5

UNIVERSIDAD NACIONAL
AUTONOMA DE MEXICO.

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN.

"REDES DE COMPUTADORAS: INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR PROXY EN PLATAFORMA LINUX EN UNA *LAN.*"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:

LICENCIADA EN INFORMÁTICA

P R E S E N T A :

MARIBEL GUTIÉRREZ REGALADO.

2-72 15

ASESOR: ING. JESÚS MOISÉS HERNÁNDEZ DUARTE

CUAUTITLAN IZCALLI, EDO DE MEXICO 2000.

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen Garcia Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

"Redes de Computadoras. Instalación y Configuración de un [illegible]"

que presenta la pasante: [illegible]

con número de cuenta: [illegible] para obtener el título de :

[illegible]

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 25 de octubre de 2000.

MODULO	PROFESOR	FIRMA
I	[illegible]	
II	[illegible]	
III	[illegible]	

AGRADECIMIENTOS

A Dios.

Por darme la vida, por permitirme culminar esta etapa tan importante de mi vida y compartir estos momentos tan felices con mis seres queridos.

A mi madre.

Por darme todo su apoyo y comprensión en todo momento, gracias pues este logro tan importante para mí también es suyo. Te quiero

A mi padre.

A la memoria de mi padre, por todo su apoyo y comprensión en todo momento, por sus consejos y regaños, pues aunque ya no estés físicamente conmigo, se que estarás orgulloso de mí en donde te encuentres.

A mí Tía Socorro

Por su apoyo y comprensión en todo momento, por ser mi amiga gracias.

A mi Tío Enrique.

Por estar siempre con nosotras apoyándonos y comprendiéndonos, este logro también es de usted.

A mis hermanas.

Por su apoyo y comprensión en mis momentos de rebeldía, por ser mis amigas y brindarme sus consejos.

A Andrés.

Por apoyarme incondicionalmente y comprenderme, por estar siempre a mi lado compartiendo este logro también es tuyo.

Al Lic. Carlos Pineda Muñoz.

Por apoyarme en todo momento, por ser un gran profesor y amigo.

Al Ing. J. Moisés Hernández.

Por permitirme quitarle un poco de su tiempo para el asesoramiento de este trabajo de investigación y por su ayuda, ya que sin usted nunca hubiera culminado este trabajo.

A Martín Bermúdez.

Por su apoyo incondicional para la culminación de este trabajo, Gracias.

A mis amigos y amigas que siempre han estado conmigo.

A todas aquellas personas que directa o indirectamente me han ayudado en la terminación de este trabajo.

A la Facultad de Estudios Superiores Cuautitlán.

Por haberme permitido culminar mis estudios superiores

A la Universidad Nacional Autóma de México..

Por todo lo que soy se lo debo a ella.

MARIBEL.

INDICE

INTRODUCCION 7

OBJETIVOS 10

1. INTRODUCCIÓN A LINUX

1.1. Descripción del Sistema Operativo 12

1.2. Historia y evolución 14

1.3. Distribuciones de Linux 16

1.4. Características de Linux 19

1.5. Ventajas y desventajas 22

2. INTRODUCCIÓN A LOS SERVIDORES PROXY

2.1. Elementos básicos de Internet 25

2.1.1 El TCP /IP de Internet 26

2.1.2 Direcciones IP 28

2.1.3 Nombres de dominio en Internet 30

2.2. Servidores Proxy 33

2.2.1 Concepto 33

2.2.2 Funciones 35

2.2.3 Servicios que proporciona 35

2.2.4 Como seleccionar un servidor Proxy 36

2.2.5 Requerimientos de hardware y software 37

2.2.6 Ventajas y desventajas de los servidores Proxy 39

2.2.7 Seguridad en los servidores Proxy 40

3. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR PROXY.

3.1. Instalación y configuración del servidor 45

3.1.1 Configuración del protocolo TCP/IP 45

3.1.2 Instalación y configuración del módem o tarjeta de red 47

3.2. Configuración de los clientes 56

3.2.1 Instalación y configuración del protocolo TCP/IP en los clientes 56

3.2.2 Configuración del acceso a Internet 61

3.2.3 Asignación de las direcciones IP a las estaciones de trabajo 65

3.2.4 Comprobación de la instalación y configuración del protocolo TCP/IP 66

3.3. Configuración del socket 67

3.3.1 El archivo de control de acceso(sockd.conf) 67

3.3.2 El archivo de ruteo(socks.conf) 68

3.4. Configuración del servidor Proxy 70

3.5. Configuración del cliente 72

3.6. Configuración de las aplicaciones 73

3.7. Configuración del *firewalls* (pared cortafuegos) 74

4. Conclusiones 79

5. Apéndice 1 80

6. Apéndice 2 83

7. Bibliografía 84

INTRODUCCIÓN.

Internet es una red que engloba una serie de redes de computadoras con la finalidad de permitir un intercambio libre de información entre sus usuarios. Desde que aparecieron más aplicaciones como los buscadores, el chat y el correo electrónico entre otros, el número de usuarios que acceden a esta red global se incrementa día a día, por lo cuál los patrones de tráfico han cambiado.

Esta red mundial permite que cualquier computadora se conecte a ella, sin importar con que dispositivos de hardware y software cuente. Este proceso lo logra mediante el uso del protocolo TCP/IP, cuya función principal es permitir la comunicación entre distintos protocolos de comunicación.

El TCP/IP es el protocolo utilizado con mayor frecuencia en el acceso a Internet. Este protocolo funciona de la siguiente forma: divide los datos en partes, llamados paquetes, a los cuales les da un número individual por paquete. Estos paquetes pueden representar texto, imágenes, sonido o gráficas. Cada paquete contiene la información que se va a enviar y la información que el protocolo necesita para hacerlo funcionar, el cuál se denomina protocolo de encabezado.

El acceso a Internet es cada vez más lento, debido a que en la actualidad existe mucho tráfico en la red, ya que día con día aumenta el número de usuarios a esta biblioteca mundial. Por tal razón es necesario optimizar las direcciones IP en el acceso a Internet, y una forma de hacerlo es mediante la instalación de un servidor Proxy.

La función original de los proxies es la seguridad. Sin embargo no es su única función, también se instalan en servidores de Internet, ya que también pueden ayudar a controlar el tráfico de la red.

En base a lo anterior el enfoque que se le da a este trabajo no es el de seguridad, sino el de acceso controlado a Internet. Esto es, los equipos que se encuentran detrás del proxy sólo son clientes de Internet, por lo que no requieren de características de seguridad; lo que si requieren es que la dirección IP que se asigne a cada uno de ellos pertenezca a la subred de clase "C" , debido a que este tipo de direcciones se utiliza en las intranets.

La presente propuesta se planteó con el propósito de optimizar las direcciones IP con las que cuenta el dominio ***cuautitlan2***, el cuál fue asignado a la Facultad de Estudios Superiores Cuautitlán Campo 4 (FES-C4), por la Dirección General de Servicios de Computo Académico(DGSCA).

