y salida, y no es necesario separar una de otra para que éstas funcionen correctamente.

Reglas en el Firewall

Como se ha comentado, el kernel contiene cadenas de reglas para realizar el filtrado de paquetes. Se mostró también como una cadena filtra un tipo específico de tráfico (entrada o salida). Ahora se muestra cuales son estas reglas.

Las reglas en un Firewall se crean de igual forma como se a mencionado con anterioridad, se tiene una condición que debe de cumplirse para que el paquete de entrada o salida tenga los permisos para poder llegar a su destino. Los valores que se deben utilizar para crear una regla se muestran a continuación:

ACCEPT
: Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.

DENY
: Este valor quiere decir que los paquetes no podrán ser aceptados. Aquellos paquetes que coincidan con la regla (DENY) no podrán llegar a su destino y son tirados a la basura.

REJECT
: Es casi igual al valor DENY pero es más fina la forma de negar el acceso de los paquetes. Por ejemplo los mensajes ICMP se envían de regreso al origen de este paquete, indicándole que éste ha sido rechazado (Los valores DENY y REJECT son todos ellos paquetes ICMP).

MASQ
: Este valor es únicamente utilizado para el envío y cadenas definidas por el usuario y puede ser utilizado únicamente si el kernel es compilado con el soporte de enmascaramiento. Con eso, los paquetes serán enmascarados como si se tratara del equipo maestro (la máquina que tiene instalado el Firewall). Desafortunadamente, los paquetes que regresen del equipo remoto al que se enviaron los paquetes enmascarados, deben de pasar por el equipo maestro y este debe desenmascarar el paquete para que pueda ser recibido por su origen.

REDIRECT
: Este valor indica que únicamente los paquetes serán redireccionados de la entrada las cadenas definidas por el usuario y pueden ser únicamente utilizados cuando el kernel es compilado con el soporte de "Transparent Proxy". Con esto, los paquetes pueden ser redireccionados al soquet local de la máquina maestra siempre y cuando estos sean enviados desde un host remoto.

RETURN
: Este valor es definido por las colas, esto quiere decir que el procesamiento de paquetes continuara en la próxima regla de la siguiente cadena.

Las condiciones de las declaraciones se vuelven más complejas a medida que se tienen diversos tipos de paquetes que filtrar. Los paquetes IP se agrupan por tipo de paquete, los cuales tienes características semejantes entre ellos, así con esto, se puede determinar más fácilmente que paquetes coinciden con alguna regla o no. Las reglas contienen un conjunto de valores para cada uno de los parámetros. Estos parámetros se especifican en la regla de filtrado:

PROTOCOL
: El protocolo de paquetes es revisado. El protocolo especificado puede ser uno de los siguientes: TCP, UDP, ICMP o todos ellos, de igual forma pueden ser valores numéricos que representan a cada uno de estos protocolos y los hace diferentes uno de otro. Los nombres y valores de estos protocolos se almacenan en el archivo /etc/protocols

SOURCE
: De donde provienen los paquetes. La información fuente contiene la dirección IP que muestra la procedencia o un rango de direcciones al igual que la mascara de esas redes, estas también pueden incluir la especificación del puerto o ICMP. Este puede proporcionar el nombre del servicio que se solicita el número del puerto, el valor número de ICMP o el nombre del servicio ICMP que se solicita.

DESTINATION
: Es el mismo valor como en el parámetro SOURCE pero esta vez se especifica a donde el paquete va a ser enviado.

INTERFACE
: Los mismos valores como en el parámetro SOURCE pero esta vez indica por que interfaces el paquete debe de ser enviado.

FRAGMENT
: Esto significa que la regla únicamente observara fragmentos de un paquete completo.

SYN BIT SET
: Únicamente coinciden paquetes del tipo TCP y si se encuentra habilitado y el SYN BIT a ACK y FIN se encuentran limpios. Estos pueden ser paquetes utilizados para la inicialización de conexión de una petición TCP; Por ejemplo, el bloqueo de paquetes de entrada hacia una internase que realiza conexiones del tipo TCP. Esta opción es útil cuando el tipo de protocolo es TCP.

Ahora... ¿Cómo instalar una regla en el Firewall y como monitorearlas? El comando para insertar, borrar y listar las reglas del firewall es */sbin/ipchains*. La sintaxis para utilizar este comando se puede encontrar en el manual ipchains.

Enmascaramiento

El enmascaramiento significa, que el router remplaza la información que viene de un paquete, es decir, le pone su propia dirección IP y número de puerto y lo envía a su destino. Y los paquetes de regreso llegan al router, esta ve a que equipo al que debe de llegar, le quita el enmascaramiento y lo envía al host que envío la petición origen.

Esto significa que con el enmascaramineto de IP se puede esconder una red completa con computadoras con direcciones no válidas, detrás de una dirección IP válida. Esto es totalmente transparente para la máquina que se encuentra dentro de la red protegida o con direcciones no válidas. Cuando se establece una conexión entre un equipo de la red local con otro de la red externa, el equipo externo no necesita saber que se está conectando con un equipo que contiene una dirección no válida. El equipo remoto pensará que se está conectado a el equipo router (o maestro), pero en realidad únicamente los paquetes están pasando a través del equipo remoto, los paquetes se reenvían al equipo que realizó la petición dentro de la red local y cuando este

equipo envía algún paquete, el equipo maestro enmascarará este paquete, como si el fuera el que originara la información al servidor remoto.

En el ejemplo que se mencionó anteriormente puede ser utilizado cuando desde el servidor maestro se conecta a Internet y detrás de éste equipo maestro se tiene conectado una red local varias computadoras conectadas a el mediante una tarjeta Ethernet. Como es sabido el equipo maestro tendría solamente la dirección IP válida que le da permiso de acceder a Internet, esta dirección IP comúnmente es proporcionada por el ISP (*Internet Service Provider* o Proveedor de Servicios de Internet) y cambia cada vez que se acceda a Internet mediante el ISP, ahora, para que las demás computadoras que se encuentran conectadas en red puedan tener acceso de salida a Internet, el servidor maestro debe de tener el enmascaramiento instalado y funcionando, de lo contrario estas no podrán tener salida. Ahora cuando el equipo maestro ya tiene acceso a Internet y está haciendo la función de ruteador de todas las máquinas internas, todo el tráfico generado por las máquinas internas podrá tener acceso a Internet a través de la máquina maestra sin problemas.

Otra característica importante, es que la LAN interna se encuentra escondida del mundo externo. Nadie podrá observar que se tiene más de una máquina que esta saliendo a Internet a través del equipo maestro y cómo está hecha la LAN interna o cuantas computadoras están conectadas a ella. Si se utilizan direcciones no registradas (o válidas) en la red interna, nadie tendrá acceso a conectarse a ellas (únicamente se podrán ver las máquinas locales en la LAN) sin que pasen por el equipo maestro (o firewall). La tabla 9 muestra el rango de direcciones IP privadas o no válidas

Tabla 8.- Rango de IP's privadas:

Class A net	10.0.0.0	->	10.255.255.255
Class B net	127.16.0.0	->	172.31.255.255
Class C net	192.168.0.0	->	192.168.255.255

Para enmascarar una red no es necesario hacer diferencias entre un tipo de equipo y otro dentro de la LAN. Mientras los equipos utilicen el protocolo TCP/IP todos ellos podrán tener acceso a Internet mediante el equipo maestro. El enmascaramiento toma efecto en el equipo maestro (el firewall que también es un gateway entre una red y otra) y no realiza alguna excepción en los equipos conectados dentro de la LAN interna.

Instalación del software necesario

La figura 38 muestra una red sencilla conectada a el equipo maestro (Firewall/Gateway). Una máquina (el equipo maestro) es utilizada como Gateway hacia Internet. La red interna (LAN) consta de un conjunto de máquinas conectadas entre si mediante una tarjeta de red Ethernet.

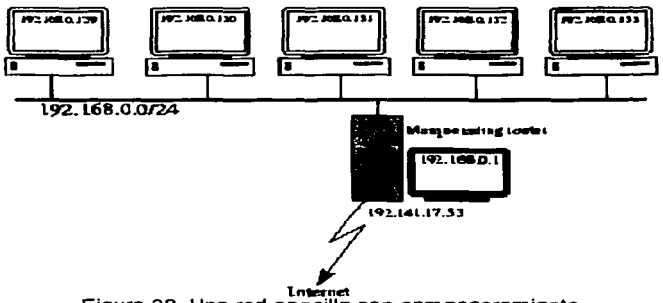

Figura 38. Una red sencilla con enmascaramiento

Todas las máquinas conectadas en la LAN interna tienen una dirección Clase C 192.168.0.0 El único equipo con una dirección válida hacia Internet es el router (equipo maestro que sirve como gateway entre la red local e Internet, así mismo funcionará como firewall) con una dirección IP 192.141.17.53. Esta es la típica configuración de una pequeña red de oficina o red casera.

Ahora se va a instalar el enmascaramiento para la máquina maestra (gateway). Primero se tiene que estar seguro de que el kernel esté configurado para poder enmascarar direcciones IP. La configuración del Kernel se puedes ver en el manual de manejo del sistema. Recordar que debe estar habilitada la opción de enmascaramiento de IP's para su correcto funcionamiento. Ahora se deben de instalar algunas reglas del firewall para poder habilitar el enmascaramiento de todo el tráfico de salida, originado por las máquinas en la red local.

Primeramente hay que crear una nueva línea llamada user_msq y enmascarar todo el tráfico ruteado através de este equipo con el comando:

```
# /sbin/ipchains -N user_msq
# /sbin/ipchains -A user_msq -s 0/0 -d 0/0 -j MASQ
```

El parámetro -N se utiliza para crear una nueva cadena. Para agregar nuevas reglas al final de la cadena se utiliza la opción *-A*. Para especificar las direcciones origen se realiza con la opción *-s* y las de salida con la opción -d.

Estas opciones toman direcciones IP como parámetros, con una máscara opcional y número de puerto. En el ejemplo se ha utilizado 0/0 que con esto se cubre todas las posibles direcciones IP. El formato general podría utilizarse de esta forma: ip/network address/netmask. La máscara puede escribirse en el formato usual que es: 255.255.255.0 para una red clase C o únicamente proporcionar el número de bits que utilizará la máscara de esa red, esto quiere decir que /24 es igual a escribir /255.255.255.0

El origen de la regla se toma por la opción *-j*. En este caso, se tomó MASQ como el origen para realizar el enmascaramiento.

Ahora, se necesita enviar los paquetes originados por la LAN a esta cadena. Como se a mostrado, con ipchains todos los paquetes ruteados serán procesados para ser enviados a la cadena, y también hay que agregar esta regla a esta cadena, la cual enviará todos los paquetes de la red local 182.168.0.0/24 hacia la nueva cadena llamada user_msq. Existe un punto más a considerar. Todos los paquetes que vienen de la red local dejarán el router (equipo maestro) en su dispositivo de salida, y es conveniente monitorear únicamente

los paquetes de este dispositivo de salida y enmascarar los paquetes que saldrán con la dirección IP válida. La opción *-i* hace esta tarea y toma el dispositivo de salida como su argumento. De esta forma:

```
#/sbin/ipchains -A forward -s 192.168.0.0/24 -d 0/0 -i ppp0 -j user_msq
```

Esta regla concuerda con todos lo paquetes que se envíen a través de este dispositivo (ppp0) con la dirección fuente de la clase C de la red 192.168.0.0 destinada a cualquier dirección y lo pone en la cadena user_msq.

La instalación esta casi terminada. La cadena IP esta instalada y todos los paquetes que son originados por la LAN se encuentran enmascarados.

Algunos protocolos tienen alguna extraña definición que hace un poco más difícil reconocer los paquetes de regreso. El FTP por ejemplo es tal protocolo. Las conexiones no se establecen únicamente del cliente al servidor, pero el servidor también se conecta con el cliente. Esto significa, que el núcleo del linux tiene que reconocer esas conexiones como parte de una conversación entre la máquina enmascarada del cliente y el servidor FTP en Internet, y transmitir estos paquetes a la máquina en el LAN. Esto no es parte del enmascaramiento estándar en el kernel.

Sin embargo el kernel tiene módulos para utilizar un número de protocolos que necesiten la dirección especial. La tabla 10 muestra una lista de estos módulos. El módulo del ip_masq_user se puede utilizar para poner la dirección en ejecución especial en el espacio del usuario para los protocolos que (todavía) no son utilizados por otros módulos.

Tabla 9.- Módulos especiales de enmascaramiento:

ip_masq_cuseeme	CuSeeMe protocolo para video conferencia
ip_masq_irc	Chat (plática en línea)
ip_masq_raudio	Real Audio (audio y video en demanda por Internet)
ip_masq_vdolive	VDO Live (videoconferencia en línea)
ip_masq_ftp	File Transfer Protocol
ip_masq_quake	Quake (videojuego en línea)
ip_masq_user	Control especial de enmascaramiento

Si se van a utilizar estos módulos en el router, es necesario cargar las referencias de estos protocolos de esta manera:

```
# /sbin/insmod ip_masq_cuseeme
# /sbin/insmod ip_masq_irc
# /sbin/insmod ip_masq_raudio
# /sbin/insmod ip_masq_vdolive
# /sbin/insmod ip_masq_ftp
# /sbin/insmod ip_masq_quake
```

Ahora se ha terminado y el enmascaramiento debe trabajar absolutamente bien. Ahora se puede controlar si todas las reglas se encuentran trabajando correctamente, listándolos con el comando ipchains de la siguiente forma:

```
# ipchains -L forward -n
Chain forward (policy ACCEPT):
target prot opt source destination ports
user_msq all ------ 192.168.0.0/24 0.0.0.0/0 n/a
```

```
# ipchains -L user_msq -n
Chain user_msq (1 references):
target prot opt source destination ports
MASQ all ------ 0.0.0.0/0 0.0.0.0/0 n/a
```

Como se observa, se puede listar la cadena usando el parámetro - *L* y el nombre de la cadena. No especificar ningún nombre, enumerará todas las cadenas que existen. El parámetro - *n* asigna a ipchains para que este imprima la salida en valores numéricos que se resuelve de la resolución de las direcciones IP e impresión de los nombres.

Script para hacer funcionar el enmascaramiento

Si existe la necesidad de utilizar el enmascaramiento, entonces es probable activar el script cada vez que la máquina se inicializa. Entonces es necesario utilizar un script que se almacene dentro de */etc/rc.d/init.d* y realice esta tarea automáticamente. El script *masquerade* (de enmascaramiento) que se almacena dentro de /etc/rc.d/init.d funcionará para que cada vez que se inicie el equipo este arranque el programa para funcionar el enmascaramiento. Este programa funciona exactamente igual como se mostró en la sección anterior. Este inicia la cadena user_msq y envía el tráfico a ser enmascarado a la cadena. Las cuatro variables que existen para iniciar las reglas son las siguientes:

MSQ_START
: El enmascaramiento se levantará cuando esta variable se encuentre con la opción "yes". De otra forma uno debe de inicializar el script manualmente si esta opción se encuentra en "no".

MSQ_DEV
: Dispositivo donde el enmascaramiento toma efecto. Este dispositivo es la interfaces de salida de tu router (equipo maestro) que puede ser ppp0 o eth0.

MSQ_NETWORKS
: Aquí se agregan las direcciones de las redes locales a ser enmascaradas separadas por un espacio. Se puede especificar direcciones IP o redes en esta opción.

MSQ_MODULES
: Los módulos son necesarios para el enmascaramiento (Ver tabla 10)

Para tener la misma funcionalidad como la que se mostró en la sección anterior, el archivo */etc/sysconfig/firewall/config* debe de quedar de la siguiente forma:

```
# Masquerading settings
#
MSQ_START="yes"
MSQ_NETWORKS="192.168.0.0/24"
MSQ_DEV="ppp0"
MSQ_MODULES="ip_masq_cuseeme ip_masq_ftp ip_masq_irc \
ip_masq_quake ip_masq_raudio ip_masq_vdolive"
```

El script -*masquerade*- soporta las opciones "Start, stop, reload". También se puede observar la lista de conexiones enmascaradas con la opción "status". Un ejemplo de ella seria así:

```
# /sbin/init.d/masquerade status
BB Masquerading v2.1
IP masquerading entries
prot expire source destination ports
UDP 04:51.46 Netwinder.suse.com norad-48.mcdn.net 1177 (61031) -> domain
UDP 04:36.02 Netwinder.suse.com norad-48.mcdn.net 1175 (61028) -> domain
TCP 01:11.29 Netwinder.suse.com www.apple.com 2153 (61027) -> telnet
TCP 01:56.27 Netwinder.suse.com sfbay1.yahoo.com 2155 (61032) -> www
```

Como se muestra en el ejemplo de arriba, se ven cuatro conexiones enmascaradas originadas por el equipo Netwinder.suse.com. Existen dos peticiones de DNS a norad-48.msdn.net, una sesión telnet a www.apple.com y una conexión a sfbay1.yahoo.com

El Firewall: Objetivos

Antes de proseguir con la instalación del firewall y las reglas de filtrado de la información, se tienen que definir los propósitos del firewall. La primera cosa por supuesto es proteger la red de área local contra intrusos del Internet. Pero no se desea probablemente bloquear todo el tráfico del exterior. Se pueden tener servicios que deban ser accesibles, como el WEB, FTP o mail server. También puede haber los equipos en los que se confíe y puedan tener acceso a la red local. Por ejemplo los contratistas, o las cuentas de mantenimiento son visitantes posibles que no se desea negarles el acceso. Se puede desear controlar quién puede tener acceso desde Internet a los equipos de trabajo locales.

Aspectos generales

La primera parte es como negar el acceso desde el exterior, mientras que el tráfico salida pueda tener acceso al exterior. ¿Este es en realidad un problema? El filtrado de paquetes puede ser muy grande, y no se sabe si algún paquete que llegó fue iniciado desde dentro de alguna máquina de la red local, o uno de alguna máquina del exterior, por lo que en estos momentos no se sabe sobre conexiones de todos modos. Las reglas del filtro observan cada paquete como una entidad separada.

Para distinguir entre el tráfico de salida y de entrada, se necesita saber un poco sobre la estructura del servicio del TCP/IP (*Transfer Control Protocol / Internet Protocol*, protocolo de control de transferencia / Protocolo de Internet). Tomando como muestra SMTP (*Simple Mail Transfer Protocol*, protocolo simple del transporte del correo) como ejemplo. El SMTP es utilizado por MTAs (*Mail Transport Agent*, agentes de transporte del correo) para transportar el correo a partir de una computadora principal a otra. Para hacer esto la máquina principal que desea entregar el correo abre una conexión al puerto 25 en la máquina receptora, sabiendo (o esperando) que un servidor del SMTP esté escuchando las conexiones entrantes en este puerto. Si es así ambos agentes del correo negociarán algunos parámetros y el correo será enviado a la máquina receptora. Esto quiere decir, que si se bloquea el puerto 25 en la máquina, nadie podrá entrar en contacto con el mail server. Casi todos los servicios del TCP trabajan esta manera. Hay los accesos especiales donde un demonio espera conexiones entrantes, bloqueando este acceso dará lugar a una negación de este servicio. Esto da una política para la protección selectiva de los servicios para el tráfico entrante. ¿Pero qué hay sobre las conexiones salientes? Bien, el TCP/IP tiene números de acceso a partir de la 0 a 65535. Los primeros 1024 accesos (0 a 1023) son reservados para los servicios del sistema. Esto quiere decir, que las conexiones salientes tienen números de acceso más arriba de 1023, y todos los paquetes entrantes que intenten alcanzar los puertos más arriba de 1023, son contestaciones a las conexiones iniciadas por peticiones internas.

Entonces, lo que se hace es bloquear todos los puertos debajo de 1024 y permitir que el tráfico a los puertos más altos pase. Esto es bueno como regla general, pero la vida es dura, y hay anomalías. Algunos servicios sensibles están situados en números de acceso más altos. El ya popular servicio de HTTP utiliza el número de puerto 3128 por valor por defecto. Los servidores con bases de datos también tienden ha utilizar altos números de puertos. Por ejemplo, mySQL utiliza el puerto 3306. Entonces, bloquear los puertos del 0 al 1023 es lo suficiente para controlar algunos accesos. Se debe observar que es lo que está en funcionamiento en el sistema y cerciorarse de que se tiene una lista completa de todos los accesos que puedan ser una blanco para los ataques del exterior y verificar que estos están bloqueados.

Script para que funcione el firewall

Esta vez no se instalará todo a la vez. El firewall es mucho más complejo que el enmascaramiento. La forma de instalación del enmascaramiento se vio en la sección anterior y se proporcionó una comprensión general de cómo el comando ipchains es utilizado para instalar reglas del firewall dando un ejemplo de mundo verdadero. Pero como el mundo verdadero no es siempre tan fácil como en este caso. Si se está interesado, en

leer el script, este se localiza en /etc/rc.d/init.f/firewall. Con la descripción dada en esta sección, no es realmente duro entender qué contiene.

Para entender cómo trabaja, se dará una red de ejemplo otra vez. A continuación se muestra la figura 39, y como se observa, es un poco más compleja que en el ejemplo de enmascaramiento.

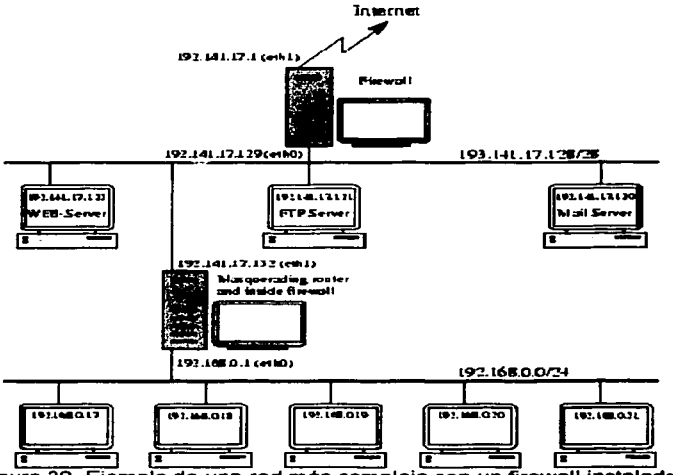

Figura 39. Ejemplo de una red más compleja con un firewall instalado.

Como se observa, se cuenta con dos segmentos esta vez. Las direcciones privadas IP de las máquinas internas dentro del segmento (192.168.0.0/24) están conectadas con el otro segmento a través de un firewall enmascarado. Las máquinas en el segmento exterior tienen direcciones IP válidas y están conectadas a través de este equipo, que proporcionan los servicios que pueden y deben ser accesibles desde el Internet. La conexión de este segmento a Internet es realizada por una máquina que está como gateway y firewall. Esta topología tiene algunas ventajas sobre todas las máquinas que pudieran estar únicamente en un solo segmento. La estación de trabajo local esta protegida por dos firewall. Si alguien desea entrar a esta máquina por el primer firewall, esta persona únicamente tendrá permiso a las máquinas que proporcionan los servicios, como HTTP o FTP que se les proporciona a las personas del exterior, pero no podrá entrar al segundo segmento que está protegido por el otro firewall. Por supuesto él podrá dañar o destruir el Web site, pero los datos sensibles verdaderos todavía están protegidos por el segundo firewall. Bajo ninguna circunstancia podrá tener acceso directo al segmento interior si éste no se le permite.

Como funciona este script

Con el conocimiento básico mencionado anteriormente sobre servicios del TCP/IP, es fácil diseñar un filtro. Para agregar las reglas necesarias a la cadena de entrada de información al que remiten todos los paquetes de entrada que provienen del dispositivo que apunta al mundo exterior e irá a la dirección IP que se desea proteger con la variable *user_fw* de la cadena definida. Todos los paquetes que vienen de la red local y que van al exterior serán enviados a la variable *user_out* de la cadena definida.

Entonces se agregan las reglas a la variable *user_fw* de la cadena. La primera cosa por hacer es evitar el *spoofing*. El *Spoofing* significa que alguien está fingiendo estar en el interior de la red local, pero realmente está viniendo del exterior. Esto se hace generalmente falsificando o substituyéndolo por una dirección de la red local. La detección de esta clase de paquetes es algo fácil, como ningún paquete de la LAN están viniendo del dispositivo que señala al exterior, se pueden eliminar todos los paquetes que tengan una dirección local y que provengan del dispositivo de entrada de el firewall agregando las reglas de negación para estos paquetes. Lo siguiente es válidar los paquetes de las máquinas en las cuales se confían el acceso dentro de la regla. Con la variable ACCEPT, esta aceptará todos los paquetes de estas direcciones que se le mencionen. Se debe tener cuidado con esto, pues estos paquetes pueden ser "*spoofed*". Entonces se tiene que crear una lista con reglas válidas para los diferentes tipos de servicio como FTP, HTTP, HTTP seguro (SSL), SSH, SMTP, NNTP y DNS. Esto se verá en el párrafo siguiente donde se explica la configuración. Entonces si se tomarán un rango de puertos, cerrarlos para el tráfico de UPD y de TCP. Hay que recordar, que las reglas llevan un orden secuencial. Se puede aquí dar el acceso para los servicios que se quieran permitir, pues los paquetes legales han sido detectados por las reglas en la cadena antes de que los paquetes vengan del dispositivo. Otro punto interesante, es válidar todo que no se ha negado hasta ahora.