En la actualidad el dominio Cuautitlán2 ya rebasó su límite de direcciones IP, las cuales han sido asignadas a cada una de las dependencias que conforman esta entidad, por tal motivo se planteó la instalación y configuración de un Servidor Proxy. Esto traerá como consecuencia, que por medio de una intranet se tenga acceso a los servicios de Internet. De esta forma se contará con más direcciones IP disponibles para otras necesidades prioritarias.

El servidor proxy se instalará en el laboratorio de computo de la Licenciatura en Informática, este se encuentra ubicado en la FES-C4. La instalación de este servidor se hará con la finalidad de optimizar las direcciones IP con las que cuenta el área, además de que permitirá la agilización de los accesos a Internet.

Por otra parte la plataforma con la que trabajará el proxy será Linux, ya que no necesita ningún tipo de licencia para su uso y no tiene ningún costo, además de que posee ciertas características flexibles de red, en comparación con otros sistemas operativos; lo cuál facilita la instalación del proxy.

En el presente trabajo de investigación se habla sobre la instalación y configuración de un servidor Proxy sobre plataforma LINUX en una red LAN; solución con la cuál se optimizan las direcciones IP en el acceso a Internet. El trabajo consta de tres capítulos.

En el primer capítulo, se describe el sistema operativo LINUX, su origen y evolución, sus características, las distribuciones más importantes de este Sistema Operativo, así como las ventajas y desventajas que presenta como plataforma para redes.

En el segundo capítulo se presentan los elementos básicos de Internet, se describen el TCP/IP de Internet, las direcciones IP y los nombres de dominio. Se toca el tema de los servidores Proxy, ¿que son?, ¿cuales son sus funciones?, ¿que servicios proporcionan?, ¿como se seleccionan? y las partes por las cuales esta conformado; las ventajas y desventajas que proporcionan este tipo de servidores. Otro punto también importante que se menciona es la seguridad en Internet, por medio del contrafuegos.

En el tercer capítulo se describen los pasos fundamentales para la instalación y configuración de un servidor Proxy en una LAN, se mencionan la instalación y configuración del Protocolo TCP/IP en el servidor y en los clientes, la instalación del módem o tarjeta de red, la configuración del acceso a Internet, la asignación de las direcciones IP, la configuración de los archivos de control de acceso y de ruteo, la configuración de las aplicaciones y del cortafuegos.

Por último se incluyen dos apéndices: el primero incluye el glosario de los términos empleados en este trabajo y el segundo contiene un índice de figuras.

OBJETIVOS

GENERAL:

- Optimizar la utilización de las direcciones IP en el acceso a Internet por medio de la instalación y configuración de un Servidor Proxy en plataforma LINUX en una LAN.

ESPECÍFICOS:

- Definir el Hardware necesario para la implementación de un Servidor Proxy.
- Definir el Software necesario para la implementación de un Servidor Proxy.
- Identificar los beneficios que ofrece LINUX como Sistema Operativo de un Servidor Proxy.
- Identificar las ventajas y desventajas que proporcionan los Servidores Proxy en el acceso a Internet.

CAPITULO I.

INTRODUCCIÓN A LINUX.

1.1 DESCRIPCION DEL SISTEMA OPERATIVO.

Uno de los sistemas operativos más importantes dentro de la historia de la informática moderna ha sido Unix, el cuál es un sistema operativo que se inventó a finales de la década de los 70; en los laboratorios de Bell, una empresa americana de telecomunicaciones.

LINUX, es un sistema Unix para PC's con la peculiaridad de que es 'libre'. Es un sistema operativo que es compatible con Unix. Tiene dos características muy particulares que lo diferencian del resto de los sistemas Operativos que podemos encontrar en el mercado. La primera: es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, y la segunda, es que el sistema viene acompañado del código fuente, lo cuál significa que el usuario es libre de adecuarlo a sus necesidades sin problemas, siempre en función de sus conocimientos y bajo su responsabilidad.

Con el software libre no suele ir sólo el ejecutable (binario) del programa, sino que éste va acompañado del código completo del mismo en el lenguaje de programación en el que se escribió, con el propósito de modificarlo libremente, en base a los conocimientos y necesidades específicas de cada usuario, la finalidad del software libre es que cada usuario publique dichas modificaciones por el bien de la comunidad interesada en el área informática.

El sistema esta formado por el núcleo del sistema (kernel) más un gran número de programas y bibliotecas de funciones que hacen posible su utilización.

LINUX se distribuye bajo la GNU Public License (Licencia Pública GNU), por lo tanto, el código fuente tiene que estar siempre accesible. Este sistema ha sido diseñado y programado por una multitud de desarrolladores alrededor del mundo.

El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa.

Día a día, más y más programas y aplicaciones están disponibles para este sistema, y la calidad de los mismos aumenta de versión a versión. La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen gratuitamente bajo los términos de licencia de la GNU Public License.

En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir sus productos para LINUX y la presencia del mismo en empresas aumenta rápidamente por la excelente relación entre la calidad y el precio que se consigue con LINUX.

Las plataformas en las que se puede utilizar LINUX son 386-, 486-. Pentium, Pentium Pro, Pentium II, Amiga y Atari, también existen versiones para su utilización en otras plataformas, como Alpha, ARM, MIPS, PowerPC y SPARC.

En la actualidad, este sistema operativo es utilizado por miles de usuarios para desarrollo de software, redes y como plataforma de usuarios finales. De entre los miles de sistemas operativos alternos que existen, Linux a pesar de ser una plataforma joven, se ha convertido en una opción interesante, independientemente de que esta venga de Unix.

El núcleo de LINUX no usa código de AT&T o de cualquier otra fuente propietaria, la mayoría de los programas disponibles para LINUX son desarrollados por el proyecto GNU(Licencia Pública General) de la Free Software Foundation(Fundación de Software Libre),en Cambridge, Massachusetts.

Este Sistema está disponible en Internet en cientos de servidores FTP y en distribuidores en discos CD-ROM de revendedores que lo ofrecen empacado con manuales e información que es realmente la que cuesta porque el software es libre(gratuito). El núcleo del LINUX está legalmente protegido por la licencia publica GNU (GPL).

LINUX incluye compiladores, ensambladores, debuggers, editores de texto, paquetes de email, lectores de noticias, navegadores, servidores y programas para la creación y edición gráfica, maneja los archivos de forma jerárquica al igual que el DOS, la diferencia es que el DOS está diseñado para procesadores x86, que no soportan verdaderas capacidades para múltiples tareas.

1.2 HISTORIA Y EVOLUCIÓN.

LINUX surgió a principios de la década de los noventa, para ser exactos en el año 1991; en aquel año un estudiante de informática de la Universidad de Helsinki, llamado Linus Benedict Torvalds empezó a programar las primeras líneas de código de este sistema sin imaginarse a lo que llegaría este proyecto.