Cuando la cadena para el tráfico entrante se instala, las reglas para el tráfico saliente se agregan a la variable *user_out* de la cadena. Esto se hace solamente si se desea vigilar el tráfico saliente de todos los equipos de la LAN. Si éste es el caso, una regla para válidar se agrega para cada máquina que requiera tener el acceso. Entonces una regla de negar bloquea tráfico del resto de las máquinas.

Las opciones se fijan para válidar y para negar las reglas para registrar si están especificados en la instalación. Antes de que se haga cualquier otra cosa, es cierto que se debe de controlar el flujo del servicio, y las condiciones de la máquina para tener un buen firewall (tener una direccioón IP válida y soporte del Kernel de Linux para el firewall).

Soporte para el servicio proxy

Una cosa no mencionada hasta ahora es el soporte para el servicio proxying transparente. Pues no se relaciona directamente con el firewall y se ha pospuesto hasta esta sección. El Kernel de Linux utiliza (si está configurado correctamente) el cambio de dirección de paquetes destinados a las máquinas remotas a los accesos locales. Esto puede ser utilizado para la entrada y salida de tráfico. Por ejemplo, se puede volver a redirigir todas las conexiones salientes al puerto 80 (HTTP) a un acceso local, para filtrarlas a un proxy server local. También para esto, las reglas se agregan a la cola de las variables *user_fw* y *user_out* si este servicio es especificado dentro de la configuración.

Configuración del firewall

Al igual que el script para el funcionamiento de enmascaramiento, el firewall también tiene un script para su configuración y puesta en marcha dentro del directorio /etc/rc.d/init.d/firewall y el archivo de configuración se localiza en: */etc/sysconfig/firewall/config*

Estas variables tienen el prefijo FW _ y siguen el mismo formato. Contienen una lista de IP's o de las direcciones de red con las máscaras opcionales, separada por espacios en blanco. La descripción de estas reglas se encuentra abajo. Se tiene que utilizar una dirección IP, los nombres de las máquinas que no tendrán resolución de IP. Durante el proceso de instalación del firewall todo el tráfico de la red será bloqueado, así que ninguna petición del servidor de nombres se puede utilizar para resolver nombres de direcciones IP.

En vez de especificar una dirección IP se puede utilizar también la cadena especial *IP@device*. Esta substituirá la dirección IP que tiene el dispositivo de entrada de la red que tiene en ese momento que se ejecuta el script del firewall. Esto es útil si se tiene una conexión dialup donde la dirección IP se cambia cada vez que se conecta al ISP.

A continuación se muestra una lista con la mayoría de las variables para configurar el firewall. La mayoría de las variables usadas tienen significados obvios:

FW_START
: El firewall comenzará solamente si el script se encuentra dentro de los archivos de arranque y la variable se fija a " yes". No obstante se puede inicializar el script de forma manual incluso si este se fija a " no".

FW_WORLD_DEV
: Dispositivo que debe ser protegido. Se puede tener una lista de dispositivos aquí, si es que se tiene más de un dispositivo de salida -*es decir dispositivos virtuales para los servidores del WEB*-. Todo el tráfico en estos dispositivos será vigilado por las reglas del firewall. Si se tiene conexión dialup PPP éste puede ser el dispositivo ppp0. Puede ser un dispositivo ISDN si se marca hacia fuera con una tarjeta del ISDN.

FW_LOCALNETS
: Lista de redes locales. Solamente las direcciones IP listadas aquí estarán protegidas. Si se desea proteger el firewall por sí mismo, la dirección IP de él debe de estar listado aquí.

FW_TCP_LOCKED_PORTS
: Los números de acceso TCP que se deseen bloquear aquí deben de listarse en un rango que consista en pares de números separados por dos puntos. Por ejemplo: "1:6 8:1023". Los puertos 1 a 6 y 8 a 1023 se encuentran bloqueados. El valor por omisión es bloquear todos los puertos hasta 1023. Verificar que se tengan los puertos más importantes aquí.

FW_UDP_LOCKED_PORTS
: Los números de puertos UDP que deben ser bloqueados siguen la misma sintaxis que con los puertos TCP. Se recomienda para fijar esto a 1:1023 así que todos los accesos reservados estarán bloqueados.

FW_INT_DEV
: Dispositivo para la red interna. Se monitorea el tráfico de salida usando este dispositivo. Como con el dispositivo que va hacia la red exterior, se pueden enumerar más de un dispositivo aquí.

FW_LOG_DENY
: Si esta variable está marcada con " yes " todas las violaciones de las reglas del firewall se registran dentro de */var/log/messages*. Esto significa que cada tentativa de romper el firewall será registrada.

FW_LOG_ACCPET
: Si esta variable está marcada con " yes " todos los paquetes que estén permitidos dentro de las reglas del firewall serán registrados dentro de */var/log/messages*. Esto significa que cada uno los paquetes que pasan por el firewall (permitidos) serán registrados dentro de ese archivo. Hay que tener cuidado con esta opción, pues crea muchas entradas del registro.

FW_FTPSERVER
: Direcciones de los sitios de FTP que son libremente accesibles desde el exterior. Esto no significa que todos los servicios de esta máquina están disponibles. Solamente el tráfico de FTP será permitido, el resto del tráfico todavía será bloqueado (igual que para el resto de los servicios cubiertos por las configuraciones separadas del firewall).

FW_WWWSERVER
: Direcciones de los sitios de WWW que son accesibles desde el exterior. Iguales que para FTP, solamente conexiones del HTTP se pueden hacer a este equipo.

FW_SSLSERVER
: Direcciones de los sitios de *Secure-Socket-Layer* (SSL) WWW que son accesibles del exterior. Es necesario, que el acceso del SSL se especifique en FW_SSLPORT.

FW_SSLPORT
: Puerto donde el SSL espera recibir peticiones. Aquí se puede incorporar solamente un número.

FW_MAILSERVER
: Direcciones de los sitios SMTP que son accesibles desde el exterior.

FW_DNSSERVER
: Direcciones de los sitios DNS que son accesibles desde el exterior.

FW_NNTPSERVER
: Las direcciones de los sitios del NNTP que son accesibles para noticias (véase abajo para las alimentaciones de las noticias).

FW_NEWSFEED
: Direcciones de los servicores de noticias que se permiten conectar con los servidores del NNTP. Las dos variables *FW_NNTPSERVER* y *FW_NEWSFEED* necesitan ambas ser instaladas.

FW_ROUTER
: Direcciones del router de Internet. Esta únicamente puede ser utilizada si la dirección del router no proporciona los rangos que están en la variable *FW_LOCALNETS*, pero está situada en un lado desprotegido del firewall. La figura 40 ilustra este esquema. Se observa que la conexión a Internet está hecha con el router en uno de sus dispositivos, y otro de ellos conectado con el firewall hacia el propio segmento por su Ethernet (esto es importante, ya que ninguna otra máquina tiene que estar en este segmento).

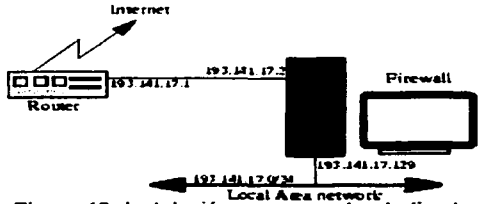

Figura 40. Instalación con un router dedicado

Otra cosa importante (y desafortunada) es, que la dirección IP de este router está dentro de la red que se desea proteger, en este caso la red 193.141.17.0/24. Sin tomar en consideración, que todo el tráfico que viene del router será eliminado, pues parecería un ataque tipo spoofing (hay que recordar que las direcciones IP de la red protegida no deben de provenir del propio dispositivo de salida, como se mencionó anteriormente). Fijando la dirección del router dentro de la variable *FW_ROUTER*, los paquetes con esta dirección origen pueden desviar el filtro spoofing. Pero aquí se ve porqué se debe de evitar una entrada como esta. Si alguien realmente hace un spoofing hacia la dirección de él pueden pasar el firewall.

Intentar evitar esto, es decir, usando subredes para dar a su router una dirección que no pertenezca a la red interna. Este parámetro fue agregado al firewall para poder manejar estas opciones en redes existentes, donde no era posible cambiar a una topología mejor. Si se diseña una red este tipo, no se utilice esta característica!

FW_INOUT

Si esta variable se cambia a " yes" leerá el archivo /etc/sysconfig/firewall/fw-inout. Las direcciones IP listadas dentro de este archivo podrán tener acceso al otro extremo del firewall.

FW_TRANSPROXY_IN

Aquí se puede incorporar una lista de puertos y de direcciones IP para redirigir el tráfico entrante a los puertos locales. Cada entrada consiste en una dirección IP origen de los paquetes de entrada, la dirección IP destino y el puerto, y el puerto local que debe ser redireccionado, todo esto separado por comas:

Source IP, Target IP, Target Port, Local Port

Esto quiere decir que si un paquete que provenga de un equipo y este trae la dirección IP fuente (Source IP) y este desea ir a un equipo que contenga el destino (Target IP) y el número de puerto al que se desea conectar, este es redireccionado al puerto local. Es decir si se desea volver a redirigir todo el tráfico a cualquier WEB Server en su red al web server local, se puede utilizar la variable *FW_TRABS_PROXY_IN* de esta forma:

0/0,192.141.17.0/0,80,80

FW_TRANS_PROXY_OUT

De igual forma que la variable de arriba, pero para conexiones salientes. FW_TRANSPROXY_OUT tiene el mismo significado para el tráfico saliente que FW_TRANSPROXY_IN para los paquetes entrantes. La diferencia es que la variable _ OUT filtra el tráfico del dispositivo que se determino en la variable FW_INT_DEV, mientras que _IN hace lo miamo con FW_WORLD_DEV.

FW_FRIENDS

Si esta variable se cambia a " yes " entonces el archivo /etc/sysconfig/firewall/fw-friends se lee. Si no ninguna máquina en la red local tiene acceso a salir a la Internet.

FW_SSH

Esta variable da acceso del tipo SSH -acceso 22- para esos equipos que se encuentren dentro del archvo: */etc/sysconfig/firewall/fw-ssh*.

Además de leer el archivo /etc/sysconfig/firewall de configuración, el firewall además lee algunos otros archivos que están dentro del directorio /etc/sysconfig/firewall, para conseguir mayor información sobre algunos parámetros de configuración.

/etc/sysconfig/firewall/fw-friends

Las máquinas que tienen acceso ilimitado a la red local se agregan dentro de este archivo. Se debe de agregar la dirección IP de cada máquina en líneas separadas por equipo. Los comentarios se pueden insertar en las líneas que comienzan con el signo de "#". Este archivo será leído solamente si FW_FRIENDS se fija a "yes". Si no ninguna máquina del exterior tiene acceso completo a la red local.

/etc/sysconfig/firewall/fw-inout

Solamente los equipos listados aquí tienen acceso directo a Internet o salir de la red local. Recuerdar que para que funcione la variable *FW_INOUT* se fija a "yes". Cada máquina no incluida en esta lista será bloqueada. Los comentarios están marcados con el signo "#" al inicio de cada línea. Si FW_INOUT se fija a "no" entonces cualquier máquina de la red local puede tener acceso al Internet.

/etc/sysconfig/firewall/fw-ssh

Si FW_SSH se encuentra en "yes" entonces todas las máquinas mencionadas tienen acceso al puerto 22. Esto significa que pueden tener acceso demonio sshd *(demonio seguro del shell)* en la red local.

La red del ejemplo mostrada en la figura 40 hace que dos máquinas estén como firewall. La tabla 11 muestra las configuraciones para estas dos máquinas.

Tabla 10.- Parámetros del firewall para la red ejemplo:

Variable	Dentro del firewall	Fuera del firewall
FW_START	yes	yes
FW_WORLD_DEV	eth1	Eth1
FW_LOCALNETS	192.168.0.0/24	193.141.17.128/28
FW_FTPSERVER		193.141.17.131
FW_WWWSERVER		193.141.17.133
FW_SSLSERVER		
FW_SSLPORT		
FW_MAILSERVER		193.141.17.130
FW_DNSSERVER		
FW_NNTPSERVER		
FW_NEWSFEED		
FW_INT_DEV	eth0	eth0
FW_LOG_ACCEPT	no	no
FW_LOG_DENY	yes	yes
FW_ROUTER		
FW_FRIENDS	no	no
FW_INOUT	no	no
FW_SSH	no	no
FW_TRANSPROXY_OUT		
FW_TRANSPROXY_IN		
FW_TCP_LOCKED_PORTS	1 al 1023	1 al 1023
FW_UDP_LOCKED_PORTS	1 al 1023	1 al 1023

Lo más importante es que las variables FW_WORLD_DEV y FW_LOCALNETS estén con los valores correctos. Estas variables especifican donde el filtro de paquetes estará vigilando el tráfico, y qué direcciones

IP deben de estar protegidas. También, como se mencionó anteriormente, las variables _LOCKED_PORTS son importantes, pues que servicios estarán bloqueados por el filtro.

El script para levantar el firewall, contiene los comandos necesarios para levantarlo. La estructura es muy similar al script de enmascaramiento. Este script tiene las opciones:

start
: Inicia el proceso de levantar las reglas del firewall, el filtrado de paquetes, definiciones realizadas por el usuario, etc.

stop
: Detiene las reglas, cadenas y definiciones realizadas por el usuario.

reload, restart
: Lo mismo que hacen stop y start juntos

status
: Imprime la lista que está manejando en ese momento el firewall.

Cómo montar y desmontar unidades de disco en el entorno de Gnome [17]

A diferencia de Windows y MS-DOS, en Linux, además de no haber una asignación de letras -*a:\ b:\ c:\ d:\ e:*- para las unidades de disco y las particiones, es necesario indicarle al sistema cuando se utilizará una unidad de disco extraíble para poder acceder a esta y cuando se dejará de utilizar para poder retirarla y cambiarla por otra. Una vez configuradas las unidades de disco en el sistema se necesitará conocer algunos métodos y atajos para montarlas y desmontarlas rápidamente.

Métodos

Lo primero que se debe hacer antes de pretender montar y desmontar unidades de disco es configurar adecuadamente éstas en el sistema. Antes de que existiesen los entornos gráficos como GNOME, montar y desmontar las unidades de disco requería de utilizar varios comandos UNIX en una ventana terminal. Por fortuna los nuevos procedimientos a seguir son más sencillos para los usuarios novatos, reduciéndose la labor a solo un par de clicks con el mouse.

Utilizando comandos

Aprender la utilización de los comandos *mount* y *umount* es necesario si se quiere entender que es lo que realmente ocurre en el trasfondo cuando se utiliza una aplicación gráfica o los iconos del escritorio.

Al disponerse a montar una unidad de disco o partición, se tiene primero que identificar de qué dispositivo se trata, qué formato tiene y en donde se quiere montar dicha unidad o partición. La mayoría de las tarjetas madre tienen capacidad para soportar hasta cuatro discos duros o unidades IDE *(CDROMS y Zip Drives, por ejemplo)*, y dos unidades de disco flexible o *floppies*.

De este modo se considera lo siguiente:

1. Disco duro o unidad IDE primaria maestra equivaldría a /dev/hda en Linux
2. Disco duro o unidad IDE primaria esclava equivaldría a /dev/hdb en Linux
3. Disco duro o unidad IDE secundaria maestra equivaldría a /dev/hdc en Linux
4. Disco duro o unidad IDE secundaria esclava equivaldría a /dev/hdd en Linux
5. Unidad de disco flexible de 3½ pulgadas a /dev/fd0 en Linux
6. Segunda unidad de disco flexible de 3½ pulgadas o unidad de cinta equivaldría a /dev/fd1 en Linux

Salvo por las unidades de CDROM y Floppies, las unidades de disco duro contienen particiones, mismas a las que en la tabla de particiones se les asigna un número de acuerdo a su posición en el disco duro. Siendo así, se puede tener un esquema similar al siguiente:

Tabla 11.- Posible esquema de un Sistema con dos sistemas operativos:

Dispositivo	Para el sistema	Para Windows	Para Linux	Formato o tipo
/dev/hda1	Primera partición primaria del disco duro	C:\	/mnt/windows/ [1]	vfat (Windows)
/dev/hda5	Primera partición lógica en el disco duro	Invisible e inaccesible	/boot/	ext2 (Linux)
/dev/hda6	Segunda partición lógica en el disco duro	Invisible e inaccesible	/	ext2 (Linux)
/dev/hda7	Tercera partición lógica en el disco duro	Invisible e inaccesible	swap	swap (Linux)
/dev/hdc > /dev/cdrom	CDROM como unidad IDE secundaria maestra	D:\	/mnt/cdrom/	iso9660
/dev/hdd4 [2]	Zip Drive como unidad IDE primaria esclava	E:\	/mnt/zipdrive/	vfat (Windows)
/dev/fd0 > /dev/floppy	Unidad de floppy de 3½ pulgadas	A:\	/mnt/floppy/	auto (vfat/ext2)

[1] Desde Linux la partición correspondiente para Windows puede montarse en cualquier punto de montaje deseado.
[2] Las unidades Zip Drive IDE/ATAPI siempre utilizan la cuarta partición del dispositivo.

Habiendo observado la tabla 12 y tomándola como base, la sintaxis a utilizar como *root* para el comando *mount* sería del siguiente modo:

```
mount -t [tipo] /dev/[dispositivo] /punto/de/montaje/
```

Como ejemplo el caso de montar el dispositivo */dev/hda1*, que corresponde a la partición donde se encontraría la instalación Windows y todos los archivos personales del usuario, en un punto de montaje previamente creado, */mnt/windows/*. La línea de comando correspondería a la siguiente:

```
mount -t vfat /dev/hda1 /mnt/windows
```

Hecho lo anterior, se podrá acceder a los directorios contenidos en dicha partición donde estaría instalado Windows, con solo cambiar a */mnt/windows/*:

```
cd /mnt/windows/
```

Utilizar el comando *ls* a fin de ver el contenido del directorio en el cual ahora se encuentra:

```
ls -l
```

Lo anterior da como salida lo siguiente:

```
. ..  Archivos de programa  Mis documentos  windows
```

Para poder acceder a directorios que utilizan espacios como parte de su nombre, como ocurriría con *Archivos de programa* y *Mis documentos*, es necesario utilizar el comando *cd* seguido del nombre de dicho directorio encerrado entre comillas, como se muestra del siguiente modo:

```
cd "Mis documentos"
```

Si en este momento se quisiera desmontar la unidad con el comando *umount*, el sistema nos enviaría un mensaje de error indicando que no es posible desmontar la unidad pues ésta se encuentra ocupada. A fin de poder desmontar dicha unidad, es necesario salir de ésta y que ningún otro proceso o programa se encuentre utilizando algún contenido de dicha unidad. Es decir, ejecutar lo siguiente:

```
cd /home/su_login/
```

Una vez cumplido esto, solo restaría ejecutar el siguiente comando para desmontar */dev/hda1* de */mnt/windows/*:

```
umount /mnt/windows/
```

Si se quiere que también los usuarios, y no solo *root*, puedan montar dicha partición que se está ejemplificando, tecleando tan solo una sencilla línea de comando o valiéndose de los iconos sobre el escritorio o alguna aplicación, es necesario que la partición o unidad de disco esté especificada en el archivo /etc/fstab del siguiente modo:

```
/dev/hda1 /mnt/windows        vfat      user,rw,exec,nosuid,noauto,gid=100    0 0
```

La línea específica que del dispositivo */dev/hda1* que tendría como punto de montaje */mnt/windows/* y que posee formato en FAT o FAT32 *(vfat)*, podrá ser montada y desmontada por los usuarios *(user)* en modo de lectura y escritura *(rw)*, con permisos de ejecución de programas *(exec)*, sin permitir la ejecución de programas con SUID *(nosiud)*, y que el contenido de la partición le pertenecerá por defecto al grupo *users (gid=100)*, al cual pertenecen todos los usuarios del sistema, y dicha partición, al igual que las unidades de disco extraíble, no será montada en durante el arranque del sistema *(noauto)*. Los usuarios sin privilegios solo tendrían que ejecutar la siguiente línea de comando para poder montar y acceder a la partición que corresponde a la instalación de Windows:

```
mount /mnt/windows/
```

Fundamentándose sobre el esquema ejemplificado en la tabla 12, lo siguiente sería lo que correspondería a las entradas en */etc/fstab* para configurar una partición de Windows, unidad de floppy, unidad de CDROM y Zip Drive IDE/ATAPI:

```
/dev/hda1 /mnt/windows        vfat      user,rw,exec,nosuid,noauto,gid=100    0 0
/dev/hdc  /mnt/cdrom          iso9660   user,ro,exec,nosuid,noauto    0 0
/dev/hdd4 /mnt/zipdrive       vfat      user,rw,exec,nosuid,noauto,gid=100    0 0
/dev/fd0  /mnt/floppy         vfat      user,rw,exec,nosuid,noauto,gid=100    0 0
```

Disk management

Es un programa incluido con la paquetería de utilidades *(gnome-utilities)* de GNOME. Se localiza en «Menú de GNOME > Programas > Sistema > Disk management». Permitirá montar y desmontar las unidades de disco como son Floppies, unidades de CD-ROM y Zip Drives, siempre que estos estén especificados en el archivo */etc/fstab*. Su funcionamiento es sencillo, bastará con hacer click en los botones «Montar» o «Desmontar». Proporciona, además, información de estado y permitirá dar formato a los disquetes (ver figura 41).

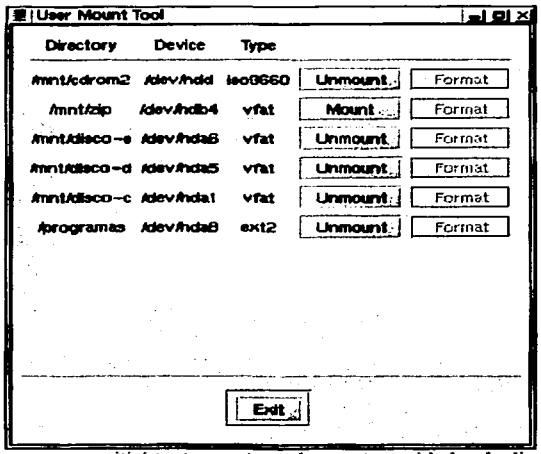

Figura 41. Diskmanagement permitirá tanto montar y desmontar unidades de disco como dar formato a disquetes.

Aplicar montador de discos en el panel de GNOME

Pueden agregarse applets *(apliques)* que realizarán las funciones de montaje y desmontaje de las unidades de disco con un solo clic del mouse. Para agregarlos al panel se necesita hacer clic en le menú de GNOME, y selecciónese «Apliques > Utilerias > Montador de discos». Esto agregará un applet al panel (ver figura 42), al cual solo bastará configurar haciendo clic derecho sobre este y luego clic izquierdo en «Propiedades» para que surja la ventana correspondiente (ver figura 43). Especifíquese la ruta completa que corresponde al punto de montaje (ejemplo: /mnt/floppy). Se podrá también especificar un icono distinto si así se requiere. Hágase clic en aceptar. Cabe aclarar que dicho applet consume alrededor de 0.5 MB de RAM.

Figura 42. Applets montadores de disco en el panel.

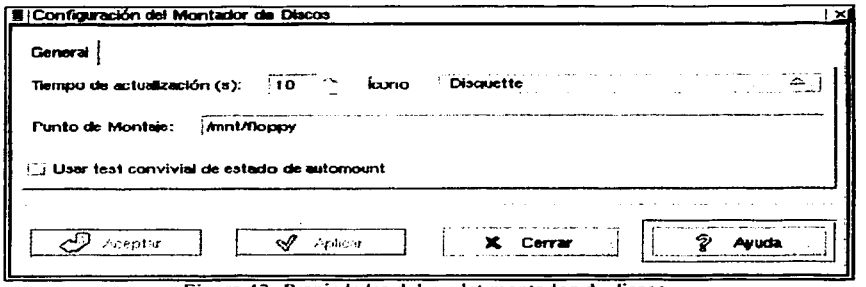

Figura 43. Propiedades del applet montador de discos.

Iconos del escritorio

Si se acaba de configurar o añadir alguna unidad de disco o partición, hagase clic derecho sobre el escritorio de GNOME y elijase "Actualizar dispositivos", a fin de que se realice dicha acción y aparezcan los iconos correspondientes sobre el escritorio de GNOME (figura 44). Cada uno representa una unidad de disco. Bastará con hacer clic derecho sobre alguno y elegir *Montar dispositivo* o *Desmontar dispositivo*. Si se desea, también se podrá especificar un icono en personalizado para cada unidad eligiendo *Propiedades*.

Figura 44. Iconos de las unidades de disco existentes en el sistema se podrán ver y acceder desde el escritorio de Gnome.

Si se hace doble clic sobre alguno de estos iconos, y, por supuesto, hay un disco o disquete insertados, Gnome lo montará automáticamente y abrirá el adminstrador de archivos para mostrar su contenido.

Instalación de un sistema de archivos de red, *Network File System* (NFS) [18]

NFS, acrónimo de *Network File System*, es un popular protocolo utilizado para compartir volúmenes entre máquinas dentro de una red de manera trasparente, más comúnmente utilizado entre sistemas basados sobre UNIX. Es útil y fácil de utilizar, sin embargo no en vano es apodado *cariñosamente* como *"No File Security"*. NFS no utiliza un sistema de contraseñas como el que tiene SAMBA, solo una lista de control de acceso determinada por direcciones IP o nombres. Es por esto que es importante que el administrador de la red local o usuario entienda que un servidor NFS puede ser un verdadero e inmenso agujero de seguridad si este no es configurado apropiadamente e implementado detrás de un firewall.

Solo se recomienda utilizar NFS dentro de una red local detrás de un firewall que permita el acceso solo a las máquinas que integren la red local, nunca para compartir sistemas de archivos a través de Internet. Al no contar con un sistema de autentificación por contraseñas, es un servicio susceptible del ataque de alguna persona mal intencionada. SAMBA es un mucho mejor y más seguro protocolo para compartir sistemas de archivos.

Procedimientos

Teniendo en cuenta los aspectos de seguridad mencionados, es importante seguir los procedimientos descritos a continuación al pie de la letra, y que posteriormente se comprometa también consultar a detalle la documentación incluida en el paquete nfs-utils, ya que éste proporcionará información adicional y completa sobre aspectos avanzados de configuración y utilización.

Configurando el servidor NFS

Se requiere tener instalados nfs-utils y portmap. Se pregunta al sistema si estos están instalados con la siguiente línea de comando:

```
rpm -q nfs-utils portmap
```

Lo cual debe de regresar algo como lo siguiente:

```
nfs-utils-0.3.1-13.7.2.1
portmap-4.0-38
```

En caso de que falte alguno de estos paquetes, se inserta el CD de instalación en la unidad correspondiente, se abre una terminal o consola y se ejecuta lo siguiente:

```
mount /mnt/cdrom/
rpm -Uvh /mnt/cdrom/RedHat/RPMS/paquete_faltante
```

Cabe mencionar que lo mejor será siempre utilizar las versiones de nfs-utils y portmap más actuales. Salvo por RedHat Linux 7.1 o LinuxPPP 7.x, el resto de las versiones anteriores de RedHat y LinuxPPP incluyen paquetes de nfs-utils y portmap con serios agujeros de seguridad. Se recomienda visitar el servidor FTP de la distribución utilizada y descargar los paquetes actualizados, que seguramente incluirán los parches de seguridad necesarios.

Si se utiliza Redhat 6.x o LinuxPPP 6.x, la más reciente versión de *nfs-utils*, que corresponde a la 0.3.1, requerirá además que actualice el paquete *mount* a su versión 2.10r o superior, y que también se podrá encontrar en el mismo directorio del servidor FTP.

Lo siguiente será configurar un nivel de seguridad para *portmap*. Esto se consigue editando los archivos */etc/hosts.allow* y */etc/hosts.deny*. Se debe especificar qué direcciones IP o rango de direcciones IP pueden

acceder a los servicios de portmap y quienes no pueden hacerlo. Se puede entonces determinar en /etc/hosts.allow como rango de direcciones IP permitidas de la manera siguiente:

```
portmap:192.168.1.0/255.255.255.0
```

Esto corresponde a la dirección IP de la red completa y la máscara de la subred. Adicionalmente se puede especificar direcciones IP individuales sin necesidad de establecer una máscara. Esto es de utilidad cuando se desea compartir volúmenes con otras máquinas en otras redes a través de Internet. Ejemplo:

```
portmap:192.168.1.0/255.255.255.0
portmap:192.168.20.25
portmap:192.168.30.2
portmap:216.200.152.96
portmap:148.240.28.171
```

Una vez determinado qué direcciones IP pueden acceder a portmap, solo resta determinar quienes no pueden hacerlo. Evidentemente se refiere al resto del mundo, y esto se hace agregando la siguiente línea:

```
portmap:ALL
```

Es importante destacar que la línea anterior es **INDISPENSABLE** y **NECESARIA** si se quiere tener un nivel de seguridad decente. De manera predeterminada las versiones más recientes de nfs-utils no permitirán iniciar el servicio si esta línea no se encuentra presente en /etc/hosts.deny.

Una vez configurado portmap, debe reiniciarse el servicio de portmap:

```
/etc/rc.d/init.d/portmap restart
```

Si se tiene un DNS, dar de alta las direcciones IP asociadas a un nombre o bien editar /etc/hosts y agregar las direcciones IP asociadas con un nombre. Esto servirá como listas de control de accesos. Ejemplo del archivo /etc/hosts:

```
127.0.0.1       localhost.localdomain   localhost
192.168.1.254   servidor.mi-red-local.org servidor
192.168.1.2     algun_nombre.mi-red-local.org     algun_nombre
192.168.1.3     otro_nombre.mi-red-local.org      otro_nombre
192.168.1.4     otro_nombre_mas.mi-red-local.org otro_nombre_mas
192.168.1.5     como_se_llame.mi-red-local.org    como_se_llame
192.168.1.6     como_sea.mi-red-local.org     como_sea
192.168.1.7     lo_que_sea.mi-red-local.org       lo_que_sea
```

Se procede a determinar que directorio se va a compartir. Se puede crear también uno nuevo:

```
mkdir /home/nfs/
```

Una vez hecho esto, se necesita establecer qué directorios en el sistema serán compartidos con el resto de las máquinas de la red, o bien a que máquinas, de acuerdo al DNS o /etc/hosts se le permitirá el acceso. Esto se debe de agregar en /etc/exports determinando con que máquinas y en que modo se hará. Se puede especificar una dirección IP o bien nombre de alguna máquina, o bien un patrón común con comodín para definir que máquinas pueden acceder. De tal modo se puede utilizar el siguiente ejemplo:

```
/home/nfs *.mi-red-local.org(ro)
```

En el ejemplo anterior se esta definiendo que se compartirá /home/nfs/ a todas las máquinas cuyo nombre, de acuerdo al DNS o /etc/hosts, tiene como patrón común **mi-red-local.org**, en modo de solo lectura. Se utilizó un asterisco (*) como comodín, seguido de un punto y el nombre del dominio. Esto permitirá que *como_se_llame.mi-red-local.org*, *como_sea.mi-red-local.org*, *lo_que_sea.mi-red-local.org*, etc., podrán

acceder al volumen /home/nfs/ en modo solo lectura. Si se quiere que el acceso a este directorio sea en modo de lectura y escritura, se cambia (ro) por (rw):

```
/home/nfs *.mi-red-local.org(rw)
```

Ya que se definieron los volúmenes a compartir, solo resta iniciar o reinciar el servicio nfs. Utilizar cualquiera de las dos líneas dependiendo el caso:

```
/etc/rc.d/init.d/nfs start
/etc/rc.d/init.d/nfs restart
```

A fin de asegurar de que el servicio de *nfs* esté habilitado la siguiente vez que se encienda el equipo, se debe ejecutar lo siguiente:

```
/sbin/chkconfig --level 345 nfs on
```

El comando anterior hace que se habilite *nfs* en los niveles de corrida 3, 4 y 5.

Como medida de seguridad adicional, si se tiene un *firewall* implementado, cerrar, para todo aquello que no sea parte de la red local, los puertos tcp y udp 2049, ya que estos son utilizados por NFS para escuchar peticiones.

Configurando las máquinas cliente

Para probar la configuración, es necesario que las máquinas clientes se encuentren definidas en el DNS o en el archivo */etc/hosts* del servidor. Si no hay un DNS configurado en la red, deberán definirse los nombres y direcciones IP correspondientes en el archivo /etc/hosts de todas las máquinas que integran la red local. A continuación se crea, como *root*, desde cualquier otra máquina de la red local un punto de montaje:

```
mkdir /mnt/servidornfs
```

Y para proceder a montar el volumen remoto, se utiliza la siguiente línea de comando:

```
mount -t nfs servidor.mi-red-local.org:/home/nfs /mnt/servidornfs
```

Si por alguna razón en el DNS de la red local, o el archivo /etc/hosts de la máquina cliente, decidió no asociar el nombre de la máquina que funcionará como servidor NFS a su correspondiente dirección IP, se puede especificar ésta en lugar del nombre. Ejemplo:

```
mount -t nfs 192.168.1.254:/home/nfs /mnt/servidornfs
```

Se podrá acceder entonces a dicho volumen remoto con solo cambiar al directorio local definido como punto de montaje, del mismo modo que se haría con un disquete o una unidad de CDROM:

```
cd /mnt/servidornfs
```

Si se desea poder montar este volumen NFS con una simple línea de comando o bien haciendo doble clic en un icono sobre el escritorio, será necesario agregar la correspondiente línea en /etc/fstab. Ejemplo:

```
servidor.mi-red-local.org:/home/nfs      /mnt/servidornfs          nfs
user,exec,dev,nosuid,rw,noauto 0 0
```

La línea anterior especifica que el directorio /home/nfs/ de la máquina servidor.mi-red-local.org será montado en el directorio local /mnt/servidor/nfs, permitiéndole a los usuarios el poder montarlo, en modo de lectura y

escritura y que este volumen no será montado durante el arranque del sistema. Esto último es de importancia, siendo que si el servidor no está encendido al momento de arrancar la máquina cliente, este se colgará durante algunos minutos.

Una vez agregada la línea en /etc/fstab de la máquina cliente, si utiliza GNOME Midnight Commander, el administrador de archivos de GNOME-1.1 y 1.2, solo restará iniciar una sesión gráfica, hacer clic derecho sobre el escritorio y seleccionar Actualizar dispositivos o *Rescan devices*. Esto colocará un icono adicional sobre el escritorio que deberá ser tratado del mismo modo que se haría con un disquete o unidad de CDROM.

Figura 45. Unidad Instalada por medio de NFS

Si se utiliza GNOME-1.4 o superior, éste incorpora Nautilus como administrador de archivos, mismo que auto detecta cualquier cambio en /etc/fstab. Solo se hace clic derecho sobre el escritorio y se selecciona el disco que se desea montar.

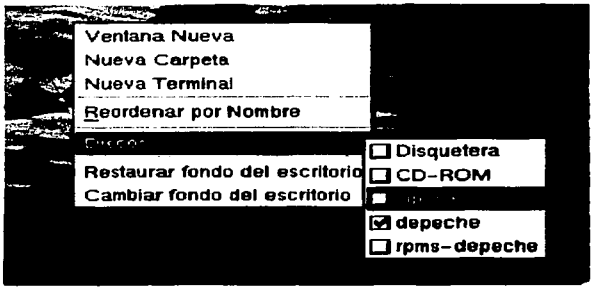

Figura 46. Selección de unidad a montar via NFS

Instalación de Linux por medio de un servidor NFS

Este es quizás el uso más común para un volumen NFS. Permite compartir un volumen que contenga una copia del CD de instalación de alguna distribución y realizar inclusive instalaciones simultáneas en varios equipos. Tiene como ventaja el que la instalación puede resultar más rápida que si se hiciese con un CDROM, siendo que la tasa de trasferencia de archivos será determinada por el ancho de banda de la red local, y permitirá instalar Linux en máquinas que no tengas unidad de CDROM.

Una vez creado y configurado un volumen a compartir se copiará todo el contenido del CD de instalación en éste:

```
cp -r /mnt/cdrom/* /home/nfs/
```

En el directorio *images* del CD se encuentran varias imágenes para crear disquetes de arranque. Se utilizará bootnet.img para crear el número de disquetes necesarios para cada máquina en la que se realizará una instalación, y que permitirán acceder a la red. Se inserta un disquete y se ejecuta lo siguiente:

```
cd /home/nfs/images/
dd if=bootnet.img of=/dev/fd0 bs=1440k
```

Añadir en /etc/hosts, o bien dar de alta en el DNS, las direcciones IP, que serán utilizadas por las nuevas máquinas, asociadas a un nombre con el dominio que específico como regla de control de acceso en /etc/exports *(es decir *.mi-red-local.org)*. Para /etc/hosts, puede quedar algo así:

```
127.0.0.1       localhost.localdomain   localhost
192.168.1.254   servidor.mi-red-local.org servidor
192.168.1.2     algun_nombre.mi-red-local.org     algun_nombre
192.168.1.3     otro_nombre.mi-red-local.org      otro_nombre
192.168.1.4     otro_nombre_mas.mi-red-local.org otro_nombre_mas
192.168.1.5     como_se_llame.mi-red-local.org     como_se_llame
192.168.1.6     como_sea.mi-red-local.org          como_sea
192.168.1.7     lo_que_sea.mi-red-local.org       lo_que_sea
192.168.1.8     nueva_máquina.mi-red-local.org      nueva_máquina
192.168.1.9     otra_nueva_máquina.mi-red-local.org  otra_nueva_máquina
```

Utilizar estos disquetes para arrancar en los equipos, ingresar una dirección IP y demás parámetros para ésta máquina y cuando se pregunte ingresar la dirección IP del servidor NFS y el directorio en éste donde se encuentra la copia del CD de instalación. El resto continuará como cualquier otra instalación.

Cómo configurar Sendmail [17]

La mayoría de las distribuciones de Linux incluyen de manera predeterminada Sendmail, un poderoso servidor de correo electrónico ampliamente utilizado alrededor del mundo. Este requiere de una correcta configuración para su mejor aprovechamiento y poder disponer de un nivel de seguridad aceptable.

Es muy común que los administradores inexpertos no se molesten siquiera en establecer un nivel de seguridad apropiado en sus redes locales, y mucho menos en el servidor de correo, el cual ven como un servicio más. Es un error común el configurar Sendmail para que permita enviar correo como sea a cualquier costo. Usualmente este costo significa convertirse en *Open Relay*, y por lo tanto en un paraíso para personas que se dedican al envío masivo de correo comercial (Spam).

Para la correcta configuración de Sendmail se toman las siguientes consideraciones:

- Se cuenta con un dominio propio.
- Que se **tiene un IP permanente** o estática, **y no una dinámica**, y que se trata de un enlace dedicado, como E1, DSL, T1 o T3, etc. Es decir, **NO** se conecta a Internet por medio de un modem.
- Se tiene perfectamente configurada la red local y parámetros de red del servidor.
- Que se utiliza **Red Hat Linux 7.1 o 7.2** o al menos **Sendmail-8.11.6** y xinetd-2.3.3.

Las siguientes instrucciones permitirán:

- Enviar y recibir correo electrónico.
- Establecer un buen nivel de seguridad.
- Filtrar el molesto *Spam*, o correo masivo no solicitado, que a muchos aqueja a diario, para toda la red local.

Requerimientos y lista de materiales

- Un servidor con al menos 32 MB RAM y alguna distribución de Linux instalada.
- Deben de estar bien configurado los parámetros de red y un servidor de nombres *(DNS)*.
- Preferentemente, aunque no indispensablemente, deberá utilizar DOS tarjetas de red. Lo que si será obligatorio es disponer de al menos dos interfaces. Una para acceder a la red local y otra para acceder hacia Internet (una de estas puede ser virtual, o eth0:0, o bien una segunda interfaz real, o eth1).
- Tener instalados los paquetes sendmail, sendmail-cf, m4, make, xinet e imap **que vienen incluidos en el CD de instalación** o servidor FTP de actualizaciones para la versión de la distribución que se utilice.

Tomar en consideración que, de ser posible, se debe utilizar la versión estable más reciente de todo el software que se vaya a instalar al realizar los procedimientos descritos en este trabajo, a fin de contar con los parches de seguridad necesarios. **Ninguna versión de sendmail anterior a la 8.11.6 se considera como apropiada** debido a fallas de seguridad de gran importancia, y ningún administrador *competente* utilizaría una versión inferior a la 8.11.6. Por favor visitar el sito web de la distribución predilecta para estar al tanto de cualquier aviso de actualizaciones de seguridad. Ejemplo: para Red Hat Linux 7.1 y 7.2 hay paquetería de actualización en los siguientes enlaces:

- ftp://updates.redhat.com/7.1/en/os/i386/, si posee alguna distribución basada sobre Red Hat Linux 7.1
- ftp://updates.redhat.com/7.2/en/os/i386/, si posee alguna distribución basada sobre Red Hat Linux 7.2

Procedimientos

Preparativos

Lo primero será establecer que es lo que se tiene en la red local y que es lo que se hará con esto. Determinar qué máquinas de la red local, específicamente las direcciones IP, necesitan poder enviar y recibir correo electrónico y cuales NO deben hacerlo.

Determinar como se desea recuperar los mensajes de correo electrónico que arriben al servidor. **POP3** o **IMAP**.

POP3: Es el protocolo de recuperación de correo electrónico más utilizado en la actualidad. Permite recuperar el correo pero este se almacenará localmente en el disco duro de las máquinas de los usuarios.

IMAP: Este protocolo almacena el correo electrónico, y permite la creación de carpetas de usuario, en el servidor. De modo tal, los usuarios pueden acceder desde cualquier parte del mundo a su buzón de correo y carpetas personales. IMAP también facilita la utilización de *webmails* (servicios de correo basado sobre web).

Determinar el nombre de todos los posibles nombres o aliases que tenga el servidor. Ejemplo: mi-dominio.org, mail.mi-dominio.org, servidor.mi-dominio.org, mi-red-local-org, mail.mi-red-local.org, etc.

Configurar las dos tarjetas de red, una para la red local con la IP inválida y otra para la dirección IP real.

Verificando parámetros de red

Se debe definir el nombre de la máquina que funcionará como servidor de correo. Normalmente se utiliza el esquema *nombre_máquina.nombre_dominio*. Un ejemplo del nombre de la máquina servidor sería

servidor.mi-dominio.org.mx. Se debe de asegurarse de que esto se encuentra perfectamente definido en */etc/sysconfig/network* y */etc/hosts*:

Para */etc/sysconfig/network*, es decir, el nombre que se le asigna a la máquina, correspondería lo siguiente:

```
NETWORKING=yes
HOSTNAME=servidor.mi-dominio.org.mx
GATEWAY=148.243.59.254
```

Para */etc/hosts*, es decir, la información de los hosts y las direcciones IP, correspondería lo siguiente:

```
# Primero, se verifica que las direcciones IP del
# servidor estén asociadas correctamente a un nombre
# largo y uno corto. Los espacios son con tabuladores.
127.0.0.1       localhost.localdomain                   localhost
148.243.59.1    servidor.mi-dominio.org.mx              servidor
192.168.1.1     intranet.mi-red-local.org.mx            intranet
#
# Opcionalmente aqui se pueden agregar también
# los nombres y direcciones IP de la máquinas
# de la red local.
192.168.1.2     máquina2.mi-red-local.org.mx máquina2
192.168.1.3     máquina3.mi-red-local.org.mx máquina3
192.168.1.4     máquina4.mi-red-local.org.mx máquina4
```

Además de configurar correctamente un DNS, definir bien los *DNS* o servidores de nombres de dominios correspondientes. Esto se debe hacer en el archivo */etc/resolv.conf*, de un modo similar al siguiente:

```
search mi-dominio.org.mx
#
# El IP de la máquina que tiene el DNS de la red local.
nameserver 192.168.1.1
#
# Los DNS del proveedor de servicios.
nameserver 200.33.213.66
nameserver 200.33.209.66
```

Confirmando la instalación de Sendmail

Es importante tener instalados los paquetes *sendmail* y *sendmail-cf*, ya que se utilizará el servidor de correo *Sendmail* para el envío de los mensajes y filtrado de correo masivo no solicitado *(Spam)*, y el paquete *imap*, mismo que permitirá utilizar el servicio de IMAP y POP3. Para asegurarse de esto, se puede utilizar la siguiente línea de comando:

```
rpm -q sendmail sendmail-cf imap
```

Esto debe devolver las versiones de *sendmail*, *sendmail-cf* e *imap* que se tienen instaladas. Si no fuese así, se debe cambiar a *root*, si aún no se ha hecho, y proceder a instalar estos paquetes. Introducir el CDROM de su distribución y seguir el siguiente procedimiento:

```
mount /mnt/cdrom

cd /mnt/cdrom/RedHat/RPMS

rpm -Uvh sendmail-* imap-*

cd $home

eject /mnt/cdrom
```

Se debe instalar *sendmail-cf* o no será posible compilar los archivos necesarios para configurar *Sendmail*. El paquete *imap*, el cual contiene el daemon (proceso del sistema) para el protocolo POP3, es el que permitirá recuperar el correo desde el servidor en el resto de las máquinas que integren la red local con cualquier cliente de correo electrónico.

Configurando Sendmail

Antes de continuar, se debe editar el archivo /etc/mail/local-host-names, en el cual se deben de listar todos y cada uno de los aliases que tenga el servidor que se está configurando, así como los posibles sub-dominios. Es decir, todos los dominios para los cuales se estará recibiendo correo en un momento dado.

```
# Incluir aqui todos los dominios para los que se
# reciban correo.
mi-dominio.org.mx
servidor.mi-dominio.org.mx
mail.mi-dominio.org.mx
mi-red-local.org.mx
intranet.mi-red-local.org.mx
mail.mi-red-local.org.mx
```

Se procede entonces a modificar el archivo */etc/mail/sendmail.mc*, con previo respaldo del original, a fin de preparar la configuración del servidor de correo.

```
cp /etc/mail/sendmail.mc /etc/mail/sendmail.mc.default
```

Por defecto Sendmail solo permitirá enviar correo solo desde la interfaz *loopback* (127.0.0.1), es decir, desde el mismo servidor. Si se desea poder enviar correo desde las máquinas de la red local **comentar la línea** o bien, si se tienen varias, añadir las interfaces desde las cuales se quiere que escuche peticiones sendmail y **omitir** las que no debe, como sería una red local secundaria con restricciones.

```
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
```

Si se quiere filtrar Spam de manera eficiente, la mejor manera de empezar a hacerlo es rechazando correo proveniente de dominios NO RESUELTOS, es decir dominios que no están registrados en un DNS y que por lo tanto SON inválidos. Para tal fin, a menos que se requiera lo contrario, es necesario **mantener comentada** la siguiente línea:

```
dnl FEATURE(`accept_unresolvable_domains')dnl
```

Es necesario establecer que **mi-dominio.org.mx** corresponderá a la máscara que se utilizará para todo el correo que se emita desde el servidor. Se debe, por tanto, añadirse una línea justo debajo de *MAILER(procmail)dnl* y que va del siguiente modo:

```
MASQUERADE_AS(mi-dominio.org.mx)dnl
```

Todo en conjunto, ya modificado, debería de quedar del siguiente modo (**NO modificar el orden de las líneas**):

```
divert(-1)
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID(`linux setup for Red Hat Linux')dnl
OSTYPE(`linux')
define(`confDEF_USER_ID',``8:12'')dnl
undefine(`UUCP_RELAY')dnl
undefine(`BITNET_RELAY')dnl
define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
```

```
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/sendmail.st')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
dnl TRUST_AUTH_MECH(`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS', `DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confTO_QUEUEWARN', `4h')dnl
dnl define(`confTO_QUEUERETURN', `5d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(local_procmail)dnl
FEATURE(`access_db')dnl
FEATURE(`blacklist_recipients')dnl
EXPOSED_USER(`root')dnl
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
dnl FEATURE(`accept_unresolvable_domains')dnl
dnl FEATURE(`relay_based_on_MX')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
MASQUERADE_AS(mi-dominio.org.mx)dnl
```

Luego se procesa con el siguiente comando para generar /etc/sendmail.cf:

```
m4 /etc/mail/sendmail.mc > /etc/sendmail.cf
```

Se abre ahora el archivo */etc/mail/access* y se agregan algunas líneas para definir quienes podrán hacer uso del servidor de correo para poder enviar mensajes:

```
# Por defecto, solo se permite enviar correo desde localhost...
localhost.localdomain                   RELAY
localhost                       RELAY
127.0.0.1                       RELAY
# se debe añadir los nombres y direcciones IP
# que ahora tenga el servidor
mi-dominio.org.mx   RELAY
servidor.mi-dominio.org.mx    RELAY
mi-red-local.org.mx           RELAY
intranet.mi-red-local.org.mx RELAY
192.168.1.1                             RELAY
148.243.59.1                            RELAY
#
# Agregar también los nombres COMPLETOS de la máquinas
# y direcciones IP que integran la red local.
# Solo especificar aquellas máquinas que tendrán
# permitido enviar y recibir correo. No es buena idea
# especificar redes completas. Especificar máquinas
# individuales, aunque signifique ingresar manualmente un
# centenar de entradas. Es más seguro de este modo.
máquina2.mi-red-local.org.mx RELAY
máquina3.mi-red-local.org.mx RELAY
máquina4.mi-red-local.org.mx RELAY
192.168.1.2                             RELAY
192.168.1.3                             RELAY
192.168.1.4                             RELAY
```

```
# etc.
#
# Y también se puede agregar las direcciones de correo
# electrónico de aquellos a quienes se consideran
# "indeseables"../../explinux/, o que se quiera bloquear.
Spam@algun_Spamer.com                    REJECT
info@otro_Spammer.com                    REJECT
#
servidor.indeseable.com                  REJECT
part.com.mx                              REJECT
newlad.com                               REJECT
dmc.com.mx                               REJECT
propnewidea.com                          REJECT
lapromocion.com                          REJECT
hosting.com.mx                           REJECT
solopromos.com.mx              REJECT
# etc.
```

En este archivo también se pueden agregar las direcciones de correo electrónico que se desee bloquear, como son las de quienes envían correo masivo no solicitado *(Spam)*.