El comienzo de este sistema operativo estuvo basado en MINIX, el cuál es un pequeño sistema Unix, que fue desarrollado por Andy Tanenbaum. Las primeras discusiones sobre LINUX fueron en el grupo de noticias comp.os.minix, en estas discusiones se hablaba sobre el desarrollo de un pequeño sistema Unix para usuarios de Minix que querían más.

En agosto de 1991, Linus Torvalds terminó la primera versión del kernel de Linux, sin embargo nunca la dio a conocer ya que esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que los usuarios tenían acceso a un sistema Minix para su compilación.

La primera versión oficial de Linux se dio a conocer el 5 de octubre de 1991. Con ésta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C), pero funcionaban más elementos en el sistema. En esta etapa de desarrollo ni se pensaba en los términos de soporte, documentación y distribución.

Después de la versión 0.03, Linus salto en la numeración hasta la 0.10. Posteriormente a esta versión surgieron más y más programadores a lo largo y ancho de Internet, que empezaron a trabajar en el proyecto y después de sucesivas revisiones, Linus incrementó el número de versión hasta la 0.95 la cuál se dio a conocer en Marzo de 1992.

Después de algún tiempo casi más de un año en diciembre de 1993 el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 surgió hasta el 14 de marzo de 1994. La versión actual del núcleo es la 2.2 y sigue avanzando día a día con el objetivo de perfeccionar y mejorar el sistema. Dicha versión soporta muchos más periféricos, desde procesadores hasta joysticks, sintonizadores de televisión, CD ROMs no ATAPI y reconoce una buena cantidad de tarjetas de sonido. También incluye soporte para tipos de archivos para Macintosh HFS, Unix UFS y en modo de lectura, HPFS de OS/2 y NTFS, de NT.

1.3 DISTRIBUCIONES DE LINUX.

En realidad Linux, sólo es el kernel del Sistema Operativo(el núcleo del sistema). Este kernel es el que controla el funcionamiento del sistema. Sin embargo todos los sistemas operativos necesitan todo un conjunto de utilidades y herramientas de instalación, configuración y uso. Es aquí en donde juegan su papel las diferentes distribuciones. Todos los programas que corren por encima de este sistema, vienen de otras fuentes. La mayor fuente de este tipo fue y sigue siendo el proyecto GNU(GPL), del cuál se han aportado casi la totalidad de sus programas a Linux.

La figura 1 muestra los componentes del sistema operativo Linux.

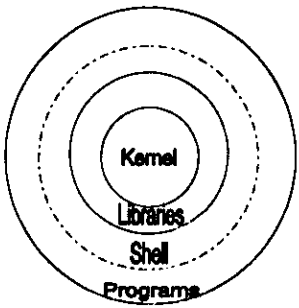

Figura 1. Componentes del S.O. Linux.

Linux es un proyecto en constante desarrollo y las nuevas versiones de su kernel(núcleo), estarán disponibles para el público en general, sean estables o no. Sin embargo existen ciertas características en el número de versión que ayudan a diferenciar si es o no estable. Las versiones x.y.z, en donde "y" sea par, son versiones estables, y el incremento en "y" indica que hubo alguna corrección de errores. Por ejemplo de la versión 1.2.2 a la versión 1.2.3 sólo hubo corrección de errores. Las versiones x.y.z en donde "y" es impar son versiones preliminares o versiones beta que se encuentran bajo prueba y que son usados sólo con fines de pruebas Por ejemplo: versión 1.3.3, 2.3.5. La versión estable del kernel es la 2.2 y sé esta esperando la versión 2.4.

El sistema operativo Linux no cuenta con una versión estándar única de este Sistema. Existen varias distribuciones sobre este sistema Operativo, ya que como este software es libre cada usuario hace las modificaciones que requiere de acuerdo a sus necesidades y después las pone a disposición del público en general. Por esta razón existen varias distribuciones de Linux, y cada una de ellas cuenta con su documentación e instalación propia. Algunas de las distribuciones más comunes son:

Slackware

Es una de las distribuciones más extendida en todo el mundo y la más conocida en España. Fue creada por Patrick J. Volkerding el 28 de septiembre de 1994, su actualización es muy fácil, además esta distribución incluye una gran cantidad de software como X-Window, TeX, y otros. Dicha distribución consiste en un juego de disco, cada uno contiene un tipo particular de software (por ejemplo, el disco d contiene las herramientas de desarrollo tales como el compilador GCC, y así sucesivamente). La instalación de los discos puede hacerla de la forma que más convenga. Slackware es fácil de instalar.

Red Hat

Creada por Red Hat Software, en Connecticut, EE.UU. Una de sus ventajas es el atractivo sistema de instalación (en modo gráfico) y el cómodo mantenimiento de componentes de software, lo que facilita enormemente las frecuentes actualizaciones. Se puede obtener tanto gratuitamente en la red como adquiriendo el CD-ROM correspondiente.

Otras empresas comercializan también sistemas basados en Red Hat, como Caldera Inc. y Pacific Hi-Tech. Aún poco conocida, sobre todo para principiantes. Dicho sistema de gestión de componentes de software es obra suya.

Pero lo han ofrecido con carácter abierto y gratuito a los demás desarrolladores bajo la licencia de GNU, por lo que es previsible que en el futuro otros muchos asuman este sistema en sus propias distribuciones, lo que facilitará enormemente las actualizaciones. Los creadores de esta distribución se encuentran en **http://www.redhat.com.**

Debian

Es una organización sin ánimo de lucro con miles de colaboradores a lo largo del mundo. Esta es la distribución preferida de los puristas del Software Libre, pues su política de inclusión de aplicaciones en su distribución exige que sea una aplicación totalmente libre, preferiblemente sujeta a las licencias GPL ó LGPL. Además, es la distribución que incluye el mayor número de paquetes en la misma. Esto puede llegar a ser un poco pesado a la hora de seleccionarlos en la instalación.

La Free Software Fundation (FSF) es bien conocida entre los usuarios de software gratuito para Unix. Son los creadores del sistema **GNU**, su futuro es Unix gratuito. Ya hay mucho material pero no un sistema operativo completo, así que mientras tanto ofrecen un Unix integrado por el núcleo de Linux y el software de GNU. Está distribución se encuentra en **http://www.debian.org.**

S.U.S.E.

Esta distribución alemana es la mayor distribución europea, y se caracteriza por su facilidad de instalación y su inclusión del entorno gráfico de usuario de base.

Caldera Open

Esta distribución recientemente ha adoptado a Debian como distribución base, para añadirle una serie de mejoras en el proceso de instalación para el usuario novato; como procesadores de texto (Worperfect 8.0, StarOffice 5.1), aplicaciones comerciales para Linux y una larga serie de mejoras para atraer a los que aún no han instalado Linux y se siente un poco frustrados por la aparente complejidad del proceso de instalación.

1.4 CARACTERÍSTICAS DE LINUX

Las dos características principales y sobresalientes de este sistema operativo son: el de ser un multitarea y multiusuario.

Al mencionar que es multitarea, se refiere a que puede realizar una serie de procesos al mismo tiempo. Este utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que están siendo utilizados en un determinado momento serán ejecutados, siendo el sistema operativo el encargado de ceder tiempo de microprocesador a cada programa. Con el hecho de ser multiusuario, permite que la computadora pueda ser utilizada por más de un usuario, con el propósito de compartir recursos, tales como archivos, impresoras y espacio en disco por mencionar algunos.

Estas son las dos características principales que hacen que Linux sea un sistema flexible y potente, que ofrece a los usuarios una serie de ventajas, en comparación con otros sistemas operativos menos complejos. Además de que es un sistema operativo completamente de 32 bits, lo que proporciona un rendimiento sobresaliente.

Entre otras características básicas importantes se encuentran las siguientes:

- Multiplataforma: Corre en muchas plataformas, no solo en Intel.
- Multiprocesador: Es decir cuenta con soporte para sistemas con mas de un procesador esta disponible para Intel y SPARC.
- Funciona en modo protegido 386.
- Tiene capacidad para ejecutar aplicaciones dos mediante un emulador llamado DOSEMU:
- Carga de ejecutables por demanda: LINUX sólo lee del disco aquéllas partes de un programa que están siendo usadas actualmente.
- Compatible con POSIX, System V y BSD a nivel fuente.
- Pseudo-terminales (pty's).

- Política de copia en escritura para la competición de páginas entre ejecutables; esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: a una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha. Un total de 16 zonas de intercambio de 128 Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2 Gb para intercambio. Este límite se puede aumentar fácilmente con el cambio de unas cuantas líneas en el código fuente.
- La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta puede a su vez ser reducida cuando se ejecuten grandes programas. Contiene librerías compartidas de carga dinámica (DLL's) y librerías estáticas.
- Se realizan volcados de estado (core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.
- Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente.
- Emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática. Cualquier máquina que ejecute LINUX parecerá dotada de coprocesador matemático.

  Por supuesto, si la computadora ya tiene una FPU (unidad de coma flotante), esta será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

- Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de vídeo). Se crean dinámicamente y puedes tener hasta 64.
- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no es necesario ningún comando especial para usar la partición MS-DOS, este parece un sistema de archivos normal de Unix (excepto por algunas restricciones en los nombres de archivo y permisos).
- Soporta otros protocolos diferentes al TCP/IP para las comunicaciones, aunque el TCP/IP es el más usado.
- Es un sistema operativo seguro ya que no existe ningún virus que represente una amenaza para Linux, ya que los virus creados para Windows y programas que trabajan en este, no pueden ser ejecutados en Linux, lo cuál permite que la información se encuentre a salvo.
- Los métodos de seguridad de Linux son mejores que los de otros sistemas operativos, por lo que es menos probable que se filtren Hackers o que fluya información fuera de su PC sin su autorización. En Linux el acceso a los directorios y los archivos, así como la capacidad de borrar o modificar estos, depende de los permisos de usuario que estos tengan.
- Soporta los teclados de la mayoría de los países, con sus acentos y es fácil añadir nuevos.
- Un modo llamado ***UMSDOS*** permite a linux instalarse en una partición DOS normal.

1.5 VENTAJAS Y DESVENTAJAS.

Linux es un sistema operativo estable, confiable y robusto. Está echo para poder trabajar las 24 horas del día todos los días del año, e incluso durante varios años sin sufrir colapso.

Este sistema al igual que los demás sistemas operativos cuenta con ventajas y desventajas. Entre algunas de sus ventajas podemos encontrar las siguientes:

1. Estabilidad; éste sistema no se traba a cada rato.
2. Seguridad, es mucho más seguro que otros Sistemas Operativos.
3. Compatibilidad, reconoce la mayoría de los otros sistemas operativos en una red.
4. Velocidad, es mucho más veloz para realizar las tareas.
5. Posee el apoyo de miles de programadores a nivel mundial.
6. Es ideal para la programación, ya que se puede programar en LINUX para distintas plataformas.
7. Se puede usar en casi cualquier computadora, desde una 386.
8. Puede manejar múltiples procesadores. Incluso hasta 16 procesadores.
9. Libre de virus, aún no se conoce ningún virus para LINUX.
10. Maneja discos duros de hasta 16 TeraBytes.
11. Se consiguen parches con facilidad, además de ser gratuitos.
12. Los fabricantes de Hardware le están dando su apoyo, como IBM y COMPAQ.
13. Vendedores y desarrolladores implementan un sistema de certificación para LINUX.
14. La corporación DATA Internacional predice que el crecimiento de este programa será de la orden de un 25 por ciento anual en el nuevo milenio.

Este sistema posee muy pocas desventajas, de entre éstas se puede hacer referencia a las siguientes:

1. No cuenta con una empresa que lo respalde, por lo que no existe un verdadero soporte.
2. Corre el riesgo de llegar a fragmentarse como fue el caso de Unix.
3. Se necesita algo de experiencia y algunos conocimientos básicos de Unix para poder configurarlo adecuadamente, sobre todo lo relacionado con multimedia y redes. Pero una vez configurado correctamente, utilizando un ambiente gráfico de ventanas, como Gnome o KDE, bajo X Window, es sumamente sencillo de utilizar, tanto como lo es Windows.
4. Los gráficos 3D presentan un pobre desempeño sobre esta plataforma.

CAPITULO II.

INTRODUCCIÓN A LOS SERVIDORES PROXY.

2.1 ELEMENTOS BASICOS DE INTERNET.

Internet es en realidad, un conjunto de redes independientes (de área local y área extensa) que se encuentran conectadas entre sí, permitiendo el intercambio de datos y constituyendo por lo tanto una red mundial que resulta el medio idóneo para el intercambio de información, distribución de datos de todo tipo e interacción personal con otras personas.

La gran rapidez con la que Internet se ha expandido y popularizado en los últimos años, ha supuesto una revolución muy importante en el mundo de las comunicaciones, llegando a causar cambios en muchos aspectos de la sociedad.

Internet esta formada por aproximadamente veinte millones de usuarios y cuatro millones de computadoras conectadas en todo el mundo, con equipos y sistemas operativos tan diferentes como Winx, Macintosh, OS/2, MS- DOS y UNIX por mencionar algunos, comunicándose de forma transparente por medio de el protocolo TCP/IP.

Durante mucho tiempo, el uso comercial de Internet estuvo limitado, debido a que la red estaba sostenida casi en su totalidad por fondos gubernamentales y a que su propósito era estrictamente académico. En la actualidad las políticas que restringen el uso de la red han empezado a cambiar, lo cual es benéfico para los pequeños negocios que no cuentan con los recursos necesarios para mantener una red nacional privada como lo hacen las grandes corporaciones. Esto ha permitido la reducción de costos, por lo cuál actualmente cualquier persona puede comprar este servicio a precios accesibles.