Al concluir, se debe también compilar este archivo para generar otro en formato de base de datos a fin de ser utilizado por *Sendmail*:

```
cd /etc/mail
make
```

O bien se puede ejecutar lo siguiente:

```
makemap hash /etc/mail/access.db < /etc/mail/access
```

Será de utilidad designar un *alias* a la cuenta de correo de *root* a fin de recibir los mensajes generados por el sistema en una cuenta común de usuario. Abrir el archivo */etc/aliases*, en donde al final se encontrará las siguientes líneas:

```
# Person who should get root's mail
root:                jperez
```

Esto corresponde a la cuenta de correo local hacia donde se redirecciona el correo de *root*. Descomentar la última línea y asignar el nombre de la cuenta de usuario que utiliza normalmente:

```
# Person who should get root's mail
 root:               jperez
```

A fin de que este nuevo alias surta efecto y pueda ser utilizado por *Sendmail* se debe utilizar el comando *newaliases*:

```
/sbin/newaliases
```

Terminados los detalles de la configuración, se reinicia sendmail del siguiente modo y estará listo un servidor de correo que se podrá utilizar para enviar mensajes para toda la red local utilizando el servidor SMTP del proveedor de servicios:

```
/etc/rc.d/init.d/sendmail restart
```

Generalmente *Sendmail* está incluido entre los servicios que de forma predeterminada se inician con el sistema. Si por alguna razón *Sendmail* no estuviese habilitado, ejecutar lo siguiente a fin de habilitar *sendmail* en los niveles de corrida 3, 4 y 5:

```
/sbin/chkconfig --level 345 sendmail on
```

Si está funcionando un *firewall*, recordar que debe de estar abierto el puerto 25, de otro modo el correo saldría pero no entraría. Añadir o verifiar que esté presente una línea en el guión de firewall similar a la siguiente:

```
#SMTP
/sbin/iptables -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 25 -j ACCEPT
```

Habilitando los servicios POP3 e IMAP

Si se utiliza Red Hat Linux 7.x o versiones posteriores o equivalentes, se debe notar que *inetd* ha sido sustituido por *xinetd*, y utiliza métodos de configuración muy distintos.

Se puede habilitar los servicios ipop3 (POP3 tradicional, autenticación en texto plano), *pop3s* (POP3 seguro, autenticación con criptografía), *imap* (IMAP tradicional, autenticación en texto plano) e *imaps* (IMAP seguro, autenticación con criptografía). Utilizar aquellos que se considere como más apropiados para la red local de acuerdo a las capacidades de los clientes de correo electrónico utilizados. Tomar en cuenta que la autenticación por medio de texto plano es definitivamente un método inseguro, y siempre será mejor usar los servicios que permitan establecer conexiones seguras.

Se pueden habilitar los servicios de manera automática e inmediata ejecutando los siguientes comandos (solo habilitar aquellos que realmente se necesiten):

```
/sbin/chkconfig ipop3 on
/sbin/chkconfig pop3s on
/sbin/chkconfig imap on
/sbin/chkconfig imaps on
```

También se pueden habilitar manualmente con un editor de texto, lo cual es sugerido a fin de habilitar opciones adicionales, como direcciones IP específicas a las cuales se les estaría permitido cierto servicio. Acceder a al directorio /etc/xinet.d/ y editar los archivos *ipop3*, pop3s, imap e imaps, según se requiera. Estos requieren de editar una sola línea para habilitar el servicio:

```
service pop3
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/ipop3d
        log_on_success          += USERID
        log_on_failure          += USERID
        disable                 = no
        only_from               = 192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4 localhost
}
```

Lo mismo aplica para el protocolo IMAP e IMAPS.

Hecho lo anterior, es necesario reiniciar el *daemon* xinetd con la siguiente línea de comando:

```
/etc/rc.d/init.d/xinetd restart
```

¿Que hacer con el Spam?

Sin duda alguna una de las cosas más molestas de Internet es el correo comercial no solicitado, comúnmente llamado Spam. Las empresas que incurren en esta forma de marketing no tienen el mínimo respeto por los demás, y saturan cientos de miles de buzones de correo a diario. Las empresas que incurren en este tipo de

promoción deberían ser boicoteadas y los responsables de enviar el correo deberían ser apedreados públicamente. El siguiente es un método civilizado para combatirlos.

No importa que tan molesto sea, o cuantos mensajes con insultos y llamadas telefónicas de reclamo se hagan a las oficinas de las empresas que incurren en esta poco ética forma de promoción, estas personas no les interesa la opinión de a quienes ellos perjudican haciendo malgastar el ancho de banda o bloqueando servidores de correo. Ellos compran y hacen uso sin autorización de discos con cientos de miles de direcciones de correo electrónico con un solo objetivo: promocionar como sea productos y servicios, en su mayoría, inútiles.

El combate al Spam requiere de la colaboración de los administradores de las redes, quienes deben atender y dar seguimiento a las quejas y tomar las acciones ejemplares pertinentes. Los usuarios deben participar reportando incidentes a los administradores de las redes involucradas.

Empresas que, por alguna razón, y gracias a *lagunas legales*, recurren al envío de Spam, pueden ser bloqueadas por completo añadiendo una entrada que rechace correo generado por los servidores de empresas que incurran en Spam. Esto se hace editando /etc/mail/access y generando /etc/mail/access.db. Ejemplo:

```
part.com.mx                    REJECT
newlad.com                     REJECT
dmc.com.mx                     REJECT
propnewidea.com                REJECT
lapromocion.com                REJECT
hosting.com.mx                 REJECT
solopromos.com.mx              REJECT
```

Acto seguido se ejecuta el siguiente comando:

```
makemap hash /etc/mail/access.db < /etc/mail/access
```

Y se reinicia Sendmail. En adelante todo correo enviado desde los dominios anteriormente mencionados, será rechazado por completo para toda la red.

Otra opción más del administrador es bloquear también el acceso a los dominios involucrados a través de IPChains o IPTables. Esto no impedirá que llegue correo, pero servirá para boicotear a las empresas que utilizan Spam para promocionarse, al no permitir el acceso a "**sus**" redes desde "**nuestras**" redes locales.

Para determinar la dirección IP de un dominio en particular, solo baste ejecutar el comando *host*, el cual devolverá la dirección IP y quizá algo de información adicional, como si se trata del alias de otro dominio.

```
host solopromos.com.mx
solopromos.com.mx. has address 200.57.146.18
```

Una vez determinadas las direcciones IP problemáticas, solo hay que añadir algunas líneas en el script de *Firewall* que se este utilizando de modo tal que queden bloqueadas de manera permanente, por lo menos desde la red local. Ejemplo:

```
/sbin/iptables -A INPUT -s 216.219.236.81 -d 0/0 -j DROP
/sbin/iptables -A INPUT -s 64.65.27.126 -d 0/0 -j DROP
/sbin/iptables -A INPUT -s 200.57.146.18 -d 0/0 -j DROP
```

Mientras más usuarios y administradores participen reportando y castigando el Spam, correspondientemente, esta molestia desaparecerá eventualmente, o al menos se hará saber a quienes se promocionan de este modo que NO AGRADA lo que hacen.

Configuración de Apache para CGI [17]

Apache es uno de los pocos servicios que no necesitan de mayores modificaciones después de su instalación a fin de funcionar. De hecho solo se necesita se inicie el servicio y se publiquen las páginas correspondientes. El soporte para los distintos módulos se habilita por sí solo a través de scripts incluidos dentro de cada uno de los paquetes RPM que se instalen, como serían PHP, mod_perl, mod_dav, mod_ssl, etc.

Generalmente, al concluir la instalación de Red Hat Linux, el administrador se encontrará con que no le es posible utilizar scripts CGI *(acrónimo de Common Gateway Interface)*. Como una medida de seguridad, las opciones que permiten la ejecución de scripts CGI están deshabilitadas. Configurar Apache para que ejecute scripts CGI no es complicado y solo requerirá editar algunas líneas del archivo */etc/httpd/conf/httpd.conf*.

Procedimientos

Aunque Linuxconf sea una herramienta muy útil para configurar diversos servicios en Linux, distribuciones basadas sobre Red Hat 6.2 y versiones anteriores no lo son para configurar Apache. Se recomienda utilizar algún editor de texto, abrir el archivo */etc/httpd/conf/httpd.conf*, haciendo primero un respaldo de este por si acaso cometiese un error al teclear, proceder a editarlo como se describe a continuación.

Aproximadamente a los 2/3 del archivo, editar las líneas de la configuración del directorio */cgi-bin* del servidor de modo que queden del siguiente modo:

```
<Directory "/home/httpd/cgi-bin">
    AllowOverride None
    Options Indexes Includes ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

Ejecución de CGI fuera del directorio cgi-bin

Si se desea que sea posible ejecutar scripts CGI fuera de */cgi-bin*, se debe primero descomentar, o bien escribirla si no existiese, la siguiente línea:

```
AddHandler cgi-script .cgi
```

Después agregar *ExecCGI* a la configuración del directorio raíz de Apache, de forma que quede del siguiente modo:

```
<Directory "/home/httpd/html">
    Options Indexes Includes FollowSymLinks ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

Probando la configuración

Asegurar de que Apache se está ejecutando, utilizar algun editor de texto para crear un archivo llamado *tiempo.pl*, mismo que se guardará en el directorio */home/httpd/cgi-bin*. Este deberá llevar lo siguiente como contenido:

```
#!/usr/bin/perl

print "content-type: text/html\n\n";
print scalar localtime;
```

```
print "\n";
```

Se debe de cambiar el permiso del archivo anterior con la siguiente línea de comando:

```
chmod 755 /home/httpd/cgi-bin/tiempo.pl
```

Utilizar entonces el navegador web y probar la siguiente dirección: *http://localhost.localdomain/cgi-bin/tiempo.pl*. Si el navegador da una salida similar a la siguiente, se habrá configurado exitosamente Apache para ejecutar scripts CGI:

```
Fri Apr 28 21:17:51 2000
```

Problemas posteriores

Error más común número 1

```
Forbidden
You don't have permission to access /algun/directorio/guion.cgi on this server
```

Significa que el archivo no cuenta con los permisos apropiados de lectura, escritura y ejecución. La mayoría scripts CGI que se encuentran en Internet requerirán al menos permiso 755 para poder ser utilizados.

Error más común número 2

```
Internal Server Error
The server encountered an internal error or misconfiguration and was unable to complete your
request.
```

Significa que hay problemas con el script CGI en si y no con Apache. En la mayoría de los casos se requerirá que el administrador revise línea por línea para localizar un posible error o parámetro incorrecto. Cuando aplique, verificar que la primera línea del guión que apunta hacia donde se encuentra *perl* sea correcta. Verificar también si el directorio que albergue el guión CGI requiere algún permiso en particular, como sería 777 en el caso de algunos scripts CGI.

Como configurar Apache para bloquear agentes de usuario indeseables [18]

Los robots para capturar direcciones de correo, a su vez aprovechados para enviar Spam, y el abuso de ciertos agentes de usuario, como Teleport Pro, continua siendo el dolor de cabeza de todos los administradores de servidores de correo alrededor del mundo.

Los robots especializados en la captura de direcciones de correo electrónico provenientes de sitios web se han convertido en un lucrativo negocio para empresas que distribuyen a nivel mundial discos CD-ROM repletos de estas. El principal problema para el administrador consiste en proteger las direcciones de correo electrónico que los visitantes regulares podrían dejar en algún foro de discusión o tablón de mensajes.

Otro problema aún mayor es el abuso de agentes de descarga de sitios web completos a los discos duros locales de los usuarios. Este tipo de actividad no sería tan problemático si no fuese debido al excesivo consumo de ancho de banda y a la increíblemente estúpida ocurrencia de los usuarios de que descargarán más rápidamente un sitio web haciéndolo hasta con **diez o veinte hilos simultáneos**. Esto significa problemas para aquellos sitios web que utilizan bases de datos, debido a que este tipo de clientes llegan a abrir hasta cientos de conexiones simultáneas conllevando al bloqueo de la base de datos, y subsiguiente *Denial of Service* que perjudicará al no permitir que el resto de los usuarios puedan acceder a los sitios web de manera legítima.

Una forma de combatir estos molestos fenómenos consiste en bloquear el acceso de robots y agentes de usuario desde los servidores web.

Los procedimientos:

Spambots

Nota: Para mayores referencias sobre este método, consultar uno de los artículos originales (en inglés) que se encuentra localizado en http://evolt.org/article/Using_Apache_to_stop_bad_robots/18/15126/.

Determinar que agentes de usuario están accediendo a un sitio web no es complicado, y solo bastará con revisar el archivo de registro de acceso de Apache, regularmente localizado en */var/log/httpd/access_log*. Desde este se puede examinar que agentes de usuario han sido utilizados para acceder al servidor.

Los agentes de descarga o copia web son fáciles de identificar, pues regularmente llevan nombres descriptivos (Web Copies, WebStreaper, WebReaper), o bien se pueden consultar en Robotstxt.org para una lista detallada por tipo y así no confundir un *robot* útil con uno perjudicial. Lo más difícil es determinar que Agentes de Usuario (User Agents) o clientes se están utilizando para realizar la captura de direcciones de correo. Sin embargo puede establecerse una *"trampa"* utilizando el archivo robots.txt. Esta consiste en añadir la siguiente línea:

```
Disallow: /email-addresses/
```

El directorio */email-addresses/* no debe existir. A diferencia de los robots útiles y que llevarán valioso tráfico, como los de los indexadores de los sitios de búsqueda (no se pretende bloquear los robots de Google ni otros buscadores), la mayoría de los robots utilizados para capturar direcciones de correo no respetan las reglas establecidas en robots.txt y suelen buscar y acceder directorios que puedan contener direcciones a como de lugar. Se debe esperar al menos un par de semanas, o, mejor aún, un mes. Pasado este tiempo, puede revisarse el contenido de */var/log/httpd/access_log* y revisar aquellas líneas que indicarán que clientes fueron utilizados para acceder a */email-addresses/*.

Puede utilizarse el siguiente comando para determinar quienes accedieron a */email-addresses/*:

```
grep /email-addresses access_log | awk '{print $12}' | uniq
```

O bien:

```
cat access_log |grep email-address
```

Ejemplo:

```
216.219.236.81 - - [24/Oct/2001:10:45:16 -0600] "GET /email-addresses/ HTTP/1.0" 404 294 "-"
"EmailWolf"
```

Una vez determinados los culpables, solo hay que editar /etc/httpd/conf/httpd.conf y algunas líneas que califiquen a los clientes justo encima de *<Directory "/var/www/html">*. Ejemplo:

```
SetEnvIfNoCase User-Agent "^EmailSiphon" bad_bot
SetEnvIfNoCase User-Agent "^EmailWolf" bad_bot
```

Esto establece como variable **bad_bot** a cualquier cliente que acceda al sitio web y que se identifique como EmailSiphon o EmailWolf. Recordar que se requiere que se encuentre habilitado el módulo de Apache mod_setenvif. A continuación se añade **Deny from env=bad_bot** a la configuración del directorio raíz de Apache:

```
<Directory "/var/www/html">
    Options Indexes Includes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
    Deny from env=bad_bot
</Directory>
```

Esto establece que se denegará el acceso, devolviendo un error 403 común y corriente, a cualquier cliente que sea clasificado como **bad_bot**.

En resumen, esta sería un ejemplo de toda la configuración a aplicar:

```
SetEnvIfNoCase User-Agent "^EmailSiphon" bad_bot
SetEnvIfNoCase User-Agent "^EmailWolf" bad_bot

<Directory "/var/www/html">
    Options Indexes Includes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
    Deny from env=bad_bot
</Directory>
```

Agentes de copiado o descarga web

Como es sabido, es común que en sitos web, que hacen utilizar MySQL, en ocasiones se bloquee el acceso a la base de datos, devolviendo el mensaje:

Warning: Host 'tu_dominio.com' is blocked because of many connection errors. Unblock with 'mysqladmin flush-hosts'

En muchos casos es debido a que no se trata de la única aplicación con que se accede a una misma base de datos y se utiliza *mysql_pconnect()* (conexión persistente) en lugar de una más saludable y convencional *mysql_connect()*, algo ya bien conocido por usuarios de PHP-Nuke. Pero cuando se usa el parámetro de conexión correcto y aún así se sufre de recurrentes bloqueos de bases de datos, esto es culpa total de los clientes de copia web como WebZIP, eCatch, WebReaper, WebStripper, WebCopier y otros *robots* como Scooter-W3-1.0. Ahora entonces, ¿cómo solucionar este problema?.

Dichos clientes suelen abrir (de manera simultánea) **cientos de páginas en solo unos minutos**, y por lo tanto estableciendo **docenas y hasta cientos de conexiones a MySQL**. La utilización de dichos clientes sobre sitos web que utilizan MySQL puede ser definitivamente abusiva de cualquier modo que se quiera ver.

¿Cómo se puede solucionar esto? La respuesta es bloqueando el acceso a los web, o secciones críticas que utilicen MySQL, a dichos clientes. Esto se puede hacer con Apache en el archivo */etc/httpd/conf/httpd.conf* o bien desde *robots.txt*.

Bloquear desde httpd.conf, puede hacerse del mismo modo que se estableció en el punto anterior, sobre como bloquear los *spambots* o colectores de direcciones de correo.

```
SetEnvIfNoCase User-Agent "^EmailSiphon" bad_bot
SetEnvIfNoCase User-Agent "^EmailWolf" bad_bot
SetEnvIfNoCase User-Agent "^WebZIP" bad_bot
SetEnvIfNoCase User-Agent "^WebStripper" bad_bot
SetEnvIfNoCase User-Agent "^Teleport Pro" bad_bot
SetEnvIfNoCase User-Agent "^eCatch" bad_bot
SetEnvIfNoCase User-Agent "^WebCopier" bad_bot
SetEnvIfNoCase User-Agent "^Wget" bad_bot

<Directory "/var/www/html">
    Options Indexes Includes FollowSymLinks
```

```
    AllowOverride None
    Order allow,deny
    Allow from all
    Deny from env=bad_bot
</Directory>
```

Para *robots.txt*, otro método menos efectivo pero más simple y tolerante, consiste en poner un archivo denominado *robots.txt* en el directorio raíz del sitio web. Dicho archivo es utilizado de manera estándar por los robots (o web-bots) para determinar que directorios acceder o no acceder para distintas funciones, como indexar sitios web en los motores de búsqueda. A los clientes de copia web, por lo general, se les añade también soporte para lectura de *robots.txt*, como una manera de evitar el abuso sobre sitios web.

En este archivo se pueden establecer reglas para distintos clientes. Dicho archivo puede definir a un agente en particular y regla específica para éste. Ejemplo:

```
User-agent: WebZIP
Disallow: /
```

Lo anterior define que para cualquier cliente identificado como "WebZIP" no le estará permitido indexar (y por lo tanto descargar) el contenido de todo el sitio web. Otro ejemplo:

```
User-agent: WebStripper
Disallow: /phpnuke
```

Lo anterior especifica que cualquier cliente identificado como WebStripper no le estará permitido indexar (y por lo tanto descargar) el contenido de */phpnuke* en el sitio web.

Ahora, poniendo en práctica lo anterior, el siguiente sería el ejemplo de como se puede mantener saludable el sitio con PHP + MySQL:

```
User-agent: WebZIP
Disallow: /

User-agent: WebStripper
Disallow: /

User-agent: Teleport Pro
Disallow: /

User-agent: Wget
Disallow: /

User-agent: eCatch
Disallow: /

User-agent: WebCopier
Disallow: /
```

Hay varias docenas de clientes más que pueden añadirse de este mismo modo. No hay nada de malo en bloquear dichos clientes, siendo que no son visualizadores web, sino herramientas de descarga que no solo no hacen un uso ético de los recursos web sino que abusan de ellos, y que además, en varios casos particulares, violan leyes de derechos de autor.

¿Por que bloquear el accesos a todo el sitio web? Simple: dichos clientes hacen que se consuma más ancho de banda del necesario, y además es raro que los usuarios que utilizan estas herramientas realmente vean TODO el material que descargaron. Simplemente es contenido web que almacena en el disco duro y que puede que nunca lleguen siquiera a consultar. Así que de cualquier modo que se quiera ver, es un desperdicio de valioso y costoso ancho de banda permitir a los visitantes utilizar dichos clientes sobre los sitios web.

El archivo Htaccess

También es posible habilitar el filtrado de agentes de usuario editando y añadiendo parámetros en el archivo *.htaccess* del directorio raíz. Ejemplo:

```
SetEnvIfNoCase User-Agent "^Bloodhound" bad_bot
SetEnvIfNoCase User-Agent "^eCatch" bad_bot
SetEnvIfNoCase User-Agent "^GetRight" bad_bot
SetEnvIfNoCase User-Agent "^LeechFTP" bad_bot
SetEnvIfNoCase User-Agent "^Mass Downloader" bad_bot
SetEnvIfNoCase User-Agent "^Prozilla" bad_bot
SetEnvIfNoCase User-Agent "^Offline Explorer" bad_bot
SetEnvIfNoCase User-Agent "^RealDownload" bad_bot
SetEnvIfNoCase User-Agent "^SiteSnagger" bad_bot
SetEnvIfNoCase User-Agent "^Teleport Pro" bad_bot
SetEnvIfNoCase User-Agent "^WebCopier" bad_bot
SetEnvIfNoCase User-Agent "^Web Downloader" bad_bot
SetEnvIfNoCase User-Agent "^webfetcher" bad_bot
SetEnvIfNoCase User-Agent "^WebFountain" bad_bot
SetEnvIfNoCase User-Agent "^Wget" bad_bot
SetEnvIfNoCase User-Agent "^WebMirror" bad_bot
SetEnvIfNoCase User-Agent "^WebReaper" bad_bot
SetEnvIfNoCase User-Agent "^WebStripper" bad_bot
SetEnvIfNoCase User-Agent "^WebZIP" bad_bot
SetEnvIfNoCase User-Agent "^e-collector" bad_bot
SetEnvIfNoCase User-Agent "^EmailSiphon" bad_bot
SetEnvIfNoCase User-Agent "^EmailWolf" bad_bot

deny from env=bad_bot
```

Cómo agregar cuentas de usuario [17]

Linux es un sistema operativo con muchas características y una de estas es el estar diseñado para ser utilizado por múltiples usuarios. Aún cuando se tenga una PC con un único usuario, es importante recordar que no es conveniente realizar el trabajo diario desde la cuenta de *root*, misma que sólo debe utilizarse para la administración del sistema.

Una cuenta de *usuario* contiene las restricciones necesarias para impedir que se ejecuten comandos que puedan dañar el sistema *(programas troyanos como el Bliss)*, se alteren accidentalmente la configuración del sistema, los servicios que trabajan en el trasfondo, los permisos y ubicación de los archivos y directorios de sistema, etc.

Procedimientos

Generalmente el paso que procede a una instalación de Linux es la creación de cuentas de usuario. Existen distintos métodos, todos son sencillos y permiten crear una cuenta con su propio directorio de trabajo y los archivos necesarios.

Actualmente existen recursos como el programa instalador de Red Hat Linux® 6.1 y distribuciones basadas sobre esta, programas que funcionan desde un entorno gráfico, como es Linuxconf, y recursos que funcionan en modo de texto o desde una ventana terminal, como son los comandos tradicionales, *useradd* y *passwd*, y algunos otros programas, como YaST y la versión correspondiente de Linuxconf.

Casi al concluir el proceso de instalación de Red Hat Linux 6.1 se proporciona la opción de crear, con opciones predeterminadas, cuentas de usuarios en la misma pantalla en donde se ingresa la contraseña de *root*. El procedimiento solo requiere que se ingresen los nombres de usuarios o *logins* y que se teclee, con

confirmación, la contraseña correspondiente. Opcionalmente se pueden especificar el nombre completo del usuario y directorio de trabajo *(home)*.

En algunos casos, una vez que se accede por primera vez al sistema, será necesario hacer ciertas modificaciones o agregar más cuentas. Definitivamente no es práctico re-utilizar el programa de instalación para tal efecto. Puede hacerse todo lo necesario desde un entorno gráfico con Linuxconf o bien desde el modo de texto o una ventana terminal con los comandos ***useradd*** y ***passwd***.

Creando una cuenta en el modo de texto: *useradd* y *passwd*

Este procedimiento puede realizarse de forma segura tanto fuera de X Window como desde una ventana terminal en el entorno gráfico del que se disponga. Fue el método comúnmente utilizado antes de la aparición de programas como YaST y Linuxconf. Sin embargo aún resulta útil para la administración de servidores, cuando no se tiene instalado X Window, YaST o Linuxconf *(o las versiones de estos que se han instalado no trabajan correctamente)*, o bien se tienen limitaciones o problemas para utilizar un entorno gráfico.

Lo primero: el comando *useradd*

El primer paso para crear una nueva cuenta consiste en utilizar el comando ***useradd*** del siguiente modo:

```
[root@localhost root]$ useradd nombre_del_usuario
```

Ejemplo:

```
[root@localhost root]$ useradd Joel
```

Lo segundo: el comando *passwd*

Después de crear la nueva cuenta con ***useradd*** lo que sigue a continuación es especificar una contraseña para el usuario. Determinar una que le resulte fácil de recordar, que mezcle números, mayúsculas y minúsculas y que, preferentemente, no contenga palabras que se encontrarían fácilmente en el diccionario.