El enorme crecimiento que ha tenido Internet en los últimos años se debe en gran parte a que es una red basada en los fondos gubernamentales de cada país que forma parte de Internet, lo que permite que se proporcione un servicio prácticamente gratuito.

A principios de 1994 comenzó a un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

El Internet crece aceleradamente, por lo cuál sus canales de comunicación mejoran constantemente, con el propósito de aumentar la rapidez de envío y recepción de datos. Cada día que pasa se publican en la red miles de documentos nuevos, y se conectan por primera vez miles de personas.

Con relativa frecuencia aparecen nuevas posibilidades de uso de Internet, y constantemente se están inventando nuevos términos para poder entenderse en este nuevo mundo que no para de crecer.

En la actualidad Internet presenta un crecimiento mensual del 20%, el número de máquinas conectadas se ha venido duplicado año con año desde 1988, y se espera en un futuro no tan lejano sea mucho mayor su expansión. Este crecimiento que se ha venido dando en Internet es tanto en recursos como en el número de usuarios.

2.1.1 EL TCP/IP DE INTERNET.

TCP/IP son las siglas de "Transmission Control Protocol / Internet Protocol". Éste es el lenguaje establecido para la Red Internet. Antes de su creación, este protocolo tuvo mucho éxito en máquinas con UNIX.

TCP/IP no es un único protocolo, en realidad lo que se conoce con este nombre, es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

El TCP/IP es el protocolo común utilizado por todas las computadoras que son conectadas a Internet, de manera que éstas puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectadas redes de clases muy diferentes y con dispositivos de hardware y software que en muchos casos son incompatibles, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, ya que este se encarga de que la comunicación entre todos sea posible, en virtud a que es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

La principal característica del TCP/IP, es que establece la comunicación por medio de paquetes de información. Cuando un servidor quiere mandar a otro un archivo de datos, lo primero que hace es partirlo en trozos pequeños (alrededor de unos 4 Kb) y posteriormente enviar cada trozo por separado. Cada paquete de información contiene la dirección en la Red donde ha de llegar y también la dirección de remite por si hay que recibir respuesta.

Los paquetes viajan por la Red de forma independiente. Entre dos puntos de la Red suele haber muchos caminos posibles, cada paquete escoge uno dependiendo de factores como saturación de las rutas o posibles atascos; de este modo, encontramos normalmente situaciones como que parte de un archivo que se envía desde EE.UU. hasta España pase por cable submarino hasta el Norte de Europa y de allí hasta España, y otra parte venga por satélite directamente a Madrid. Esta importante característica permite que Internet sea la red más estable del Mundo. Al ser una red tan grande y compleja existen cientos de vías alternativas para un destino concreto. Así aunque fallen algunos servidores intermediarios, o no funcionen correctamente algunos canales de información siempre existe comunicación entre dos puntos de la Red.

Otra notable y muy positiva consecuencia del uso de este protocolo es que admite la posibilidad de que algún paquete de información se pierda por el camino. Puede ocurrir que una computadora intermediaria se apague o se sature justo cuando un

trozo de un archivo que estemos enviando o recibiendo pase por dicho computadora. En algunos servicios de Internet, como el FTP, esto no es un problema, puesto que automáticamente se vuelve a pedir el envío del paquete perdido, para que el archivo solicitado llegue a su destino íntegramente.

Sin embargo, en otros servicios como es la Navegación por la World Wide Web, la pérdida de uno de estos paquetes implica que en nuestras pantallas no aparezca una imagen o un texto en el lugar donde debería estar. De todos modos, siempre existe la posibilidad de volver a solicitar dicha información.

Este punto, más que una ventaja podría parecer un inconveniente; sin embargo no es así, puesto que es mejor que se pierda un pequeño porcentaje de la información a transferir, a que se pierda toda por un corte de la red. Como el TCP/IP funciona basándose en paquetes, siempre queda abierta la posibilidad de volver a solicitar el paquete perdido, y completar la información sin necesidad de volver a transferir todo el conjunto de datos.

2.1.2 DIRECCIONES IP

Cada computadora que se conecta a Internet se identifica por medio de una dirección IP. Las direcciones IP permiten que el envío de datos entre computadoras se haga de forma eficaz. Estas direcciones contienen 32 Bits, esta formada por cuatro campos de 8 bits los cuáles se encuentran separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255.

Es importante señalar que no está permitido que coexistan en la Red dos computadoras distintas con la misma dirección IP, puesto que de ser así, la información solicitada por uno de los clientes no sabría a cual de ellos dirigirse.

Las direcciones IP están compuestas de una dirección de red, seguida de una dirección de subred y de una dirección de host.

La dirección de Internet se utiliza para identificar tanto a la computadora en concreto como la red a la que pertenece, de manera que sea posible distinguir a los computadoras que se encuentran conectadas a una misma red. Con este propósito y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se han establecido cinco subclases diferentes de direcciones, las cuáles representan cinco rangos de valores.

Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red, esto significa que podrán existir más de dieciséis millones de computadoras en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPANET es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de ***clase A***. Lo normal para las grandes organizaciones es que utilicen una o varias redes de ***clase B***.

Clase B: Estás direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso, el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.

En caso de que el número de computadoras que se necesita conectar fuese mayor, sería posible obtener más de una dirección de ***clase B***, evitando de esta forma el uso de una de ***clase A***.

Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores, este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254.

De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadoras en cada red. Esté tipo de direcciones permite un menor número de host que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Clase D: En esta clase se reservan todas las direcciones para multidestino, es decir una computadora transmite un mensaje a un grupo especifico de computadoras de esta clase. Las direcciones están comprendidas entre 224.0.0.0 y 239.255.255.255

Clase E: Esta clase se utiliza únicamente con fines experimentales. Las direcciones se encuentran comprendidas entre 240.0.0.0 y 247.255.255.255.

2.1.3 NOMBRES DE DOMINIO EN INTERNET

Mejor conocido como DNS, este sistema opera en todos los países que se encuentran conectados al Internet. Cuando se formaban las primeras redes, a mediados de los 70, todas las máquinas tenían una dirección numérica conocida como Dirección IP, así si uno deseaba conectarse a x máquina, se le llamaba por su dirección IP y como eran muy pocas, resultaba sencillo saber de memoria el número de dirección IP. Sin embargo, con el crecimiento exponencial del Internet se volvió cada vez más difícil entrar x ó z servidor, razón por la cuál se crea el DNS, y es por medio de este que se pueden asignar direcciones con letras, esto provocó que fuera más fácil accesar a algún servidor.