Aunque el sistema siempre tratará de prevenir cuando se escoja una *mala* contraseña, el sistema no impedirá que se haga. Especificar una nueva contraseña para un usuario, o bien cambiar la existente, se puede realizar utilizando el comando ***passwd*** del siguiente modo:

```
[root@localhost root]$ passwd nombre_del_usuario
```

Ejemplo:

```
[root@localhost root]$ passwd Joel
```

El sistema requerirá entonces proceder a teclear la nueva contraseña para el usuario y volver a teclearla para confirmar. No se observará el *echo*, por seguridad, el sistema no mostrará los caracteres tecleados, por lo que se debe hacer con cuidado. Si se considera que tal vez se cometieron errores de tecleado, puede presionarse las veces que sean necesarias la tecla <Backspace> o <Retroceso>. De cualquier forma el sistema le informará si coincide o no lo tecleado. Si todo salió bien se recibirá como respuesta del sistema ***code 0***. Si en cambio recibe ***code 1***, significa que deberá repetir el procedimiento, ya que ocurrió un error.

Este procedimiento también puede utilizarse para cambiar una contraseña existente.

Opciones avanzadas

En muchos casos pueden no ser necesarios, pero si se esta administrando un servidor o estación de trabajo, o bien se es un usuario un poco más experimentado, y se quiere crear una cuenta con mayores o menores restricciones, atributos y/o permisos, pueden utilizarse las siguientes opciones de ***useradd***:

-c comment
: Se utiliza para especificar el archivo de comentario de campo para la nueva cuenta.

-d home dir
: Se utiliza para establecer el directorio de trabajo del usuario. Es conveniente, a fin de tener un sistema bien organizado, que este se localice dentro del directorio ***/home***.

-e expire date
: Se utiliza para establecer la fecha de expiración de una cuenta de usuario. Esta debe ingresarse en el siguiente formato: AAAA-MM-DD.

-g initial group
: Se utiliza para establecer el grupo inicial al que pertenecerá el usuario. De forma predeterminada se establece como único grupo ***1***. Nota: el grupo asignado debe de existir.

-G group,[...]
: Se utiliza para establecer grupos adicionales a los que pertenecerá el usuario. Estos deben separarse utilizando una coma y sin espacios. Esto es muy conveniente cuando se desea que el usuario tenga acceso a determinados recursos del sistema, como acceso a la unidad de disquetes, administración de cuentas PPP y POP. Nota: los grupos asignado deben de existir.

-m
: Se utiliza para especificar que el directorio de trabajo del usuario debe ser creado si acaso este no existiese, y se copiaran dentro de este los archivos especificados en ***/etc/skel***.

-s shell
: Se utiliza para establecer el ***Shell*** que podrá utilizar el usuario. De forma predeterminada, en Red Hat Linux se establece ***bash*** como ***Shell*** predeterminado.

-u uid
: Se utiliza para establecer el UID, es decir, la ID del usuario. Este debe ser único. De forma predeterminada se establece como UID el número mínimo mayor a 99 y mayor que el de otro usuario existente. Cuando se crea una cuenta de usuario por primera vez, como ocurre en Red Hat Linux 6.x, generalmente se asignará ***500*** como UID del usuario. Los UID entre 0 y 99 son reservados para las cuentas de los servicios del sistema.

Ejemplo:

```
[root@localhost root]$ useradd -u 500 -d /home/Joel -G floppy,pppusers,popusers Joel
```

Esto creará una cuenta de usuario llamada ***Joel***, que se encuentra incluida en los grupos **floppy, pppusers *y* popusers**, que tendra un UID=500, utilizará ***Bash*** como shell y tendrá un directorio de trabajo en ***/home/Joel***.

Existen más opciones y comentarios adicionales para el comando ***useradd***, estas se encuentran especificadas en los manuales *(Man pages)*. Para acceder a esta información, utilice el comando ***man useradd*** desde una ventana terminal.

Eliminar una cuenta de usuario

En ocasiones un administrador necesitará eliminar una o más cuentas de usuario. Este es un procedimiento principalmente utilizado en servidores y estaciones de trabajo a los cuales acceden múltiples usuarios. Para tal fin se utilizará el comando **userdel**.

El comando userdel

La sintaxis básica de este comando es la siguiente:

```
[root@localhost root]$ userdel nombre_del_usuario
```

Ejemplo:

```
[root@localhost root]$ userdel Joel
```

Si se desea eliminar también todos los archivos y subdirectorios contenidos dentro del directorio de trabajo del usuario a eliminar, se debe agregar la opción *-r*:

```
[root@localhost root]$ userdel -r nombre_del_usuario
```

Ejemplo:

```
[root@localhost root]$ userdel -r Joel
```

Comentarios finales acerca de la seguridad [15]

Cuando, en la mayoría de los casos, un *hacker* o *cracker* consigue infiltrarse en un sistema Linux o Unix no es porque estos tengan un *hueco de seguridad*, sino porque el *intruso* pudo "*hackear*" alguna de las contraseñas de las cuentas existentes. Si se especificó durante el proceso de instalación de Linux una *mala* contraseña de *root*, algo muy común entre usuarios novatos, es altamente recomendado cambiarla.

- Evitar especificar contraseñas fáciles de adivinar. Esto se refiere particularmente a utilizar contraseñas que utilicen palabras incluidas en cualquier diccionario de cualquier idioma, datos relacionados con el usuario o empresa como son registro federal de causantes (R.F.C.), fechas de nacimiento, números telefónicos, seguro social, números de cuentas de académicos o alumnos y nombres de mascotas, la palabra *Linux*, nombres de personajes de ciencia ficción, etc.
- Evitar escribir las contraseñas sobre medios físicos, memorizarlas.
- Si se necesita almacenar contraseñas en un archivo, se hace utilizando encriptación.
- Si se dificulta memorizar contraseñas complejas, utilizar entonces contraseñas fáciles de recordar, pero cambiarlas periódicamente.
- Jamás proporcionar una contraseña a personas o instituciones que se la soliciten. Evitar proporcionarla en especial a personas que se identifiquen como miembros de algún servicio de soporte o ventas. Este último caso lo menciona con énfasis el *man page* del comando ***passwd***.

Se considera como una *buena* contraseña aquella que se compone de una combinación de números y letras, mayúsculas y minúsculas, y que contiene al menos 8 caracteres. También es posible utilizar pares de palabras con puntuación insertada y frases o secuencias de palabras, o bien acrónimos de estas.

Tomar en cuenta estas recomendaciones, principalmente en sistemas con acceso a redes locales y/o públicas, como Internet, hará que el sistema sea más seguro.

Descripción del procedimiento para crear un disquete de arranque [17]

La disponibilidad de un disquete de arranque puede ser de vital importancia bajo circunstancias de emergencia, como puede ser reparación de daños en el sector de arranque, reinstalar Lilo, probar un nuevo kernel, etc. Dependiendo de la distribución de Linux utilizada, el procedimiento puede resultar muy sencillo o requerir varios pasos. Se recomienda al usuario, sin importar su nivel de destreza, siempre contar con al menos un disquete de arranque guardado en un lugar seguro y listo para su utilización cuando las circunstancias lo ameriten.

Aunque existen herramientas gráficas que se encargan de hacer todo el trabajo por el usuario, es conveniente conocer y dominar los procedimientos básicos, ya que no siempre se contará con entorno gráfico, o bien puede tratarse de una situación de emergencia acompañada de la imposibilidad de acceder a un entrono gráfico, o bien puede tratarse de un servidor con cientos de usuarios conectados en ese momento y que resentirán el súbito consumo de recursos generado por iniciar un entorno gráfico con el único objeto de crear un simple disquete de arranque.

Una herramienta sencilla: mkbootdisk

Mkbootdisk es un script en BASH incluido en distribuciones basadas sobre RedHat, que se encarga de todos los procedimientos necesarios. Su uso es extremadamente sencillo y dará como resultado un disquete de arranque con una copia del kernel utilizado o, a elección, alguno otro instalado en el sistema.

1. Determinar primero que versión de kernel se está utilizando. ejecutar el siguiente comando:

```
rpm -q kernel
```

2. Esto deberá regresar la versión del kernel que se encuentre instalado en el sistema.

```
2.2.16-3
```

3. Insertar un disquete nuevo en la unidad, pero no se debe de montar.
4. Como *root* o superusuario, ejecutar lo siguiente:

```
/sbin/mkbootdisk 2.2.16-3 --device /dev/fd0
```

5. El programa solicitará confirmar el procedimiento que se realizará. Recuerdar que la información existente en el disquete será eliminada.
6. La creación de un disquete de arranque ha finalizado, se procede ahora a probarlo reiniciando el sistema con éste.

Procedimiento largo

Antes de la aparición de mkbootdisk, el siguiente era el procedimiento de rutina para la creación de un disquete de arranque.

1. Se accede a una consola o terminal como *root* o superusuario
2. Se inserta un disquete nuevo y se le da formato:

```
/sbin/mke2fs /dev/fd0
```

3. Se monta el disquete

```
mount /dev/fd0 /mnt/floppy/
```

4. Se copia el kernel a el disquete

```
cp /boot/boot.b /mnt/floppy/
cp /boot/vmlinuz /mnt/floppy/
```

5. Se instala Lilo en el sector de arranque del disquete, especificando el kernel que se acaba de copiar.

```
echo image=/mnt/floppy/vmlinuz label=linux | /sbin/lilo -C - -b /dev/fd0 -i
/mnt/floppy/boot.b -c -m /mnt/floppy/map
```

6. Se desmonta el disquete

```
umount /mnt/floppy/
```

7. La creación de un disquete de arranque ha finalizado, se procede ahora a probarlo reiniciando el sistema con éste.

GUÍA DE REFERENCIA RÁPIDA DE ADMINISTRACIÓN LINUX [18]

Se recomienda practicar un poco en alguna computadora que no sea crítica, de manera que los daños colaterales se minimicen.

Esta guía esta basada en distribuciones de **Red Hat** (http://www.redhat.com) 6.2, 7.0, 7.1 y 7.2, por lo que en versiones posteriores u otras distribuciones de Linux (Debian, Mandrake, SuSe) la ubicación de los paquetes puede variar.

También se debe recordar que, a diferencia de Windows, todas las instrucciones, nombres de archivos y demás son sensibles a mayúsculas y minúsculas.

1. Cómo iniciar una sesión remota

Para esto se necesita tener un cliente de SSH (*Secure Shell*), que encripta los datos que se transmiten durante la sesión. Una vez que se activa el cliente se solicita la dirección IP o nombre de dominio de la máquina destino en este son:

- www.semarnat.gob.mx (200.15.115.96)
- intranet.semarnat.gob.mx (200.15.115.157)

Nota importante: Si se utilizan los nombres de dominio no se coloca el prefijo "http://". Igualmente no se deben colocar subcarpetas (www.semarnat.gob.mx/directorio) para buscar se debe estar conectado al servidor.

Una vez iniciada la conexión se solicita el usuario y password respectivo. Hay que recordar que ambos son sensibles a mayúsculas y minúsculas, por lo que no es igual escribir "Pagina", "PAGINA" o "pagina".

Acto seguido aparece una ventana donde se observa:

```
[usuario@servidor carpeta]$
```

A partir de este momento ya se puede comenzar a trabajar directamente en el servidor.

Descripción del prompt

Cuando se inicia la sesión, se presenta una pantalla con un prompt como el siguiente:

```
[usuario@servidor carpeta]$
```

Este se divide en cuatro elementos principales; el primero es el **usuario** con que se inicia la sesión, luego viene una **arroba (@)** que indica la pertenencia y luego el servidor donde se está trabajando, para terminar con la **carpeta** donde se encuentra.

Recordar que en caso de duda sobre un comando específico, pueden utilizar la sintaxis:

```
[usuario@servidor carpeta]$ comando --help
```

En algunos casos es:

```
[usuario@servidor carpeta]$ comando -h
```

Lo que desplegará una pantalla con las opciones. Otro sistema de ayuda es "man":

```
[usuario@servidor carpeta]$ man comando
```

Esto puede darse en caso que no exista un archivo de "help" para un comando específico.

2. Cómo cambiar de cualquier usuario a root

Para la mayor parte de las funciones de administración de un servidor es necesario cambiar al super usuario, por lo que se debe seguir el siguiente procedimiento:

```
[usuario@servidor carpeta]$ su -l
Password:
```

Cuando se pulsa enter después de solicitar el superusuario (su) se pide teclear el password, y al dar enter cambia el shell:

Nota: por seguridad, la contraseña no se despliega en pantalla, ni siquiera como asteriscos; en caso de error se debe dar enter y repetir el procedimiento, no acepta eliminación de caracteres.

```
[root@servidor root]$
```

A partir de este momento ya se puede realizar cualquier actividad en el servidor, ya que este usuario es el propietario del sistema.

Para terminar la sesión como root

```
[root@servidor carpeta]$ exit
```

3. Cómo cambiar de carpeta y verificar la ubicación

Para navegar en un servidor UNIX, se utiliza el comando "cd" (change directory) de la siguiente forma:

```
[root@servidor carpeta]$ cd /ruta/a/la/carpeta1
```

Para subir un nivel:

```
[root@servidor carpeta]$ cd ..
```

Para bajar un nivel:

```
[root@servidor carpeta]$ cd carpeta2
```

Una forma *incorrecta* de utilizarlo es "cd.." o "cd/carpeta", similar a como se utiliza en MSDOS.

Para verificar la ubicación, se usa:

```
[root@servidor carpeta]$ pwd
[root@servidor carpeta]$ /carpeta1/carpeta2
```

4. Cómo manipular archivos y carpetas

Una función muy útil para recuperar archivos o carpetas mediante una conexión SSH directamente del servidor, sin requerir de un cliente de FTP, es:

```
[usuario@máquinalocal carpeta]$ scp usuario@midominio.com:/ruta/a/la/carpeta/archivo.ext ./

usuario@midominio.com's password:
archivo.ext          100% |*****************************|   103        00:00
```

Esto se realiza antes de iniciar una conexión remota, es decir, sin que se haya conectado previamente al servidor. Lo que se le está haciendo es solicitar mediante el equipo local que se inicie una conexión y que se descargue ciertos archivos. Esta opción no está disponible para los clientes de SSH en Windows.

Para copiar un archivo:

```
[root@servidor carpeta]$ cp archivo1 archivo2
```

Para copiar un archivo a otra carpeta:

```
[root@servidor carpeta]$ cp archivo1 /ruta/a/la/carpeta/
```

Para renombrar un archivo:

```
[root@servidor carpeta]$ mv archivo1 archivo2
```

Para mover un archivo a otra carpeta:

```
[root@servidor carpeta]$ mv archivo1 /ruta/a/la/carpeta/
```

Para eliminar un archivo:

```
[root@servidor carpeta]$ rm archivo1
```

Para crear un directorio:

```
[root@servidor carpeta]$ mkdir carpeta
```

Para cambiar de nombre un directorio:

```
[root@servidor carpeta]$ mv carpeta1 carpeta2
```

Para mover un directorio:

```
[root@servidor carpeta]$ mv carpeta1 /ruta/a/la/carpeta2
```

Para listar el contenido de un directorio:

```
[root@servidor carpeta]$ ls
```

Para eliminar todo el contenido de una carpeta (muy peligroso)

```
[root@servidor carpeta]$ rm * -F -R
```

La opción "-F" es importante porque si no se pone, se preguntará por cada archivo si se desea eliminarlo. La opción "-R" es para obligar a el comando que lo haga en todos los archivos que encuentre.

Para eliminar una carpeta (debe estar vacia previamente):

```
[root@servidor carpeta]$ rmdir carpeta
```

Para eliminar una carpeta y su contenido sin necesidad de muchos pasos (aún más peligroso):

```
[root@servidor carpeta]$ rm -rf directorio/
```

Un comentario relevante es que cuando se crean archivos o carpetas, estas se crean con el usuario y grupo de quien lo crea, por lo que si es root y se crea un archivo, el propietario (y único que lo puede editar o borrar) es root. Para esto se recomienda revisar el apartado para actualizar los permisos de archivos y carpetas.

5. Cómo verificar y cambiar el propietario de un archivo o carpeta

Por diversas circunstancias es posible que un archivo o carpeta que se encuentre en una carpeta de un usuario no le pertenezca, esto en general es raro y no afecta la operación de la página, pero impide que el propietario de la cuenta lo modifique o elimine, para verificar esto se hace lo siguiente:

```
[root@servidor carpeta]$ ls -l

-rwxr-xr-x    1 usuario      web         12784 jul 17  2000 mod_perl_cgi.html
-rwxr-xr-x    1 usuario      web         21713 jul 17  2000 mod_perl_faq.html
```

Donde "usuario" es el propietario del archivo y "web" es el grupo al que pertenece el usuario.

Para cambiar el propietario de un archivo

```
[root@servidor carpeta]$ chown user archivo.ext
```

Para cambiar el propietario de una carpeta

```
[root@servidor carpeta]$ chown user carpeta
```

Para cambiar el propietario de varios archivos en una misma carpeta

```
[root@servidor carpeta]$ cd carpeta
[root@servidor carpeta]$ chown user *.ext
```

Para cambiar el propietario de todos los archivos en una misma carpeta

```
[root@servidor carpeta]$ cd carpeta
[root@servidor carpeta]$ chown user *
```

Para cambiar el propietario de todos los archivos en diferentes carpetas

```
[root@servidor carpeta]$ cd carpeta-principal
[root@servidor carpeta]$ chown user * -R
```

Para cambiar el propietario y grupo de todos los archivos en diferentes carpetas

```
[root@servidor carpeta]$ chown user:grupo carpeta -R
```

La opción "-R" es para darle recursividad y lo haga en todos los archivos que encuentre.

Para cambiar el grupo de un archivo

```
[root@servidor carpeta]$ chgrp grupo archivo
```

Para cambiar el grupo de una carpeta

```
[root@servidor carpeta]$ chgrp grupo carpeta -R
```

6. Cómo verificar y cambiar los persmisos de carpetas y archivos

En ocasiones, es posible que vía FTP no se coloquen los archivos con los permisos adecuados para poderse ejecutar por Internet, muy común cuando se suben scripts CGI. Para verificar los permisos se hace lo siguiente:

```
[root@servidor carpeta]$ ls -l

drwxrwxr-x    6 crowley  501          4096 oct 30 22:20 cursos
-rw-r--r--    1 crowley  501          4083 sep 21  2000 formulario.html
-rwxrwxr-x    1 crowley  root        14779 jul  3 18:42 kernel-config.txt
-rw-r--r--    1 crowley  root        14002 jul  9 04:38 new-kernelconf.txt
-rw-rw-r--    1 crowley  501         19456 jul  3 18:28 nombre-alt.sdc
-rw-rw-r--    1 crowley  501          1333 jul  4 13:39 nota.html
-rw-rw-r--    1 crowley  501         16896 may 11  2001 notas-instal-linux.sdw
-rw-r--r--    1 crowley  501           489 sep 21  2000 pesos.html
-rw-rw----    1 crowley  501         14336 ene  9  2001 programa-2001-4.xls
```

La primera serie de caracteres que se observan son los privilegios de cada archivo, igualmente si es un directorio (con una "d" al inicio). Los achivos que se deben ver/ejecutar en Internet deben tener una serie de permisos como la siguiente:

```
-rwxr-xr-x    1 root     root        12784 jul 17  2000 mod_perl_cgi.html
-rwxr-xr-x    1 root     root        21713 jul 17  2000 mod_perl_faq.html
```

Es decir, de lectura (r) y ejecución (x) para todos los usuarios. Los permisos de escritura (w) sólo le pertenen al propietario.

Para cambiar los permisos de un archivo

```
[root@servidor carpeta]$ chmod 755 archivo.ext
```

Para cambiar los permisos de varios archivos de una misma carpeta

```
[root@servidor carpeta]$ chmod 755 *.ext
```

Para cambiar los permisos de todos los archivos de una misma carpeta

```
[root@servidor carpeta]$ chmod 755 *
```

Para cambiar los permisos de todos los archivos de varias carpetas

```
[root@servidor carpeta]$ chmod 755 * -R
```

7. Cómo verificar el espacio opcupado por una carpeta y subcarpetas

Para ver el espacio ocupado por una carpeta y sus subcarpetas en MB

```
[root@servidor carpeta]$ du -h /ruta/a/la/carpeta
```

Para ver el espacio total ocupado por una carpeta en MB

```
[root@servidor carpeta]$ du -sh /ruta/a/la/carpeta
```

8. Cómo verificar y cambiar la cuota de un usuario

Para ver la cuota (si está activa) de un usuario

```
[root@servidor carpeta]$ quota usuario1

Disk quotas for user usuario1 (uid 571):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
      /dev/hda5   12664   15000   20000             284       0       0
```

Esto despliega en KB la cuota del usuario, su límite y otros detalles relacionados. En caso de que un usuario haya sobrepasado su cuota, el número de bloques se despliega con un asterisco:

```
Disk quotas for user usuario2 (uid 512):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
      /dev/hda5   43764*  15000   20000    none    1304       0       0
```

Para incrementar la cuota de un usuario

```
[root@servidor carpeta]$ edquota usuario1
```

Esto presenta una nueva pantalla, en la que se ejecuta un editor llamado "vi", el cual es muy poderoso pero necesita ser manejado con cuidado:

```
Quotas for user usuario1:
/dev/hda5: blocks in use: 43764, limits (soft = 15000, hard = 20000)
        inodes in use: 1304, limits (soft = 0, hard = 0)
```

Para ser editado se debe seguir rigurosamente este procedimiento:

1. Pulsar la tecla "Insert" (insertar) en el teclado a mano derecha. En ocasiones es necesario utilizar la tecla "i" para iniciar el modo de edición.
2. Colocar con las flechas de navegación (no con el ratón) el cursor en los números de "soft = **15000**, hard = **20000**", que se aprecian en negritas.
3. Borrar con la tecla de "backspace" la cantidad a modificar.
4. Teclear el nuevo límite pero no con el teclado numérico (a mano derecha), sino con los números arriba de las letras.
5. Pulsar la tecla "Esc" (escape) para terminar el modo de edición.
6. Pulsar ":w" para salvar y luego ":q" para salir. Una abreviatura sería ":wq".

En caso de error, es más seguro quitar el modo de edición (Esc) y salir sin salvar con ":q!" (con signo de admiración) y repetir el procedimiento.

9. Cómo asignar o cambiar el password de un usuario

```
[root@servidor carpeta]$ passwd usuario
Changing password for user usuario
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

Por seguridad el password no se despliega en el monitor y se solicita que se teclee dos veces para corroborarlo. Las contraseñas residen físicamente en el disco duro de la máquina pero están encriptadas, por lo que no es posible leerlas, así que si un usuario pierde la suya, es más sencillo cambiarla que recobrarla.

10. Cómo crear usuarios y grupos de usuarios

Para crear un usuario sin un grupo específico:

```
[root@servidor carpeta]$ useradd usuario
```

También existe en algunas distribuciones de Linux la opción "adduser", que funciona exactamente igual.

Para crear un usuario con un grupo específico:

```
[root@servidor carpeta]$ useradd -g grupo usuario
```

En el caso de creación de usuarios, primero se debe colocar las propiedades y al final el nombre del usuario.

Para crear un grupo:

```
[root@servidor carpeta]$ groupadd grupo
```

Recordar asignar un password a los usuarios una vez que se hayan creado con el comando que se vió anteriormente.

11. Cómo reiniciar los servicios

Los principales servicios que se deben levantar son los relativos a la red, web, conectividad a Windows y FTP, para lo cual se ejecutan los siguientes comandos:

Para el servidor de red (network)

```
[root@servidor carpeta]$ /etc/rc.d/init.d/network restart

Shutting down interface eth0:                              [  OK  ]
Disabling IPv4 packet forwarding:                          [  OK  ]
Setting network parameters:                                [  OK  ]
Bringing up interface lo:                                  [  OK  ]
Bringing up interface eth0:                                [  OK  ]
```

Para los servicios de Web (apache)

```
[root@servidor carpeta]$ /etc/rc.d/init.d/httpd restart

Shutting down http:                                        [  OK  ]
Starting httpd:                                            [  OK  ]
```

En ocasiones, cuando se actualizan los paquetes manualmente, la ruta es diferente:

```
[root@servidor carpeta]$ /usr/local/httpd/bin/apachectl restart

Shutting down http:                                        [  OK  ]
Starting httpd:                                            [  OK  ]
```

Para el servidor conexión Windows (samba)

```
[root@servidor carpeta]$ /etc/rc.d/init.d/smb restart

Shutting down SMB services:                                [FAILED]
Shutting down NMB services:                                [FAILED]
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
```

Para el servidor de FTP (WS-FTP)

```
[root@servidor carpeta]$ /etc/rc.d/init.d/xinetd restart

Stopping xinetd:                                           [FAILED]
Starting xinetd:                                           [  OK  ]
```

Dos puntos importantes. Por un lado, es factible que un servicio marque error al momento de que se quiera detenerlo, ya que desde un principio no estaba activo, lo importante es que cuando se levante marque OK. En segundo término, otras opciones de estos comandos son "start" (iniciar), "stop" (detener) y "status".

12. Cómo reiniciar la máquina

Para reiniciar la computadora