Un usuario de Internet, no necesita conocer ninguna dirección IP para accesar a algún servidor, ya que estas direcciones las manejan las computadoras en sus comunicaciones por medio del Protocolo TCP/IP de manera invisible para el usuario. Sin embargo, se necesita nombrar de alguna manera a los servidores de Internet, para poder elegir a cual pedir información. Esto se logra por medio de los Nombres de Dominio.

Los nombres de dominio, son la traducción para los usuarios de Internet de las direcciones IP, las cuales son útiles sólo para los servidores. Así por ejemplo, Altavista.com e infosel.com, son nombres de dominio. Los nombres de domino son palabras separadas por puntos, en vez de números como en el caso de las direcciones IP. Estas palabras nos dan la idea del servidor al que nos estamos refiriendo.

Es importante resaltar que no todos las computadoras conectadas a Internet tienen un nombre de dominio. Sólo tienen un nombre de dominio aquellas que reciben numerosas solicitudes de información, o sea, las que son servidores; las computadoras cliente, es decir los que consultan por Internet, no necesitan un nombre de dominio, puesto que ningún usuario de la Red va a solicitarles información.

El número de palabras en el nombre de dominio no es fijo. Pueden ser dos, tres, cuatro, ó más. Normalmente se usan sólo dos. En Estados Unidos la última palabra del nombre de dominio representa que tipo de organización posee el servidor al que nos referimos.

Para organizar el DNS, esté se dividió en dominios que facilitan aún más el entrar a alguna dirección, los de nivel superior y de nivel geográfico, cada país es el encargado de asignar estos dominios y en general siguen el mismo estándar.

DOMINIOS DE NIVEL SUPERIOR.

En México la INTERNIC es la organización responsable de dar de alta las direcciones de Internet y ha establecido los siguientes dominios de nivel superior:

Dominios	Descripción
.edu.mx	Para instituciones de educación o investigación
.org.mx	Para asociaciones no lucrativas en México
.net.mx	Para proveedores de servicios de Internet localizados en México
.gob.mx	Para instituciones gubernamentales en México
.com.mx	Para entidades comerciales.

DOMINIOS DE NIVEL GEOGRÁFICO.

Cada país con acceso al Internet se encarga de administrar sus direcciones en el Internet, en la mayoría de los cuales se administran los de nivel superior y los de nivel geográfico cada país los asigna. Es común encontrar direcciones que no contiene nivel superior, esto debido a que en ese país no se administran dominios de nivel superior un ejemplo de estos países es España.

Los siguientes países utilizan las siguientes direcciones geográficas:

País	Dirección de nivel geográfico
Chile	.cl
Japón	.jp
New Zeland	.nz
México	.mx
Yugoslavia	.yu
Francia	.fr

Por lo tanto, con sólo ver la última palabra del nombre de dominio, se puede averiguar donde está localizado el servidor al cuál nos referimos. Cada país administra sus propias políticas para la asignación de dominios de nivel superior, pero en general se utilizan las mismas políticas.

2.2 SERVIDORES PROXY.

2.2.1 CONCEPTO

El filtrado y la autenticación son herramientas de suma importancia para mejorar la seguridad en una red, sin embargo estos dejan algunos gaps(huecos), los cuales se pueden cerrar haciendo uso de un servicio proxy. Este servicio es una aplicación que se instala en una única computadora de la red local, y que permite que varias computadoras conectadas a una misma red local puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea, además permite a los administradores tomar decisiones con respecto a la autorización o inhabilitación de algunos comandos usados por esta aplicación.

La aplicación proxy se puede instalar en un servidor dedicado o no dedicado. Un servidor Proxy es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los proxies se utilizan con frecuencia como sustitutos de los routers controladores del tráfico, para prevenir el tráfico que pasa directamente entre las redes. La figura 2 muestra cómo funciona el servidor proxy en la red privada.

Los servidores Proxy se instalan en servidores de Internet y realizan varias funciones como controlar el tipo de tráfico que fluye a través de la red, además supervisa la seguridad en la red, por mencionar algunas. La principal ventaja que proporcionan este tipo de servidores, es la velocidad de transmisión al no tener que buscar nuevamente las paginas ya visitadas en Internet. Los proxies aumentan de forma considerable la velocidad con la que se navega en Internet.

Los proxies contienen logines auxiliares y soportan la autenticación de usuarios. Un Proxy debe entender el protocolo de la aplicación que esta siendo usada, aunque también puede implementar protocolos específicos de seguridad. El servidor Proxy dará servicio a todas las terminales de la red sin importar con cuál sistema operativo cuente la terminal(unix, windowsx, linux, etc). Esto es posible, en virtud a que el protocolo TCP/IP permite la interconexión de redes y sistemas heterogéneos.

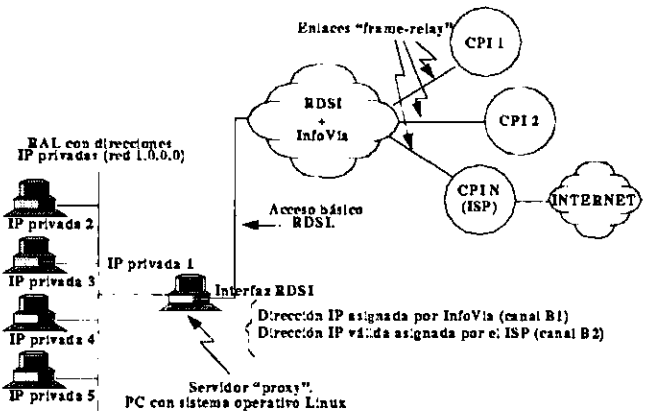

Figura 2. Funcionamiento del Servidor Proxy.

Los servidores Proxy son un elemento fundamental en la creación de una intranet de bajo costo.

Los servidores proxy permiten el ahorro de dinero, líneas telefónicas adicionales, módem, cuentas de acceso a Internet, llamadas telefónica simultaneas, además del ahorro de ancho de banda mediante el almacenamiento en disco de páginas ya visitadas.

2.2.2 FUNCIONES DE UN SERVIDOR PROXY

Los servidores Proxy se instalan en servidores de Internet y estos realizan una serie de funciones, entre éstas se encuentran el control del tráfico que fluye a través de la red, además de supervisar la seguridad en la red ya que actúa como cortafuegos, impidiendo que desde Internet se pueda accesar a la red privada. Además, actúa como un cache de paginas web, ya que son capaces de almacenar en memoria las páginas web visitadas por los usuarios y de esta manera, si algún otro u otros usuarios que quieren visitar alguna pagina que el servidor Proxy tenga guardada, de manera inmediata se le envía al usuario y no es necesario acceder nuevamente a Internet.

2.2.3 SERVICIOS QUE PROPORCIONA UN SERVIDOR PROXY

Un servidor Proxy proporciona a los puestos de una red, los mismos servicios que éstos puestos de trabajo de la red local tendrían disponibles, si estuviesen directamente conectados a Internet a través de un módem.