```
[root@servidor carpeta]$ reboot
```

Para apagar la computadora

```
[root@servidor carpeta]$ shutdown now
```

Capítulo IV

SERVICIOS DE INFORMACIÓN QUÍMICA

Capítulo IV: Servicios de Información Química.

La aplicación práctica del objetivo principal de este trabajo, puede ejemplificarse con la organización y puesta en marcha de la COSID (Coordinación de Servicios de Información Digital), la cual proporciona servicios de información competitivos a nivel nacional e internacional que apoyan los programas académicos y de investigación, y promueven los valores y habilidades de los estudiantes y profesionales, definidas en la misión de la UNAM.
Los servicios proporcionados por esta coordinación se dividen en dos grupos: los servicios de información química a distancia y los servicios presenciales.

I.- Servicios de información química a distancia.

Como se mencionó en el tercer capítulo de este trabajo, la instalación de un servidor Linux para complementar dichos servicios de la sala de cómputo, en este caso se creo un servidor Linux llamado cosid.pquim.unam.mx, el cual alberga y permite servicios asociados con los objetivos principales de dicha sala.
Dentro del servidor COSID se pueden encontrar los siguientes servicios de información química:

1.- Servicios a través de la página Web de COSID.
2.- Cuentas de correo electrónico.
3.- Foros de discusión.
4.- Servidor FTP.
5.- Lugar para páginas de profesores.
6.- Creación de una *Knoledge Base* (base de datos de conocimientos comunes) referente a información química.

1.- Servicios a través de la página Web de COSID. Dicho portal corresponde a la Coordinación de Servicios de Información Digital de la facultad de química, es un escaparate donde se pueden encontrar los programas académicos sobre información química, dentro de los que se pueden mencionar los cursos extra curriculares que se imparten dentro de la coordinación. Otro ejemplo lo constituye el material didáctico disponible para ser recuperado por los estudiantes y profesores correspondientes a las asignaturas que se imparten dentro de la institución.
Otro servicio es proporcionar acceso a las bases de datos del sistema de biblioteca UNAM que son alrededor de 100 bases de datos de interés académico dentro de la institución, los cuales pueden ser consultados dentro de la red-UNAM.
En cuanto a las revistas en formato digital, se cuenta con un gran número de ellas para recuperar información en texto completo tanto en formato HTML como en formato PDF (*Portable Document Format*)

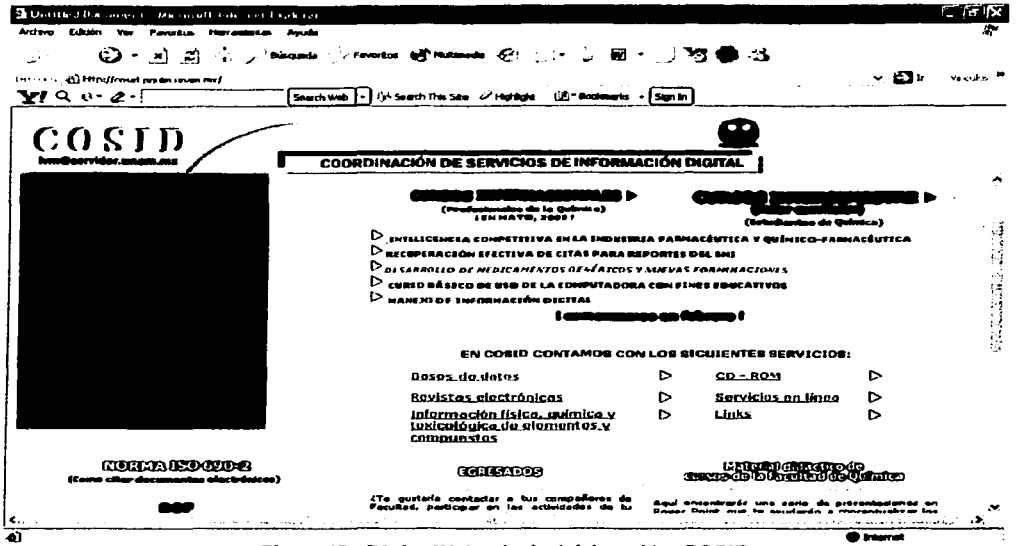

Figura 47.- Página Web principal del servidor COSID

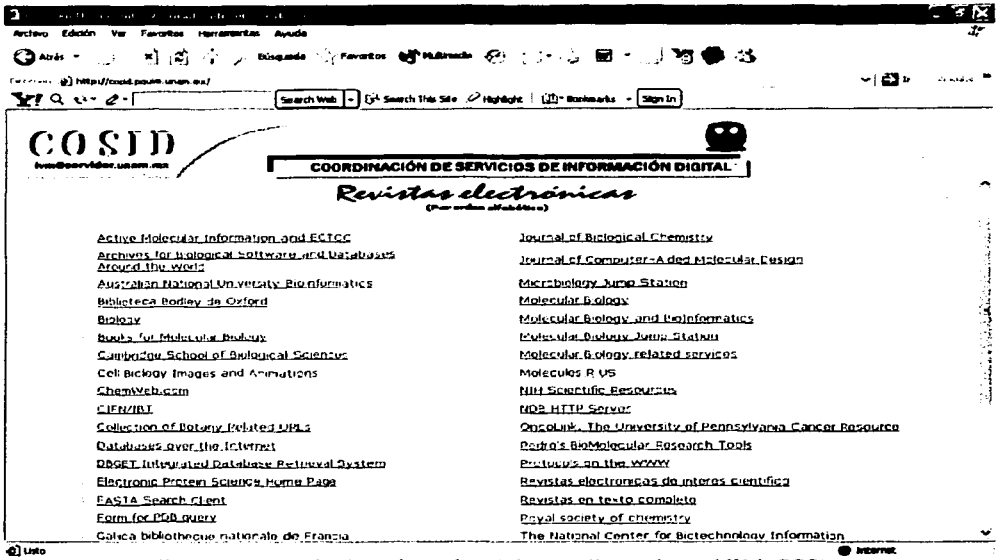

Figura 48.- Consulta de revistas electrónicas mediante el portal Web COSID.

2.- Cuentas de correo electrónico. Dicho servidor Linux, dentro del mismo sistema tiene incorporada la capacidad de prestar este servicio a los usuarios que estén dados de alta en el mismo. Permitiendo la comunicación remota tanto de profesores, alumnos y personal de la COSID, no importando en donde se encuentren físicamente. Tampoco es necesario que las partes a comunicarse se encuentren conectadas al servidor al mismo tiempo, permitiendo con esto una comunicación sin límites de tiempo y ubicación.

3.- Foros de discusión. Así como los correos electrónicos permiten la comunicación entre dos partes, los foros de discusión o listas de correo, lo hacen para muchos usuarios. Esto lo logran mediante la creación de una dirección virtual de correo, la cual se encarga de distribuir un mensaje dirigido a ella, a todas las direcciones inscritas al foro de discusión. Esto es, un usuario manda un mensaje abierto con alguna pregunta o comentario acerca de algún tema en específico (referente al nombre del foro de discusión en cuestión) y esta cuenta virtual se encarga de distribuir dicho mensaje a todos los usuarios en el foro. De la misma manera la persona que responda al mensaje seguirá la misma mecánica y así todos los miembros del foro estarán enterados de la discusión originada por el primer mensaje enviado. Cabe recordar que los mensajes manejados dentro del foro se verán similares a cualquier correo electrónico común.

4.-Servidor FTP. Este servicio aplica para todos los usuarios de COSID, tanto alumnos y profesores principalmente, como ya se analizó, dicho servicio permite transferir archivos desde cualquier computadora remota hacia el servidor y viceversa, permitiendo por ejemplo que los alumnos transfieran a algún directorio personal de un profesor, los trabajos, tareas y exámenes; dejándolos listos para que el profesor responsable de calificarlos pueda tener libre acceso a ellos y hacer su trabajo.

5.- Lugar para páginas de profesores. De la misma manera que en el punto anterior, este servicio permite mantener en contacto a toda una clase, es decir, mediante la creación de páginas de profesores ordenados por materias impartidas, los alumnos pueden consultar la bibliografía del curso, fechas de evaluaciones, así como también dicho profesor puede proporcionar las tareas y exámenes a sus alumnos por medio de dicha página.

6.- Creación de una *Knoledge Base* (base de datos de conocimientos comunes) referente a información química. Siguiendo la referencia de puntos anteriores, teniendo todos los servicios mencionados funcionando se pueden concentrar los conocimientos que vayan surgiendo gracias a ellos, dentro de una base de datos de conocimiento general (*Knowledge Base*), la cual permitirá que usuarios posteriores tengan acceso a los resultados de discusiones, exámenes, y conocimiento en general que sean resultado de dichos servicios. Dicha base de conocimientos se puede manejar desde un formato simple como texto, pasando por el hipertexto (páginas Web) o si se desea se pueden programar en alguna página Web dinámica en la cual los propios usuarios sean los que la vayan enriqueciendo.

II.- Servicios presenciales.

Los servicios presenciales pueden ser los siguientes:
1.-Localización de información en discos compactos, los cuales son los siguientes:

- **Food Science and Technology Abstracts**
  Información sobre alimentos (1969 - 1995)
- **International Pharmaceutical Abstracts**
  Información del área farmacéutica (1967 a 1995)
- **Merck Index**
  Información de sustancias. Se puede buscar dibujando la estructura, por fórmula mínima, por número CAS, nombre, etc. (Edición veinte)
- **Derwent Biotechnology Abstracts**
  Resúmenes de Patentes publicadas por el sistema Derwent (1982 a 1994)
- **Poltox I**
  Información sobre Contaminación y Toxicología (incluye los efectos sobre plantas, animales y humanos)
- **Farmacopea Martindale**
  Contiene Datos de sustancias
- **Biological Concepts**
  Contiene conceptos de Biología con notas, ilustraciones y animaciones
- **Biology Art**
  Contiene 635 imágenes de conceptos de Biología y sus aplicaciones, compilados de Starrs Biology
- **Life Science Collection**
  Cubre temas de Biología, Medicina y Agricultura. Contiene la información de revistas, libros y conferencias publicados en 21 revistas CAS abstracts
- **Pest-Bank-Pecticide Product Data**
  Producido por Purdue Reserch Fundation. Pest-Bank está basado en la National Information Pesticide Retrieval System (NIPRS), una base de datos que se encuentra en línea, que está soportada en la Purdue Research Fundation, de la Universidad de Purdue en Indiana.
- **Experta Médica CD: Drugs & Pharmacology**
  Contiene once bases de datos especializadas. Incluye abstracs y citas concernientes a Fármacos, Farmacología y Biofarmacia

2.-Servicio de revista digital. Donde se localizan y recuperan artículos de revistas en texto completo contratadas y disponibles dentro de la red-UNAM
3.-Servicio documental, donde se localizan y recuperan documentos de revistas localizadas en cualquier biblioteca del mundo, las cuales son recibidas por correo electrónico o servicio de fax
4.- Servicio de localización y recuperación de información en línea directa desde computadoras remotas, con servicios de sistemas de bases de datos que se cobran por tiempo de uso con una clave especial para ingresar a ellos.

Análisis y discusión

Con la realización de este trabajo, se intenta colaborar con el funcionamiento de un centro de cómputo de información científica digital, para ello se presentan una serie de instrucciones, para instalar una sala de cómputo con el fin de acceder a información que se requiera, en este caso servicios de información química, dichas instrucciones son solo formas básicas y resumidas para lograr los objetivos principales citados para este trabajo, en la práctica se notará que se requieren conocimientos aún más específicos como lo es por ejemplo la instalación del servidor Linux, mencionado en el capítulo 3, el cual para su completa instalación se deben leer con mucho cuidado las instrucciones brindadas por el mismo programa de instalación, ya que cabe recordar que el instalador de Linux es una plataforma muy amigable hacia el usuario principiante e intermedio, porque cuenta con breves explicaciones y ayuda a lo largo de la misma, sin embargo aun en el caso de que dichas explicaciones no sean suficientes y no se sepa acerca de lo que se está instalando o configurando en ese momento, el programa instalador cuenta con opciones predeterminadas que harán que el sistema trabaje adecuadamente, permitiendo una configuración posterior personalizada.
Por el lado de Windows este no cuenta con dichas configuraciones predeterminadas, pero aun así, esto no lo convierte en un entorno áspero para el usuario principiante / intermedio, ya que también cuenta con ayuda en cada punto de su configuración.

En el primer capítulo, al repasar las definiciones y estructuras de los mecanismos en los cuales se basan las diferentes topologías de redes, se puede comprender mejor la lógica de la tecnología empleada en la creación de una "red" de computadoras, al recordar que sólo se requieren tener dos computadoras conectadas entre si para tener una red de área local, es decir, es la misma lógica básica para casi cualquier número de máquinas interconectadas.
Dentro del mismo capítulo se puede notar que gracias a las normatividades internacionales basadas en el modelo OSI (IEEE 802.x), y a la rápida evolución tecnológica, existe una tendencia a una estandarización de manejo los sistemas de redes de computadoras.

El segundo capítulo enseña paso a paso como hacer que se comuniquen dos o más máquinas bajo el entorno Windows 9x, como se mencionó con anterioridad estos pasos se manejan de manera resumida, asumiendo que el usuario encargado de configurar dichas funciones, tiene conocimientos previos y está familiarizado con dicho sistema operativo, aquí también sobresale el hecho de que algo como compartir una impresora de modo que usuarios remotos (físicamente) a una impresora, puedan hacer uso de ella; cosa que aparentemente suena un tanto complicada, este capítulo permite realizarlo sin muchas dificultades.

Con el tercer capítulo se cuenta con lo que se puede llamar las instrucciones mínimas para la instalación de un servidor Linux, ya que dicha tecnología permite tener un servidor muy sencillo encargado solo de un par de funciones o su vez con un complicado servidor que lleva a cabo muchas tareas, todo es cuestión de internarse de manera más profunda en la documentación que existe de dicha tecnología.
Cabe mencionar que Linux es un sistema operativo abierto, es decir su código de programación lo puede conocer cualquier persona, debido a lo mismo, cualquier persona puede hacer sus propias mejoras o innovaciones al sistema, por lo que a esta tecnología se refiere, es casi imperativo que el administrador se ocupe de mantener actualizado el sistema con las nuevas versiones que se publiquen en la red, así para evitar posibles causas de inestabilidad del servidor o intrusiones maliciosas de personas con altos conocimientos que se aprovechan de las "fallas" de los programas en sus versiones recientes.

En una parte del cuarto capítulo se puede notar la importancia de contar con una sala de servicios de información dentro del área práctica, ya sea para fines educativos o en la iniciativa privada, ya que como se mencionó es casi obvia la necesidad de la información de las nuevas técnicas, metodologías, avances científicos, etc., que se van generando día con día; debido a lo dinámico que resulta ser el avance tecnológico y que la información permita el desarrollo de tecnologías de vanguardia.
Por lo anterior se propone un trabajo de revisión de la tecnología mencionada en este proyecto, para así mantener vigente la información proporcionada por el mismo.

Conclusiones

Los sistemas de información digital representan una gran ventaja sobre los sistemas tradicionales, debido que son mucho más versátiles, ya que la información de esta naturaleza es muy dinámica, es decir, se actualiza constantemente. Por lo tanto, dichos sistemas, proporcionan una completa solución a las necesidades de información del Ingeniero Químico, dentro de su área de desarrollo y aplicación.

Al contar con una sala de cómputo con las características mencionadas en el presente trabajo, se cuenta con un acceso práctico y confiable al Internet; debido a la naturaleza global del mismo, por consiguiente se cuenta con muchas fuentes de información paralelas a lo largo del planeta, esto da como resultado una recuperación de información de alta calidad en cuanto a contenido y aplicación práctica, ya que se puede comparar, corroborar y enriquecer dicha información mediante el acceso a los diferentes sistemas de información consultados tanto en línea como en Internet a través de la sala de servicios de información química.

Ahora también al tener el servicio extra que brinda la instalación del servidor Linux para complementar la dicha sala de cómputo, la información recuperada mediante el mismo, obtiene un valor mayor al ser administrada y compartida mediante el servidor Linux, por ejemplo dicha información no se pierde momentos después de ser consultada, sino que por el contrario puede ser enriquecida a un grado mayor, por diferentes usuarios de la sala, un caso práctico sería que un usuario siembra la semilla en el servidor compartiendo lo que encontró de dicho tema, esto lo puede hacer mediante la creación de un sitio web o un foro de discusión dentro del mismo, posteriormente usuarios que tienen necesidades de información similares pueden consultar dicha semilla de información dejada por el primer usuario y así tener una información base la cual se va enriqueciendo conforme mas usuarios realizan cada uno por su cuenta recuperación de información de temas similares, compartiendo a su vez su logro particular.

También se observa que conforme avanza la tecnología, las formas de acceder, por ejemplo, a bases de datos en línea, es cada vez mas sencilla, es decir, las interfases con el usuario se programan de manera mas simple y los pasos para obtener una buena recuperación de información se van reduciendo de modo que los requisitos de conocimiento preliminares sobre dicha interfase son fácilmente cubiertos por casi cualquier persona.

En este "instructivo" se plantean los pasos para diseñar y configurar una sala de información química, pero como se observa se maneja de un modo un genérico, ya que esta puede adoptar múltiples formas y objetivos, contando con una herramienta que no solo sirve para la aplicación dentro de la rama de la química; su aplicación abarca cualquier rama con necesidades de información.

Retomando los alcances de este trabajo para el área de la información química, dicha sala en su aplicación y funcionamiento real y práctico le otorga al egresado de la facultad de química un *VALOR AGREGADO*, ya que al contar con los conocimientos que le da la experiencia a través de el manejo de dicha sala para buscar y recuperar información, éste al salir al ámbito laboral se cuenta con mayores habilidades para su desempeño y desarrollo dentro de alguna institución de la iniciativa privada.

Ahora, por todo lo mostrado anteriormente, este trabajo representa un "instructivo" de una línea de partida base, para volver realidad una poderosa herramienta para el acceso a los sistemas de información química, desde cualquier lugar donde se genere la misma.

Bibliografía

1. Andrew S. Tanenbaum, "Redes de Computadoras", Prentice Hall, 3ª. Edición, 1997.
2. James Mohr, "Linux: Recursos para el usuario". Prentice Hall, México, 1998.
3. Tomas W. Madron, "Redes de Área Local", Editorial Limusa.2da. Edición.
4. Beltrao Moura José A. , "Redes Locales de Computadoras", Editorial McGraw-Hill.
5. Douglas E. Comer, "Internetworking with TCP/IP" Prentice Hall, 2da Edición, 1991.
6. G. Held, "Ethernet Networks", Willey Profesional Computing, 1994.
7. Dr. Sidnie Feit, "Arquitectura de TCP/IP, Protocolos, Implementación y Seguridad", McGraw-Hill, 1998.
8. Douglas E. Comer, "TCP/IP", Prentice Hall, 1995.
9. Cornelio Robledo, "Redes de Computadoras" , México, Edición de Autor, 1998.
10. Stallings, W., "Comunicaciones y redes de computadores", Quinta Edición, Prentice Hall, 1997.
11. Halsall, F., "Comunicaciones de datos redes de computadores y sistemas abiertos, Cuarta edición", Addison-Wesley, 1998.
12. Informática – Centro: http://www.naveviva.com/informatica/informatica-centro.htm (Noviembre 2002)
13. RedIris, SEGURIDAD EN UNIX Y REDES: http://www.rediris.es/cert/doc/unixsec/ (Noviembre 2002)
14. Itrain online, Redes de Computadoras y Seguridad en Internet: http://www.itrainonline.org/itrainonline/spanish/networking.shtml (Noviembre 2002)
15. Red Hat Linux 7.1, Official Red Hat Linux Reference Guide, Elementos básicos de seguridad de Red Hat: http://redhat.ip.pt/ftp.redhat.com/linux/7.1/emea/doc/RH-DOCS/es/rhl-rg-es-7.1/ch-security.html (Noviembre 2002)
16. Red Iris, Seguridad, Introducción y conceptos previos: http://www.rediris.es/cert/doc/unixsec/node5.html (Noviembre 2002)
17. México Extremo, Los COMOS de Linux: http://www.mexicoextremo.com.mx/ayuda/comos-linux.php3 (Noviembre 2002)
18. Linux para todos, Redes y servidores, Administración y configuración del sistema: http://www.linuxparatodos.com/ (Noviembre 2002)
19. Monografías, Redes: http://www.monografias.com/trabajos6/redex/redex.shtml (Noviembre 2002)
20. Monografías, Redes bajo Linux: http://www.monografias.com/trabajos/redeslinux/redeslinux.shtml (Noviembre 2002)
21. e-learning, http://www.e-learning.com (Noviembre 2002)
22. Monografías, Redes Inalámbricas: http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml (Noviembre 2002)

23. Glosario de Términos informáticos: http://sapiens.ya.com/herminiapaissan/diccio/ (Noviembre 2002)
24. Glosario de Internet: http://www.podernet.com.mx/2000/glosario/index3.html (Noviembre 2002)
25. Elisoft, Glosario: http://www2.elisoft.net/glosario/index.htm (Noviembre 2002)

APÉNDICE

10 Base T: Las especificaciones para una conexión *Ethernet* 10 Mb/s están definidas por el comité IEEE 802.3 que utiliza cable doblado categoría 3, 4 o 5 CSMA/CD y es usado acceder a la topología lineal. El segmento máximo son de 100 metros y se instala en topología de estrella hacia la central.

A

Acceso Dedicado: Forma de acceso a Internet en la cual la computadora está permanentemente conectada a una red. Por lo general, el acceso dedicado es utilizado por las compañías que venden servicios de acceso a la Internet a los usuarios. Las grandes empresas también están conectando sus redes internas de forma dedicada a Internet. De cualquier manera, todos los servidores de la red, como *Web sites* y servidores de FTP, mantienen una conexión permanente a la red para que los usuarios puedan acceder a ellos en todo momento. En este tipo de conexión, la computadora utiliza una dirección única (IP *address*) para ser localizada en Internet.

ADC: *Analog-Digital Coverter* (Convertidor de análogo a digital). Aparato que mayormente convierte señales análogas a señales digitales.

adjunto: Es un documento que se envía "adjunto" a un mensaje de correo electrónico. Algunos programas de correo electrónico, como Eudora por ejemplo, permiten enviar cualquier tipo de documento (texto o imágenes) junto con un mensaje. Al llegar a su destino, el documento asociado puede ser extraído del mensaje.

ADSL: (1) Es una técnica de modulación para la transmisión de datos a gran velocidad sobre el par de cobre. La primera diferencia entre esta técnica de modulación y las usadas por los módems en banda vocal (V.32 a V.90) es que éstos últimos sólo transmiten en la banda de frecuencias usada en telefonía (300 Hz a 3.400 Hz), mientras que los módems ADSL operan en un margen de frecuencias mucho más amplio que va desde los 24 Khz. hasta los 1.104 KHz, aproximadamente.

(2) Son las siglas de *Asymetric Digital Suscriber Line*, esto es, "Línea de Usuario Digital Asimétrica", una tecnología que consigue transformar el par de cobre que todos tenemos en casa en líneas de alta velocidad, sin necesidad de cambiar la instalación, con sólo colocar un módem especial en cada extremo de la línea. ADSL provee una conexión permanente, con un gran incremento de la velocidad, ya que permite aumentar la velocidad de transmisión hasta los 2 Megabits por segundo (Mbps) al recibir datos y a 300 Kbps al enviarlos. Y es que, como recoge la "A" inicial de ADSL, la línea es Asimétrica, lo que significa que, puesto que normalmente el usuario habitual de Internet recibe bastantes más datos de los que envía, se ha habilitado para un mayor tráfico el canal que más se va a usar. Además, ADSL permite que en una misma línea telefónica se pueda combinar simultáneamente la transmisión de datos con las llamadas telefónicas normales.

algoritmo: En programación, porción de código del programa que resuelve o ejecuta funciones específicas para la resolución de un problema o un proceso.

analog: *Analog* (Análogo). Mecanismo o método, en la cual los datos están representados por cantidades variables físicas continuas y que usa variaciones no discretas en frecuencia, amplitud o localización para transportar sonidos, señales, data matemática u otra información.

ancho de banda: (1) Es la capacidad de transporte de datos. Normalmente se mide en megabytes por segundo (MB/s) o en gigabytes por segundo (GB/s). Un ejemplo de esto sería una manguera de riego del jardín que transporta una cantidad determinada de litros de agua por segundo, pero cuanto mayor sea la manguera, más agua transportará. Cuanto más ancho de banda, mejor. En inglés ese término se conoce como *bandwidth*.

(2) Anchura de banda. Técnicamente es la diferencia en hertzios (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. Sin embargo, este término se usa mucho más a menudo para definir la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

ancho de bus: Se llama bus a los cables que llevan los datos de un sitio a otro de la computadora, normalmente lo que interesa de un bus es su ancho. Cada cable puede transportar un bit. Se mide en bits (b) o bytes (B). Los procesadores Pentium I, II y III tienen un bus de entrada de 64 bits.

ANSI: (1) *American National Standard Institute*. Instituto Nacional Americano de Estándar.

(2) *American National Standards Institute* (Instituto Nacional Americano de Estándares). Una organización estadounidense formada para certificar los estándares desarrollados en la varias industrias para que no sean influenciados por los intereses de una compañía o grupo. Este instituto en sí no desarrolla estándares, pero revisa e implementa aquellos desarrollados por otras organizaciones. Por ejemplo, ANSI acredita estándares para telefonía desarrollados por ATIS bajos los auspicios del Comité T1 y los estándares para celulares desarrollados por EIA/TIA.

applet: (1) Nombre dado a un pequeño archivo binario (normalmente escrito en lenguaje Java) ejecutado en su computadora como parte de la carga de una página de Web. No deben confundirse los *applets* con las páginas que contienen JavaScript.

(2) Se llama *applet* a cualquier programa pequeño hecho en Java que puede referirse en una página HTML. Los *applet* difieren de los programas hechos específicamente para Java en que no serán autorizados a acceder ciertos recursos de la PC local, como archivos y dispositivos de *hardware*, y no puede comunicarse con otras computadoras conectadas a una red local.

Archie: (1) Puede buscar información en servidores 'FTP *Anonymous*'. Los servidores Archie tienen una lista con información de los servidores 'FTP *Anonymous*' que agrupa.

(2) Un servicio que permite buscar archivos y directorios por sus nombres en Internet. También sirve para localizar otros servicios disponibles en la red. Los usuarios generalmente utilizan el servicio Archie, en conjunto con FTP.

ARPA / ARPAnet: (1) Red de telecomunicaciones precursora de Internet. El término procede de las siglas ARPA (*Advanced Research Projects Agency*) Agencia de Proyectos de Investigación Avanzada de los EEUU.

(2) Este término proviene de *Advanced Research Project Agency Network* o Red de Proyectos de Investigación Avanzados. Se considera el precursor de la red Internet. Fue desarrollado a finales de los años 60 y a comienzos de los 70 por el Departamento de Defensa Americano, como un experimento en redes mundiales que sobreviviera una guerra nuclear.

arroba / @: Este signo es uno de los componentes de las direcciones de correo electrónico y separa el nombre del usuario de los nombres de dominio del servidor de correo (ejemplo: pepe@mail.com); el origen de su uso en Internet está en su frecuente empleo en inglés como abreviatura de la preposición *at* (en).

ASCII: Son las siglas de *American Standard Code for Information Interchange* (Código estándar estadounidense para el intercambio de la información). Es el formato más común de archivos de texto, tanto en las computadoras en general como en Internet. En él, cada caracter está representado por 7 bits (unos o ceros). Puede por tanto, representar 128 caracteres. También existe una versión de 8 bits.

ATM: (1) *Asynchronous Transfer Mode*. Modo de Transferencia Asíncrona. Estándar que define la conmutación de paquetes ("*cells*" o celdas) de tamaño fijo con alta carga, alta velocidad (entre 1,544 Mbps. y 1,2 Gbps) y asignación dinámica de ancho de banda. ATM es conocido también como "paquete rápido" (*fast packet*).

(2) *Asynchronous Transfer Mode* (Modo de Transferencia Asincrónica). Es una rápida técnica multiplexica y móvil que usa el tamaño fijo de células para apoyar varios tipos de tráfico como voz, data y video.

B

backbone: (1) Eje central, columna vertebral o espina dorsal. Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (*stub*) y de tránsito (*transit*) conectadas al mismo eje central están interconectadas.

(2) En español, espina dorsal. El *backbone* es el trecho de mayor capacidad en la red y es donde se conectan varias redes locales. Los proveedores de acceso por lo general están conectados directa y permanentemente al *backbone*.

bajar / bajada: Proceso de transferir un archivo o programa desde alguna computadora fuente a la computadora local. La bajada o *downloading* es un proceso controlado mediante un protocolo, que mueve el archivo de manera tal que se asegure que permanezca intacto y sin daños.

bandwidth: Ver "ancho de banda".

baudio: (1) Término utilizado en comunicaciones para medir la velocidad de un dispositivo.

(2) Cuando se transmiten datos, un baudio es el número de veces que cambia el "estado" del medio de transmisión en un segundo. Por ejemplo, un módem de 52.000 baudios cambia 52.000 veces por segundo la señal que envía por la línea telefónica. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo, medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

(3) La frase *baud rate* se refiere a la velocidad de transmisión de información entre computadoras a través de líneas telefónicas. *Baud rate* con frecuencia se utiliza como sinónimo de bits por segundo (bps), a pesar de que técnicamente no son intercambiables. La palabra *baud* viene de J. M. Baudot, inventor del código telegráfico Baudot.

Bcc: Es una de las líneas que componen la cabecera de un mensaje de correo electrónico y su finalidad es incluir uno o más destinatarios de dicho mensaje cuya identidad no aparecerá en el mensaje recibido por el destinatario o destinatarios principales. La etiqueta de la red dicta suprimir, o al menos limitar al máximo, el uso de este procedimiento porque en cierta manera se está ocultando al destinatario que el mensaje llegará a otras personas.

Por el contrario se recomienda su uso cuando hay que enviar un mensaje a un número alto de destinatarios, para evitar que la cabecera del mensaje sea de gran tamaño. "Bcc" es un acrónimo de la frase inglesa "*blind carbon copy*" (copia ciega en papel carbón).

binario: Método para la codificación de números en forma de series de bits. El sistema numérico binario, conocido también como "base 2", utiliza combinaciones de sólo dos dígitos: 1 y 0.

bit: Unidad mínima de información de la memoria, equivalente a un "sí" (0) o un "no" (1) binarios. La unión de 8 bits da lugar a un byte.

bookmark: Traducción literal "marca páginas". Se utiliza este término para designar la característica que tienen algunos navegadores, como los de Netscape, de archivar la dirección URL de una página Web como si de una agenda se tratara. De esta manera, cuando queremos acceder a dicha página, basta con utilizar esta función, y nos conectaremos a su dirección.

bps: (1) Bits por segundo, unidad de transmisión de datos empleada principalmente en referencia a módems o comunicaciones de red.

(2) BPS (bits por segundo) es una medida de velocidad de transmisión de datos. Es utilizada para medir la velocidad de los módems y las conexiones telefónicas. También se usan los Kbps (equivalente a mil bps) y Mbps (equivalente 1 millón de bps).

bridge: (1) En el contexto del hardware suele encontrarse referida a "*North Bridge*" y "*South Bridge*". En pocas palabras, esos son los nombres genéricos que se le da a los dos componentes principales del "*chipset*" de una placa base. El *chipset* es el juego de circuitos que controlan el funcionamiento de la placa, el acceso a la memoria y los dispositivos de almacenamiento, gestión de los puertos de comunicaciones, y otras cosas por el estilo. Es decir, el *chipset* es el juego de circuitos que sirven a la CPU todo lo que esta necesita. Traducido literalmente del inglés "*bridge*" significa "puente", que es justo lo que hacen estos circuitos... son el "puente" entre la CPU y los dispositivos de una computadora.

(2) *Bridge*. Literalmente significa "puente". Unidad funcional que interconecta dos redes de área local (LAN) que usan el mismo protocolo de control de enlace lógico pero que pueden usar distintos protocolos de control de acceso al medio.

broadband: *Broadband* (Banda Ancha). Generalmente se compara ancho de banda relativo a banda angosta. Por ejemplo vídeo es considerado banda ancha en relación a voz. En sistemas de transmisión de telecomunicaciones, cualquier sistema de transmisión que opera a velocidades superiores mayores que la tasa primaria de 1.5 Mb/s en los EE.UU. o 2 Mb/s en el extranjero. Sin embargo muchos consideran 1.5-45 Mb/s como banda amplia, y consideran banda ancha a velocidades de más de 45 Mb/s.

browser: Navegador. Aplicación para visualizar documentos WWW y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servicios de información Internet; los más avanzados cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

bug: Error de programación que genera fallos en las operaciones de una computadora.

buscador: (1) Servicio WWW que permite al usuario acceder a información sobre un tema determinado contenida en un servidor de información Internet (WWW, FTP, Gopher, Usenet Newsgroups...) a través de palabras de búsqueda introducidas por él.

(2) Está diseñado para ayudar al usuario a encontrar la información o los recursos que pretende conseguir mediante la búsqueda de palabras claves. El método utilizado es normalmente un índice de recursos web que puede ser construido a partir de listas de recursos específicos o creados por *web wanderers*, *robots*, *spiders*, *crawlers* o *worms*.

byte: (1) Unidad de información, compuesta de 8 bits consecutivos. Cada byte puede representar, por ejemplo, una letra.

(2) Byte es una unidad de medida de información que está compuesta por 8 bits. Un bit es un 1 o un 0. Con un byte se pueden representar 28 cosas, o sea 255 letras distintas, 255 tonos distintos de un color, 255 sonidos distintos. El documento que estás leyendo no es más que una tira de bytes que tienen ciertos valores (letras). Si cada letra ocupara 1 byte (texto puro sin formato) realmente no costaría mucho llenar un disco duro.

C

CC: *Carbon Copy* o *Courtesy Copy*. Parte del encabezado de un correo electrónico que señala uno o más destinatarios de una copia del mensaje además del destinatario o destinatarios principales.

CD: Significa *Compact Disc*. Es un término general para todos los formatos de disco compacto, como puedan ser CD Audio, CD-ROM, CD-ROM XA, VideoCD, CD-I y otros muchos.

CD-ROM: (1) Dispositivo físico conectado a una computadora la cual permite leer un disco CD-ROM. Todos los lectores de CD-ROM también pueden reproducir CD Audio, mediante la utilización de auriculares externos y/o altavoces.

(2) *Compact Disc-Read Only Memory*. Disco compacto de sólo lectura. Es un estándar para los CDs utilizados como medio de almacenamiento para computadoras personales. La especificación del CD-ROM fue definida en el Libro Amarillo (*Yellow Book*).

(3) Un CD que sólo contiene pistas de datos tal como se define en el Libro Amarillo (*Yellow Book*).

CGI: (1) Es un interfaz que sirve para que los programas externos (pasarelas) puedan rodar bajo un servidor de información. Actualmente, los servidores de información soportados son HTTP.

(2) Interfaz de intercambio de datos estándar en WWW a través del cual se organiza el envío y recepción de datos entre navegador y programas residentes en servidores WWW.

(3) *Common Gateway Interface*. Estándar de programación que determina cómo puede interactuar una página de Web con el usuario, -por ejemplo, relleno de un formulario-. Por lo general las aplicaciones CGI están escritas en PERL o C, lenguajes de computación de complejidad variable.

(4) *Common Gateway Interface*. Conjunto de reglas que describen cómo un servidor Web se comunica con un programa dentro de la misma máquina (el "programa CGI"). Cualquier programa puede ser un CGI, con tal de que maneje sus entradas y salidas de acuerdo con dichas reglas. Usualmente, cuando se está usando un programa CGI, puede verse "cgi-bin" en el URL del navegador, aunque no siempre sucede así.

chat: Conversación en tiempo real a través de la computadora. En algunos sistemas más antiguos de *chat*, la pantalla se divide en dos. Cada parte contiene el texto de uno de los interlocutores. Los sistemas más modernos permiten la creación de "salas" de conversación en páginas electrónicas. El *chat* en Internet se hizo famoso a través de servidores de IRC (*Internet Relay Chat*), donde se hicieron las "salas" o "canales" para albergar a los usuarios.

ciberespacio: Término acuñado por el escritor William Gibson e inspirado en el estado de trance en que quedan los aficionados de juegos de vídeo durante un juego. La palabra fue utilizada por primera vez en el libro Neuromancer, publicado en 1984, y adoptada desde entonces por los usuarios de la Internet como sinónimo de la red.

clic / click: Acción del visitante al ver un anuncio y presionar sobre el mismo con el botón del mouse a fin de dirigirse al sitio del anunciante.

cliente: (1) Es un programa que solicita servicio de una computadora servidor. Internet está basada en una estructura de cliente / servidor. Para cada tipo de cliente, hay un servidor correspondiente. En la red, las programaciones clientes son los *browsers* o navegadores, mientras que los servidores son las programaciones que almacenan las páginas y verifican las autorizaciones de los usuarios para acceder determinados documentos

(2) En su sentido más común en el contexto informático, se refiere a una computadora temporalmente conectada a Internet vía una conexión módem.

Concentrador: véase: "*hub*"

controlador: Forma española de denominar los *drivers*.

cookie: (1) Son unos archivos que almacenan información en la computadora del usuario. Gracias a dicha información se puede conocer el usuario, horas de acceso, páginas visitadas, temas de interés, etc. Todo ello tiene el objetivo de reconocer al usuario para personalizar la web, y ofrecerle el contenido, servicios, comercio e información que le pueda interesar.

(2) Conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha hecho, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un archivo en el directorio del navegador para ser utilizada en una próxima visita a dicho servidor.

correo electrónico: (1) El correo electrónico es el servicio más básico, antiguo, y el más utilizado dentro de Internet. Permite intercambiar mensajes, programas, audio, vídeos e imágenes.

(2) Forma de intercambiar mensajes entre usuarios. No es necesario que el destinatario esté conectado a la red en el momento en que el mensaje llega. El usuario recibe un aviso de que tiene mensajes nuevos cuando se conecta al sistema. Es posible enviar copias de mensajes para varias personas y también guardar los mensajes enviados.

CPU / microprocesador: (1) *Central Processing Unit* o Unidad Central de Proceso. El "cerebro" de una computadora; en general, sinónimo de microprocesador. En ocasiones se usa para referirse al toda la caja que contiene la placa base, el micro y las tarjetas de expansión.

(2) *Central Processing Unit* o Unidad Central de Procesamiento. Es un Chip que contiene millones de transistores encargados de realizar las operaciones que encomendamos a la computadora. No obstante, por sí sola no sirve para nada, porque debe estar conectada a la placa madre. La placa madre provee de corriente eléctrica a la CPU y le permite comunicarse con el resto de dispositivos.

cracker: (1) Un *hacker* con intenciones destructivas o delictivas.

(2) Intruso. Un "*cracker*" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "*hackers*", y suelen disponer de muchos medios para introducirse en un sistema. Ver también: "*hacker*", "CERT", "*Trojan Horse*", "virus", "*worm*".

(3) Persona que ingresa ilegalmente en un sistema informático para robar o destruir información, o simplemente para causar desorden. También se llama *cracker* a quien descifra los esquemas de protección anti-copia de los programas comerciales, para poder utilizar o vender copias ilegales.

cuenta: Tener una cuenta en un proveedor de acceso es como ser socio de un club. El titular de la cuenta recibe un nombre de usuario (*username*) y contraseña (*password*) para acceder el sistema. Paga una mensualidad de acuerdo con los servicios que utiliza y dependiendo de los planes de pago del proveedor de acceso.

D

Datagrama: Agrupamiento lógico de información enviada como unidad de la capa de red en un medio de transmisión, sin el establecimiento de un circuito virtual.

dirección: (1) En Internet dícese de la serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: "dirección de correo electrónico" (*email address*); "IP" (dirección Internet); y "dirección hardware" o "dirección MAC" (*hardware or MAC address*).