Al instalar un servidor Proxy en una red local, será posible que desde cualquier estación de trabajo de la red local se puedan tener los siguientes servicios:

- Compartir una sola línea telefónica, un único modem, y una única cuenta de conexión a Internet de manera simultánea entre todos los puestos de trabajo de la red local.
- Navegar por Internet accediendo a paginas web.
- Escribir correos
- Recibir correos electrónicos
- Conectarse a servidores de noticias.
- Conectarse a computadoras que sean compatibles con telnet.
- Conectarse a servidores de Chat
- Conectarse a servidores Gopher

Un servidor Proxy en un sola computadora de una Red Local equivale, a una conexión a Internet en cada una de las estaciones de trabajo que conforman a la red local.

Además un servidor proxy proporciona seguridad, ya que actúa como cortafuegos impidiendo que desde Internet se pueda tener acceso a los servidores y estaciones de trabajo de la red local desde la cuál sé esta accediendo a Internet.

Los servidores proxy avanzados proporcionan la optimización del ancho de banda de su conexión a Internet, además disponen de un cache que almacena en disco las paginas Web que se han consultado por cualquier usuario de la red local.

2.2.4 COMO SELECCIONAR UN SERVIDOR PROXY

Para hacer la selección de un servidor Proxy, se deben valorar una serie de aspectos técnicos y complejos, aspectos relacionados con la instalación como: la facilidad de la instalación, la facilidad para obtener el software para la configuración del servidor, así como la solidez y experiencia del fabricante del servidor.

Un factor importante a considerar a la hora de seleccionar un servidor Proxy, es la plataforma sobre la cuál se va a instalar esta aplicación, esta plataforma puede ser windows x, Unix, o Linux. Las características de hardware con el que debe contar el servidor, son factores importantes en virtud, a que el requerimiento de hardware debe de evaluarse en relación con la plataforma a utilizar, debido a que existe hardware que ha sido diseñado especialmente para ser utilizado únicamente por la plataforma windows.

Otro aspecto importante a considerar, son los protocolos de Internet que puede manejar y si es capaz de realizar caché de las páginas web que se visitan, lo cual es de suma importancia para mejorar el rendimiento de los accesos a Internet, los cuales siempre son lentos, sobre todo cuando son varios los clientes que acceden simultáneamente a la web
Al seleccionar la plataforma se tienen que tomar en cuenta las ventajas y desventajas que proporcionan dichos Sistemas Operativos.

CSM Proxy y CSMProxy Plus son soluciones avanzadas, que cuentan con las siguientes características: Completo sistema de registro, Permiso y restricción de acceso en función de la dirección de origen, Configuración remota a través de Internet protegida con password, entre otras. Estas soluciones se pueden instalar en puestos de trabajo Windows 95 o en un servidor con Windows NT.

Algunas soluciones proxy para plataforma Linux son Squid y Socks. Squid es una solución proxy típica, a nivel aplicación con la que cuenta Linux, alguno servicios con los que cuenta son cache para HTTP Y FTP, cache transparente, entre otros, esta solución viene integrada en la distribución Red Hat de Linux. Socks es una solución a nivel sesión.

2.2.5 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

DE HARDWARE.

El requerimiento de hardware se evalúa en función a la forma de conexión a Internet; existen dos formas de conexión a Internet, la primera es por vía módem, la cuál es más barata; y la segunda es por medio de una red LAN, en esta forma de conexión su costo es más elevado en comparación con la primera alternativa de conexión.

La decisión de la forma de conexión sé evalúa en relación, con el presupuesto con el que dispone, la dependencia en donde se instalara el servidor.

Los requerimientos de hardware necesarios en caso de que el acceso a Internet sea por vía telefónica, son los siguientes: un procesador 386 con 8 MB de RAM y un disco duro de 300Mb como mínimo, un módem, de 14.400 bps, no un win módem, una conexión a Internet punto a punto y una tarjeta ethernet.

En el caso de que el acceso a Internet sea por medio de una red LAN, el hardware necesario es: un procesador 386 con 8 MB de RAM y un disco duro de 300Mb como mínimo y dos tarjetas de Red.

Los discos duros soportados por la plataforma Linux son IDE, EIDE, MFM, RLL y SCSI. En lo que se refiere a procesadores, esta plataforma soporta todos los de la familia Intel, y otras marcas como AMD y Cyrix.

Los modems que trabajan correctamente en el entorno operativo Dos, también son soportados por linux. Por otra parte en cuanto a tarjetas de red se refiere linux soporta las siguientes: 3Com,3C503,3C505,3C507,3C509, Intel EtherExpress, NE2000/NE1000, Allied Telesis AT1700, Cabletron E21xx, DEC DEPCA, HP PCLAN 27245 y series 27xxx, PCLAN PLUS 27247B 27252A.

DE SOFTWARE

Existen dos alternativas de software para soluciones proxy en Linux estos son: Squid a nivel aplicación y Socks a nivel sesión.

El servidor proxy requiere software adicional, este software es el denominado socks, el cuál se puede conseguir en ftp: sunsite.unc.edu pub LINUX system network/misc/socks-linux-src.tgz.

El archivo se llama socks.conf, este archivo se debe de descomprimir y desempaquetar los archivos en un directorio, además de seguir las instrucciones de cómo compilarlo. Hay que asegurarse de que los Makefiles sean los correctos, ya que algunos lo son y algunos no.

El programa socks necesita dos archivos de configuración distintos. Uno es el archivo de control de acceso y el otro es el archivo de ruteo. En el primero se establecen los accesos que están permitidos, y en el segundo se le dirigen las peticiones al servidor Proxy. El archivo de control de acceso debe de residir únicamente en el servidor y el archivo de ruteo debe de residir en todas las terminales.

2.2.6 VENTAJAS Y DESVENTAJAS DE LOS SERVIDORES PROXY

Entre las ventajas más importantes se encuentran las siguientes:

- Oculta la dirección interna, ya que todas las conexiones de salida utilizan la dirección del proxy.

- Otra ventaja importante a considerar es la seguridad, ya que estos servidores son implementados para proteger los puntos débiles de la seguridad en la red.

- Los servidores Proxy no necesitan una versión especial del programa cliente en la maquina del cliente, ya que una vez instalado el proxy, cada persona que se haya registrado en este tendrá acceso a la red protegida, sin tener que instalar algún software adicional.

- La velocidad de transmisión es una ventaja considerable, ya que no tiene que buscar las páginas en Internet, lo cuál permite aumentar la velocidad con la que se navega.

- Los servidores proxy también son considerados como un dispositivo de seguridad.

Estos no tiene un número límite de maquinas para acceder a Internet, sin embargo cuándo el número de máquinas es muy elevado, usarlo para aumentar el número de estas con acceso a Internet cuando se tienen pocas direcciones IP puede ocasionar muchas desventajas.

Entre las desventajas que puede ocasionar el uso de un servidor proxy se puede hacer mención a las siguientes:

- Un servidor proxy permite un mayor acceso desde dentro de la red protegida al exterior, pero mantiene el interior completamente inaccesible por el exterior.