(2) Las memorias en una computadora están numeradas dando lugar a lo que se denominan "posiciones" o lugares de almacenamiento (en sentido muy genérico). Cuando se pretende acceder a los datos contenidos o escribir en una posición concreta, se accede a ella a través de su número o dirección de memoria.

direccionamiento: Distintas formas de hacer referencia a una dirección.

dispositivo: Los dispositivos son objetos físicos que, sin pertenecer al conjunto "Procesador / memoria", permiten realizar operaciones de entrada y salida de datos. Por ejemplo, son dispositivos el teclado, el ratón, el monitor, la impresora, el micrófono, los altavoces, etc...

DNS: (1) Su utilidad principal es la búsqueda de direcciones IP de sistemas anfitriones, basándose en los nombres de éstos. El estilo de los nombres de *host* utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes, son: .com (comercial), .net (operación en la red), .org (organismo), .es (España), etc...

(2) El *Domain Name System* (DNS) convierte los nombres en Internet en sus direcciones numéricas correspondientes y viceversa. Originalmente, las computadoras en el Internet eran identificadas sólo por números, como 207.46.197.101. El DNS hizo posible darles nombres a las computadoras, como www.servidor.com, y traducirlos a sus respectivas direcciones numéricas.

download: Cuando el usuario copia un documento de la red en su computadora, está haciendo un *download*. La misma expresión puede aplicarse cuando se copian documentos en servidores de FTP, imágenes sacadas directamente de la red con un *browser* y cuando los mensajes llegan a la computadora del usuario. También se le llama *download* cuando, durante el acceso a una página de la red, se transmiten las imágenes y textos que la componen.

driver: (1) Pequeño programa cuya función es controlar el funcionamiento de un dispositivo de la computadora bajo un determinado sistema operativo.

(2) Es un programa que controla un dispositivo. Cada dispositivo, teclado, disco duro, impresora, etc... Necesita ser controlado por algún programa. Algunos "*Drivers*" vienen incorporados en el propio sistema operativo, como por ejemplo el del teclado. En otros dispositivos es necesario instalar el "*driver*" o controlador para que el sistema operativo pueda manejarlo. El "*driver*" actúa como traductor de instrucciones especificas de cada dispositivo en instrucciones genéricas que utiliza el sistema operativo.

DSL: Se refiere colectivamente a todos los tipos de líneas digitales, las dos categorías principales son ADSL y la SDSL. Otros dos tipos de xDSL son el *High-data-rate* (HDSL) y el *Single-line* o (SDSL). La tecnología DSL utiliza modulación de alto nivel para aprovechar los pares de hilo de cobre usados en telefonía. A veces le hacen referencia como tecnología de último minuto porque son utilizadas solamente para conexiones desde una estación de teléfono a una oficina o residencia, no entre estaciones intermedias. xDSL es similar a la ISDN ya que las dos operan sobre líneas de cobre existentes (POTS) y ambas requieren llegar rápidamente a una central telefónica (usualmente a menos de 20,000 pies). De todos modos, xDSL ofrece velocidades mucho mayores, hasta 32 Mbps en horas de alto flujo, y desde 32kbps hasta 1Mbps en horas de bajo flujo.

DSLAN: *Digital Subscriber Line Access Multiplexer*. Un chasis que agrupa gran número de tarjetas, cada uno de las cuales consta de varios modelos ATU-C, y que además concentra el tráfico de todos los enlaces ADSL hacia una red WAN. Que no son más que la integración de varios ATU-Cs en un mismo equipo, pudiendo así facilitar el despliegue de esta tecnología.

E

ECC: (1) *Error Correction Code*. Código de Corrección de Errores. Son 276 bytes. Es un sistema por el que se toma y graba información redundante al disco. En la reproducción, esta información redundante ayuda a detectar y corregir errores que pueden presentarse durante la trasmisión de datos.

(2) Código de Corrección de Errores. Método electrónico para verificar la integridad de los datos en DRAM. ECC es un método de detección de errores más avanzado que el de la paridad; puede detectar errores de múltiples bits y puede localizar y corregir los errores de un solo bit. ECC normalmente utiliza tres bits adicionales por cada byte de datos (en comparación con el bit adicional que se utiliza en el método de paridad).

e-commerce: Proceso de venta de productos o servicios mediante la Red.

e-mail: Ver "correo electrónico".

encriptación: Conjunto de técnicas que permiten codificar la información que circula en Internet de manera que las personas no autorizadas no puedan leerla ni manipularla.

Ethernet: Un estándar para redes de computadoras muy utilizado por su aceptable velocidad y bajo coste. Admite distintas velocidades según el tipo de hardware utilizado, siendo las más comunes 10 Mbits/s y 100 Mbits/s (comúnmente denominadas *Ethernet* y *Fast Ethernet* respectivamente).

F

FAQ: *Frequently Asked Questions*. Documento con las preguntas y respuestas más frecuentes sobre un tema específico. Cada grupo de discusión y lista de distribución acostumbra tener su propio FAQ. Se espera que los usuarios nuevos lean el FAQ de un grupo antes de hacer una pregunta. Ultimamente se ha empezado a utilizar como sinónimo de Ayuda Técnica.

fibra óptica: Tipo de cable que se basa en la transmisión de información por técnicas optoeléctricas. Se caracteriza por un elevado ancho de banda, y por tanto una alta velocidad de transmisión, y poca perdida de señal.

firewall: Es un sistema de seguridad cuyo principal objetivo es filtrar el acceso a una red. Las empresas utilizan el *firewall* para proteger sus redes internas conectadas al Internet contra la entrada de usuarios no autorizados.

floppy: Forma inglesa de denominar al disquete.

FTP: (1) *File Transfer Protocol.* Protocolo para la transferencia de archivos a través de Internet.

(2) *File Transfer Protocol.* Protocolo para transferencia de documentos. El FTP puede ser utilizado para copiar documentos de la red a la computadora del usuario y viceversa. Los navegadores de WWW pueden hacer transferencias de FTP, pero existen programas diseñados específicamente para esta tarea.

Los usuarios deben darle al programa FTP la dirección del servidor. También es necesario tener una cuenta en el servidor y con nombre de usuario (*username*) y contraseña (*password*), a menos que se trate un servidor de FTP anónimo.

FTP Anonymous / FTP anónimo: (1) Los servidores "*FTP Anonymous*" son grandes cajones de archivos distribuidos y organizados en directorios. Contienen programas (normalmente de dominio público o shareware), archivos de imágenes, sonido y video. El medio de acceso y recuperación de la información es FTP (*File Transfer Protocol*). Para entrar en estos servidores, tecleamos FTP y nombre del servidor. El sistema nos pregunta '*login*', a lo que respondemos con la palabra '*anonymous*' y en el '*password*' le indicaremos nuestra dirección de correo electrónico. Algunos servidores autentifican esta dirección. Al existir miles de servidores FTP, se hace imprescindible una herramienta de búsqueda. Archie es la solución Cliente / servidor implementada para este fin.

(2) Servicio que posibilita el acceso a bibliotecas públicas de documentos vía FTP. Se llaman "FTP anónimo" porque el usuario no tiene que identificarse, o se acepta cualquier cosa como identificación, cuando se conecta a uno de estos servidores.

G

gateway: (1) Sistema que hace de puente entre dos sistemas incompatibles, como la conexión entre el correo electrónico interno de una empresa y el e-mail del Internet.

(2) Pasarela. Hoy se utiliza el término "*router*" (direccionador, encaminador, enrutador) en lugar de la definición original de "*gateway*". Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes.

Gopher: (1) Herramienta de búsqueda que presenta información en un sistema de menús jerárquicos parecidos a un índice. Se trata de un método de hacer menús de material disponible a través de Internet. El *Gopher* es un programa de estilo Cliente-Servidor, que requiere que el usuario tenga un programa cliente *Gopher*. Aunque *Gopher* se extendió rápidamente por todo el mundo, ha sido sustituido en los últimos años por el Hipertexto, también conocido como WWW (World Wide Web).

(2) Un sistema para buscar documentos en la red por medio de menús. Los documentos almacenados en servidores *gopher* no usan conexiones de hipertexto para entrelazarse como ocurre en las páginas electrónicas. Hasta la llegada de Internet, el *gopher* era la principal herramienta de búsqueda de información en la red. La dirección de una página *gopher*, en vez de empezar por http:// empieza por gopher://. El nombre *gopher* se inspiró en la mascota de la Universidad de Minessota, donde se inventó este sistema.

H

hacker: (1) Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.

(2) Persona que disfruta investigando de los detalles de los sistemas operativos y los programas, buscando nuevas formas de aumentar sus capacidades. Aquellos que programan, a veces hasta con obsesión, que disfrutan de esto. Experto o entusiasta de cualquier disciplina, no solo de computación. Quien goza con el desafío intelectual que representa el superar las limitaciones impuestas.

(3) Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de una computadora o de una red de computadoras. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término *"cracker"*.

hipertexto: Texto capaz de incluir en su contenido enlaces con otras partes del mismo documento o con documentos diferentes. Los enlaces normalmente se indican mediante una imagen o una palabra subrayada y en color diferente al resto del texto. Al oprimir la palabra o imagen que conecta, el usuario es llevado hasta el texto o documento enlazado.

hipervínculo / hiperlink: (1) Texto o gráficos con propiedades de enlace. Cuando un usuario hace click en textos o gráficos hipervinculados, es llevado a otra localización, sea o no dentro de la misma página.

(2) Nombre que se le da a las imágenes o palabras que dan acceso a otros textos, documentos o páginas electrónicas dentro de la red. El *hyperlink* (en español también se le dice enlace, hipervínculo o conexión electrónica) puede llevar a otra parte del mismo documento, o a otros documentos.

Home Page: Muchas personas utilizan inadecuadamente la frase *home page* para definir cualquier página en la Internet. En su acepción más rigurosa, un *home page* es la página o puerta de entrada a un *Web Site*, pero el término puede ser usado también para indicar la página principal de una determinada sección.

host: Es una computadora conectada permanentemente a la red, que entre otras cosas, almacena documentos y permite el acceso de usuarios.

HTML: (1) *Hypertext Markup Language*. Lenguaje usado para escribir documentos para servidores World Wide Web (WWW). Es una aplicación de la ISO Standard 8879:1986.

(2) Lenguaje utilizado en la producción de páginas de la red. HTML es una derivación del SGML (*Standard Generalized Mark-up Language*) y permite la creación de documentos que pueden ser leídos en prácticamente cualquier tipo de computadora y transmitidos por Internet y hasta por correo electrónico. Los documentos en HTML pueden tener enlaces de hipertexto entre sí. Para escribir documentos en HTML sólo es necesario tener un editor de texto simple y conocimiento de los códigos que componen el lenguaje. Los códigos (conocidos como *tags*) son elementos tipográficos que definen la forma y uso de cada elemento del texto en un documento. El conjunto de *tags* ya está en su tercera versión, conocida como HTML 3.0, que permite crear tablas. Algunas empresas que desarrollan productos para Internet han creado extensiones propias (que sólo funcionan con sus productos) para HTML. Entre éstas se encuentran Netscape y Microsoft.

HTTP: (1) *Hypertext Transfer Protocol*. Protocolo utilizado para distribuir y manejar sistemas de información hipermedia. Una característica de *http* es la independencia en la visualización y representación de los datos.

(2) *Hypertext Transfer Protocol*. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia. Es un protocolo genérico orientado al objeto, que puede ser usado para muchas tareas como servidor de nombres y sistemas distribuidos orientados al objeto, por extensión de los comandos, o métodos usados. Una característica de HTTP es la independencia en la visualización y representación de los datos, permitiendo a los sistemas ser construidos independientemente del desarrollo de nuevos avances en la representación de los datos HTTP ha sido usado por los servidores World Wide Web (WWW) desde su inicio en 1.990.

(3) Protocolo de comunicación que posibilita las conexiones entre los clientes de WWW y los Web Sites. Las siglas HTTP se encuentran en las direcciones de las páginas electrónicas (los URLs), seguidas de ://. El prefijo HTTP informa al servidor de qué forma debe ser atendido la petición del cliente.

HUB: Punto de conexión común para dispositivos dentro de una red, normalmente une a segmentos de una red. El *hub* se encarga de distribuir la información recibida por cualquiera de sus puertos a todos los demás.

Existen tres tipos de hub:

*Pasivo; simplemente actúa a modo de repetidor de datos entre todos sus puertos.
*Gestionable; permite monitorizar su actividad y configurar puertos y tráfico en su red.
*Switches; hub inteligente, recibe la información y la entrega sólo al puerto correcto con lo que aumenta el rendimiento global de la red

I

IEEE: *Institute of Electrical and Electronics Engeneers*. Instituto de Ingenieros Eléctricos y Electrónicos.

Internet: (1) Con inicial mayúscula, significa la "red de las redes", originalmente creada en los Estados Unidos, que se tornó en una asociación mundial de redes entrelazadas que utilizan protocolos de la familia TCP/IP.

(2) Es la mayor Red Mundial de computadoras conectadas entre sí. Originalmente creada y promovida por los EE.UU. para el intercambio y conexión de Universidades y centros docentes. En sus inicios no estaba permitido el uso comercial de la misma, pero en el momento que el gobierno de los EE.UU. retiró las ayudas económicas, esta norma desapareció. Sobre las mismas fechas apareció el primer Navegador "Mosaic", contribuyendo todo ello al auge y al desarrollo de Internet.

(3) Es la red de redes. Nacida como experimento del ministerio de defensa americano, conoce su difusión más amplia en el ámbito científico-universitario. Embrión de las 'superautopistas de la información'. Para convertirse en ellas faltan mayores infraestructuras y anchos de banda. Desde el punto de vista técnico, Internet es un gran conjunto de redes de computadoras interconectadas. Desde otro punto de vista, Internet es un fenómeno sociocultural. Un usuario desde su consola, tiene acceso a la mayor fuente de información que existe. En cuanto a funcionamiento interno, Internet no se ajusta a ningún tipo de computadora, tipo de red, tecnología de conexión y medios físicos empleados. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. La familia de protocolos TCP/IP es la encargada de aglutinar esta diversidad de redes. A principios de 1.992 fué creada la Internet Society (ISOC).

Se trata de una sociedad profesional sin ánimo de lucro, formada por organizaciones e individuos de todos los sectores involucrados de una u otra forma en la construcción de Internet (usuarios, proveedores, fabricantes de equipos, administradores, etc.). El principal objetivo es fomentar el crecimiento de la Internet en todos sus aspectos (número de usuarios, nuevas aplicaciones, infraestructuras, etc.).

Intranet: Es una red de computadoras limitada a un número de usuarios determinados que generalmente están en un mismo edificio o empresa, aunque pueden estar más distanciados. Emplea tecnología Internet y protocolos TCP/IP. Limita y restringe el acceso a cualquier persona que no esté autorizada.

IP: (1) Internet Protocol. Parte del conjunto de protocolos TCP/IP encargada de la interconexión de redes. Es el fundamento básico y de más bajo nivel de Internet.

(2) Siglas para *Internet Protocol* (Protocolo de Internet). Es el protocolo responsable del envío de paquetes de información entre dos sistemas que utilizan la familia de protocolos TCP/IP, desarrollados y usados en Internet. El envío de paquetes permite dividir la información en bloques que pueden ser remitidos por separado y después reagrupados en su destino.

ISDN: *Integrated Services Digital Network*. Forma inglesa del término "RDSI".

ISP: *Internet Service Provider*. Organización que provee de acceso a Internet. Un ISP puede ser un proveedor oficial, una red de trabajo corporativa, un colegio, una universidad o incluso el gobierno.

J

Java: (1) Lenguaje de programación presentado en el año 1995 por "Sun Microsystems". Tiene la ventaja que es independiente de la plataforma que lo ejecuta, por lo tanto es ideal para Internet, hecho que ha provocado que se convierta en el lenguaje propio de Internet.

(2) Lenguaje de programación desarrollado por "Sun Microsystems" para la elaboración de pequeñas aplicaciones exportables a la red (*applets*) y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores WWW. Permite dar dinamismo a las páginas web.

JavaScript: Lenguaje desarrollado por Netscape. Aunque es parecido a Java se diferencia de él en que los programas están incorporados en el archivo HTML.

K

KB: Kilobyte, múltiplo del byte equivalente a 1024 bytes. Más correcta, aunque menos utilizada, es la forma "kb"; también se emplea "Kb".

KBPS: La velocidad de transmisión de los módems y redes de datos se mide en Bits por segundo. Cuando la transmisión es de alta velocidad se puede medir en Kbps (Kilobits por segundo) que es igual a 1024 bits por segundo.

L

lammer: Persona que suele destacarse por preguntas incoherentes en medio de discusiones importantes o no. Generalmente adolescentes o tardíos, que saben poco de computación, o con conocimientos mínimos, y que en un arranque de estupidez pretenden convertirse en *Hackers* de la noche a la mañana, molestando a quienes participan de foros de discusión o *chats* con preguntas sin sentido, insultos o comentarios fuera de lugar.

LAN: (1) *Local Area Net*, red de área local. Una red de computadoras de tamaño medio, dispersa por un edificio o incluso por todo una ciudad.

(2) *Local Area Network* o Red de Área Local, red que agrupa un número relativamente pequeño de computadoras. Las LAN se pueden conectar entre ellas a través de enlaces telefónicos o de datos dedicados, a estos enlaces se les conoce como WAN. Existen diferentes tipos de redes locales, aunque la mayoría son para PC's, también existen de diferente tipo como el AppleTalk, integrado en las computadoras Macintosh. Existen redes de varios tipos en función de su:
* Topología (forma de interconectar las computadoras).
* Protocolo, es como el lenguaje utilizado para la comunicación entre computadoras.
* Tipo de cableado, de par trenzado, BNC, fibra óptica, etc ..

link: Término inglés que significa "enlace". Ver "hipervínculo".

LINUX: Un sistema operativo multiusuario y multitarea basado en UNIX.

M

mail: Ver "correo electrónico".

mainframe: A los *Mainframes* también se les conoce con el nombre de grandes computadoras. Se dedican principalmente a la gestión, pudiendo realizar muchos trabajos a la vez. Una de sus aplicaciones puede ser controlar la red de cajeros automáticos de un Banco.
El *mainframe* será capaz de gestionar la información de todos los cajeros conectados a él.

Multistation Access Units (MAUS): Un conector MAU conecta 8 o más Estaciones de Trabajo usando algún tipo de cable de red como medio. Se pueden interconectar más de 12 dispositivos MAU.

La MAU es el circuito usado en un nodo de red para acoplar el nodo al medio de transmisión. Este aislamiento es la clave para la inmunidad de los sistemas en red ante las interferencias. La implementación y la calidad del aislamiento proporcionado varían entre diferentes topologías de red.

MB / megabyte: Megabyte, múltiplo del byte equivalente a 1024 kilobytes. Más correcta, aunque menos utilizada, es la forma "Mb". Coloquialmente, "mega".

microprocesador: Ver "CPU".

Mixed Mode Disc: Es un CD que incluye datos (pistas en formato CD-ROM) y audio (pistas en formato CD-DA). Los datos están todos contenidos en la primera pista, y el audio en una o más pistas detrás de la pista de datos.

MHz: Megahercio, múltiplo del hertzio igual a 1 millón de hertzios. Utilizado para medir la "velocidad bruta" de los microprocesadores.

microcomputadora: Las microcomputadoras son conocidas con el nombre de computadora Personal. La denominación PC proviene de su nombre en inglés *Personal Computer*. Son, sin duda, los más difundidos, no sólo para usuarios particulares, sino también para pequeñas empresas. Se pueden utilizar para una amplia gama de funciones, desde llevar la contabilidad de una empresa, hasta escuchar música.

MIME: Siglas para *Multipurpose Internet Mail Extensions*. Patrón genérico para el envío de cualquier formato de documento a través del correo electrónico y por La Red.

módem: (1) MOdulador-DEModulador, dispositivo hardware que transforma las señales digitales de la computadora en señal telefónica analógica y viceversa.

(2) El módem realiza la modulación y demodulación de las señales digitales producidas por la computadora para adaptarlas a la red de telecomunicación. De esta forma, permite a la computadora transmitir información a través de una línea telefónica. La velocidad de transmisión de los módem se mide en bits por segundo o en baudios.

(3) Equipo acoplado a la computadora que posibilita la conexión con la línea telefónica. El modem transforma las señales emitidas por la computadora en señales que pueden ser transmitidas por la línea telefónica y viceversa. La velocidad del modem es medida en bits por segundo (bps).

motor de búsqueda: Ver "buscador".

multimedia: El conjunto de imagen, sonido y vídeo aplicado al PC.

N

navegador: Es el *browser*: programa que se utiliza para navegar en Internet. Permite utilizar prácticamente todos los recursos de la red, como el correo electrónico, la transferencia de documentos y el acceso a grupos de discusión.

news / newsgroup / netnews: *Newsgroups* es como son llamados los grupos de discusión del Usenet. Los mensajes de los usuarios son almacenados e intercambiados. Los *newsgroups* de Usenet mantienen siempre una base actualizada de mensajes. Para organizar las discusiones, cada *newsgroup* está dedicado a un asunto y organizado en una jerarquía. Por ejemplo, un nombre de *newsgroup* es "news.newusers.questions". Este es el grupo donde los usuarios novatos de Internet pueden encontrar respuestas a la mayoría de sus preguntas. Además de *news*, existen las jerarquías comp (sobre computadoras), bio (sobre biología), soc (sobre aspectos sociales y culturales), misc (una jerarquía para asuntos alternativos que no cabe en ninguna de las otras), *talk*, *rec* (actividades y hobbies), etc.

NIC: Siglas para *Network Interfase Card*. Identificador único para dispositivos de red.

O

on-line: Término utilizado para designar todo tipo de transacción entre computadoras.

OSI: *Open System Interconnection* o Interconexión de Sistemas Abiertos. El modelo de referencia OSI de ISO proporciona la base para el desarrollo de estándares relativos a las redes. Este modelo enumera siete capas que definen las actividades que deben tener lugar cuando se comunican los dispositivos a través de una red. Estas siete capas (de arriba a abajo) son: aplicación, presentación, sesión, transporte, red, enlace y física.

El modelo representa las relaciones entre una red y los servicios que puede soportar como una jerarquía de capas de protocolos. Cada capa usa los servicios ofrecidos por capas más bajas además de sus propios servicios para crear otros nuevos que estén disponibles para capas superiores. En resumen, cada una de las siete capas del modelo de referencia OSI realiza tareas únicas y específicas, conoce las capas inmediatamente adyacentes, usa los servicios de la capa que está por debajo, y realiza funciones y proporciona servicios para las capas superiores.

overclocking: (1) Técnica por la cual se fuerza un microprocesador a trabajar por encima de su velocidad nominal.

(2) Significa hacer correr un microprocesador más rápido que la velocidad para la que ha sido probado y aprobado. El *overclocking* es una técnica para acelerar un poco más el funcionamiento de un sistema. En muchos casos se puede forzar a una CPU a correr más rápido que la velocidad que se le ha impuesto con sólo poner un pequeño jumper (puente) sobre la placa base. Aunque el *overcloking* tiene algunos riesgos, como el recalentamiento del procesador. Es recomendable familiarizarse con los pros y los contras antes de que probemos este sistema, ya que se puede quedar sin CPU.

P

P&P: Ver "Plug and Play".

página dinámica: Página web que cambia a menudo, normalmente a diario y/o cada vez que el usuario recarga o vuelve a la página. Su contenido está también estructurado basándose en el *input* del usuario. Por ejemplo, cuando busque algunas palabras claves en un motor de búsqueda, la página resultante será "dinámica", significando ello que la información fue creada a partir de las palabras que escribió. Las sedes web dinámicas son llevadas a menudo por entornos de aplicaciones web como Microsoft ASP o Allaire's Cold Fusion, y el contenido se extrae de una base de datos cada vez que se solicita.

página web: Archivo o archivo que constituye una unidad significativa de información accesible en la WWW a través de un programa navegador. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. El término "página web" se utiliza a veces de forma incorrecta para designar el contenido global de un sitio web.

partición: Unidad de disco lógica. Un solo disco duro puede tener más de una. Esto se refleja en la existencia de más unidades de disco.

PC: *Personal Computer*, computadora personal; nombre (registrado) con que bautizó IBM en 1.981 al que se convertiría en estándar de la informática de usuario; por extensión, cualquier computadora compatible de otra marca basado en principios similares.

pin: Cada uno de los conectores eléctricos de muchos elementos hardware, como las "patitas" de muchos microprocesadores.

ping: Aplicación usada en Internet para determinar si está o no activa la conexión a una máquina específica, o para averiguar la factibilidad de alcanzar a otra máquina. Básicamente, *Ping* envía una pequeña serie de sencillos *packets* -paquetes de datos-, y si la máquina apuntada retorna dichos *packets*, entonces esa máquina es considerada activa y disponible. La expresión fue tomada del sonar, que manda un sonido similar a un 'ping', y el eco que regresa es monitoreado y analizado. Algunos programas *Ping* también muestran la ruta seguida por los *packets*, y el tiempo empleado en ella, lo que resulta útil para seguimiento de problemas y evaluación de velocidades de conexión.

Plug and Play: Tecnología que permite la auto detección de dispositivos tales como tarjetas de expansión por parte de la computadora, con objeto de facilitar su instalación.

PnP: Ver "Plug and Play".

POP: Punto-de-Presencia local de un *backbone* de una red. Una red se extiende a través de puntos-de-presencia en las principales ciudades de una región: entrelazados por un conjunto de líneas dedicadas que componen un *backbone*.

POP3: Protocolo de Oficina de Correos. Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor. La versión 3, la más reciente y más utilizada, llamada POP3, está definida en RFC-1725.

portal: (1) Página web que nos da un conjunto de links de diferentes páginas *webs* dirigidas por diferentes temas. Suelen tener la posibilidad de hacer búsquedas de una o más palabras y darnos las páginas *webs* que las contienen.

(2) Estrategia de *WEB Site*, en ocasiones se trata de una evolución de un Buscador. Dicha Estrategia pretende atraer y fidelizar el máximo número de internautas con el fin de que cuando accedan a Internet lo hagan a través de dicha *WEB*.

Para conseguirlo, se regala a los internautas accesos a Internet, cuentas de e-mail, espacio para poner *webs*. Así mismo se pueden acceder a contenidos diversos y variados, tales como información específica, noticias, el tiempo, la bolsa, etc. Todo ello persigue varios fines, por un lado asegurarse la visita continua y repetida de los internautas, que se encuentran "obligados" a acceder al "portal" si desean por ejemplo leer su correo, y por el otro conseguir los datos de los internautas, datos que se deben dar si deseas conseguir algún servicio gratuito. Con dichos datos podrán segmentar mejor los espacios de publicidad que ofrecen y los venderán a las agencias, y por el otro podrán ofrecer productos y servicios acordes al perfil prefijado.

(3) Punto de inicio para una experiencia de un usuario en la Red que ofrece información y servicios y que a menudo incluye noticias, email, entretenimiento, compras, deportes y otros. El término de portal se refiere a una puerta virtual que el usuario atraviesa cada vez que accede a Internet. A menudo es la primera pantalla que ve cuando entra en línea.

PPP: (1) *Point to Point Protocol*, protocolo de comunicaciones en el que se basan muchas redes.

(2) Puntos Por Pulgada (en inglés, "dpi"; *Dot Per Inch*). Número de puntos que imprime una impresora en cada pulgada; "300 dpi" significa 300x300 puntos en cada pulgada cuadrada.

(3) Uno de los protocolos necesarios para mantener una conexión IP a través de una línea telefónica común. El PPP es necesario para utilizar navegadores gráficos para Internet y es bastante superior al "SLIP", otro protocolo con la misma función.

protocolo: (1) Dícese del estándar utilizado para la transmisión de los datos, especialmente en el caso de redes de computadoras.

(2) Descripción del formato de mensajes y de las reglas que dos computadoras tienen que seguir para poder intercambiar mensajes.

(3) Un conjunto de reglas que especifican el formato, la sincronización, o secuencia y verificación de errores en comunicación de datos. Dos computadoras deben utilizar el mismo protocolo para poder intercambiar información. El protocolo básico utilizado en el Internet es el TCP/IP.

proxy: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad ("firewall" o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

PYME: Pequeñe Y Mediana Empresa.

Q

queue: Cola. Conjunto de paquetes en espera de ser procesados.

R

RDSI: (1) Red Digital de Servicios Integrados, las líneas digitales de teléfono, con caudales típicos de 64 ó 128 Kbps (kilobaudios por segundo).

(2) Red digital de servicios integrados. Tipo de red telemática que ofrece una buena calidad a través de la red telefónica convencional. Para acceder a Internet a través de esta red es necesario un modem RDSI.

ROM: *Read Only Memory*, o Memoria de sólo lectura. Un tipo de memoria "estática", es decir, que no se borra al apagar la computadora y en principio en la que no puede escribirse, salvo que se empleen métodos especiales. Usada sobre todo para guardar la BIOS de la computadora.

router: Dispositivo responsable de la comunicación en una red o entre redes. Una institución, al conectarse a la Internet, instala un *router* para conectar su red local (LAN) al punto-de-presencia más próximo.

S

servidor: (1) En el modelo cliente-servidor, es el programa responsable por atender el servicio solicitado por un cliente. Todos los servicios de Internet, como Archie, *Gopher*, WAIS y WWW funcionan bajo el mismo modelo cliente-servidor. Para utilizar uno de estos servicios, el usuario tiene que usar un programa cliente para acceder al servidor.

(2) Refiriéndose al equipo, o servidor, es un sistema que ofrece recursos tales como almacenamiento de datos, impresión y acceso de discado (dial-up) para los usuarios en la red.

shareware: Una forma de distribución de software, basada en poder probarlo un tiempo antes de decidirnos a comprarlo. No confundir con *freeware* (software gratuito).

Sistema operativo: programa que administra las funciones básicas de una computadora, la cual no podría funcionar sin el.

site: Un servidor de Internet que ofrece servicios a los usuarios. Existen *sites* de FTP, WWW, *Gopher* y otros.

SMTP: *Simple Mail Transfer Protocol*. Conjunto de instrucciones que se utilizan en Internet para la transferencia de mensajes del tipo correo electrónico saliente.

software: Los programas de computadora, la lógica que permite realizar tareas al hardware (la parte física).

SPAM: SPAM es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet.

SSL: *Secure Sockets Layer*. Capa de enlace segura. Es un sistema creado por la empresa Netscape que asegura la privacidad de los datos enviados a través de la red de Internet mediante un navegador de red. Este sistema utiliza un método de encriptación y un certificado de autenticidad que asegura la identidad del servidor de la página.

Switch: ver "hub".

T

TCP/IP: *Transmisión Control Protocol/Internet Protocol*. Familia de protocolos que hace posible la interconexión y tráfico de red de Internet. Los dos protocolos más importantes son los que dan nombre a la familia: IP y TCP.

Telnet: (1) Es un proceso que permite a una computadora hacer una conexión a una computadora remoto y actuar como un terminal de ésta. A través de este servicio es posible escribir en una computadora como si se estuviera conectado directamente.

(2) Servicio de Internet para conectarse de forma remota con otra computadora, como si se hiciera desde un terminal local.

terminador: Pequeño aparato electrónico basado en resistencias eléctricas, usado en redes de cable coaxial para terminar la cadena de computadoras conectadas de forma abierta (sin hacer un anillo).

U

UNIX: (1) Un sistema operativo multiusuario y multitarea.

(2) Sistema operativo interactivo y de tiempo compartido creado en 1969 por Ken Thompson. Reescrito a mitad de la década de los '70 por ATT alcanzó enorme popularidad en los ambientes académicos y, más tarde en los empresariales, como un sistema portátil robusto, flexible y portable, muy utilizado en los ambientes Internet.

upload: Acto de transmitir un documento de la computadora del usuario hacia La Red.

URL: (1) *Universal Resource Locator*. Nombre genérico de la dirección en Internet, Indica al usuario dónde localizar un archivo HTML determinado, en la Web. La mayor parte de los documentos o recursos en Internet (excepto los de E-mail, que tienen sus propias convenciones) pueden ser representados por una URL. Cada URL tiene tres partes - protocolo, nombre y dirección de la máquina remota -, y localización del documento en dicha máquina. Una URL típica suele verse así:
"http://maquina.algunaparte.com/CiertoDirectorio/documento.html".

La primera parte denota el protocolo, en este caso http = *hypertext transport protocol*. Otros protocolos comunes son "ftp: //", "*gopher://*", "*telnet://*", "*news:*" y "mailto:". Note que los protocolos "news:" y "mailto:" son usados sólo por aquellos *browsers* que cuentan con soporte interno para ellos, como Netscape, Mosaic o Explorer.

La segunda parte de la URL es el nombre de la máquina remota en que se localiza el documento o recurso. Puede ser el nombre válido de una máquina, por ejemplo: "www.utw.com", o una dirección IP, como "198.60.58.11".

La última parte de la URL es la ubicación actual del documento o recurso deseado en la máquina remota, y sigue los estándares de denominación de directorios y archivos de dicha máquina, tal como "/~joshua/index.html" para un archivo HTML llamado "index.html", del directorio raíz del usuario en una máquina UNIX.

(2) *Uniform Resource Lodator*. Utilizado para especificar la dirección de un objeto (archivo, grupo de News, etc) en la Red.

(3) En español, Localizador Universal de Recurso. Es el nombre que reciben las diversas cosas e información que se pueden encontrar en la Red: páginas Web (http), archivos (ftp) o grupos de noticias (news). Al escribir el nombre completo de un recurso en este formato, se accede a él, normalmente desde un programa navegador o software específico.

Usenet: Conjunto de los servidores que permiten el intercambio de comentarios por parte de personas con los mismos intereses en los foros de discusión llamados *Newsgroups*.

V

virtual (dispositivo): (1) El que se imita mediante software y las capacidades de los otros dispositivos sí existentes, como por ejemplo un coprocesador matemático imitado por Linux mediante el microprocesador.

(2) Simulación de un dispositivo o periférico de computadora, como una unidad de disco duro o una impresora, que no existe, al menos, no a mano. En una red de área local (LAN), una computadora podría parecer como si tuviera un disco duro de gran capacidad, el que de hecho es accesible a la estación de trabajo mediante las vinculaciones de red con el servidor de archivos.

virus: Pequeño programa que se introduce en una computadora para hacer alguna acción determinada, en principio maligna. Su aparición es anterior a la aparición de Internet, pero la velocidad y la facilidad en el

ámbito territorial que abarca Internet, ha provocado que la red sea un gran vehículo transmisor muy importante. De echo hay virus que solo son operativos desde Internet.

VRML: ***Virtual Reality Modeling Language***. Un lenguaje de diseño usado en Internet para recrear ambientes tridimensionales "visitables" desde el navegador web.

W

WAN: (1) *Wide Area Net*, red de área ancha. Una red de computadoras de muy gran tamaño, dispersa por un país o incluso por todo el planeta.

(2) Siglas para *Wide Area Network*, una red que enlaza computadoras separadas por distancias mayores de un kilómetro.

Web: Es una red mundial de páginas de información de hipertexto, por la que se puede circular mediante un navegador o *browser*.

Whois: Servicio de Internet que permite a los usuarios hacer búsquedas en una base de datos sobre personas y otras entidades de la red, tales como dominios, redes y sistemas centrales, mantenidos en DDN-NIC. La información sobre personas muestra el nombre, la dirección, número de teléfono y dirección electrónica, etc. de la persona encargada de cada red.

WWW: (1) *World Wide Web*, o "gran telaraña mundial". La parte de Internet más conocida y utilizada.

(2) Servidor de información, desarrollado en el CERN (Laboratorio Europeo de Física de Partículas), buscando construir un sistema distribuido hipermedia e hipertexto. También llamado WEB y W3 Existen gran cantidad de clientes WWW para diferentes plataformas.

X

XDSL: El término se refiere a las diferentes variaciones de DSL (*Digital Suscriber Line* o Línea de Usuario Digital), tales como ADSL, HDSL y RADSL.

Z

ZIP: (1) Tipo de archivo comprimido. Muy utilizado, especialmente en Internet, fue ideado por la empresa PKWARE.

(2) Dispositivo de almacenamiento de datos, consistente en una unidad lectora-grabadora y un soporte de datos de forma y tamaño similares a un disquete de 3.5 pulgadas y capacidad 100 MB. Ideado por la empresa Iomega.