- Otro inconveniente lo presenta con el FTP ya que cuando se pide un ls, o un get, el servidor FTP establece una conexión con la máquina cliente y manda la información por ésta. En el caso de un servidor Proxy, este no lo permitirá, por tal motivo el FTP no funciona bien en este tipo de servidores.

- Los servidores Proxy son lentos, debido a la gran sobrecarga de información con la que cuenta. Por lo cuál cualquier otro método de acceso puede ser más rápido que este medio.

2.2.7 SEGURIDAD EN LOS SERVIDORES PROXY.

Un aspecto importante a considerar en red, es la seguridad que existe dentro de ella, ya que la información que se maneja dentro de esta es de suma importancia, debido a que la información se puede vender o comprar, o utilizarse de manera directa para proporcionar servicios que produzcan grandes ganancias.

La seguridad en una red completa se puede confiar a una sola máquina o a un servidor.

Existe una técnica general para mantener la seguridad dentro de las redes, este mecanismo es denominado cortafuegos o muro de seguridad. Este tipo de mecanismos es utilizado en el acceso a Internet, con el propósito de prevenir que no haya obtención de información por medio del exterior. Un muro de seguridad debe tener software y hardware para que pueda operar a la velocidad que opera una red.

FIREWALLS(PARED CORTAFUEGOS).

Un cortafuegos es un software o hardware que filtra los intentos de conexión a partir de criterios definidos, de manera que se pueda detectar e impedir el acceso al sistema a posibles intrusos, sin que se haya llegado a establecer un enlace directo entre el intruso y el sistema. Un cortafuego es considerado un dispositivo lógico, que protege una red privada del resto de la red pública.

Un cortafuegos nos garantiza que cualquier red que tenga algún tipo de conexión hacia el mundo exterior, o con otras redes, sea segura, evitando violaciones, y permitiendo pasar sólo los paquetes de red que son autorizados, por lo que se deben configurar los cortafuegos para lograr que sean transparentes a los usuarios normales de la red, y totalmente sólido para otros usuarios.

Existen varias aplicaciones firewalls para linux, entre estas se puede hacer mención a *Ipfwad, Ipchains, Netfilter, Ipf, Sínus firewalls y Phoenix Adaptive Firewalls* entre otros.

Un cortafuegos tiene las siguientes propiedades:

- Todo el tráfico de adentro hacia fuera, y viceversa debe pasar sobre ella.
- Solo el tráfico autorizado, definido por la política de seguridad es autorizado para pasar por él.
- El sistema es realmente resistente a la penetración.

Los cortafuegos funcionan de la siguiente forma:

1. Se toma un computadora con capacidad de enrutar (por ejemplo una PC que contenga LiNUX(como sistema operativo.)
2. Se le ponen dos interfaces (por ejemplo interfaces serie, o ethernet, etc...)
3. Se le deshabilita el reenvío de paquetes IP (IP forwarding)
4. Se conecta una interfaz a la Internet
5. Se conecta la otra interfaz a la red que se quiere proteger

Ahora hay dos redes distintas, que comparten un servidor. El cortafuegos, al que pueden comunicarse tanto con la red protegida como con la Internet.

La red protegida no puede comunicarse con la Internet, y la Internet no puede comunicarse con la red protegida, debido a que se ha deshabilitado el reenvío IP en la única computadora que las conecta. Si se quiere acceder a Internet desde la red protegida, hay que hacer primero un telnet al cortafuegos, y acceder a la Internet desde él. Del mismo modo, para acceder a la red protegida desde la Internet, se debe antes pasar por el cortafuegos.

Este es un mecanismo de seguridad excelente contra ataques desde Internet. Si alguien quiere atacar la red protegida, primero tiene que atravesar el cortafuegos. De esta manera el ataque se divide en dos pasos, y, por lo tanto, se dificulta. Si alguien quiere atacar la red protegida por métodos más comunes, como el bombardeo de emails, u otros métodos, simplemente no podrá alcanzarla. Con esto se consigue una protección excelente.

INCONVENIENTES DE LOS CORTAFUEGOS

El mayor problema de los cortafuegos es que restringen mucho el acceso a la Internet desde la red protegida. Específicamente, reducen el uso de la Internet al que se podría hacer desde un terminal.

La desventaja que presenta un cortafuegos es que sólo se puede generar la comunicación siempre y cuando exista un sistema con estas características en ambos lados de la red. Sin embargo, se puede armar un sistema bastante seguro utilizando un sistema operativo robusto, el software adecuado, y las configuraciones necesarias para tales fines.

Tener que entrar al cortafuegos y desde allí realizar todo el acceso a Internet es una restricción muy seria. Programas como Netscape, que requieren una conexión directa con la Internet, no funcionan desde detrás de un cortafuegos.
La solución a todos estos problemas es un Servidor Proxy, ya que los servidores proxy permiten el acceso directo a la Internet desde detrás de un cortafuegos. Funcionan abriendo un socket en el servidor y permitiendo la comunicación con la Internet a través de él.

El uso combinado de un cortafuegos y de un proxy es bastante seguro, Ya que se basa en el concepto de "divide y vencerás", lo cuál es ideal para resolver los problemas de seguridad informáticos.

CAPITULO III.

INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR PROXY.

3.1 INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR.

3.1.1 CONFIGURACIÓN DEL PROTOCOLO TCP/IP.

Algunos sistemas operativos al instalarse introducen por defecto los protocolos TCP/IP, entre estos se encuentran windows 95 y Linux, cuando esté último arranca se cargan automáticamente. Es importante señalar que en el caso de windows9x, solo incluye los protocolos si durante su instalación detecta las tarjetas de red. En caso contrario, tendrá que conseguir el software para la instalación del protocolo.

En el caso que Linux, no cuente con TCP/IP ó soporte para tarjetas de red, o módem, etc. Se debe reconfigurar y generar un nuevo núcleo del sistema operativo que soporte el protocolo.

Existen varias razones por las cuales Linux podría carecer de soporte para red; las dos más comunes son: 1) el núcleo que esta utilizando es de una versión obsoleta y 2) que al instalar Linux, se omitió la opción de soporte para red.

En el primer caso se tiene que buscar una versión del kernel posterior a la que se cuenta en ese momento, después se procede a reconfigurar el Kernel y generar uno nuevo que soporte el TCP/IP. Para incluir el soporte de la red tendrá que contestar afirmativamente a la pregunta correspondiente que se le hará durante el proceso de configuración del núcleo. En el segundo caso existen dos soluciones; la primera es reconfigurar el kernel actual y la segunda es bajar de algún archivo FTP el módulo que permita el soporte para red, este se baja a al host o terminal y se manda a llamar en el siguiente subdirectorio ***etc/conf.modules.***

Una vez hecho esto, se deben modificar los archivos de configuración que usa NET-4. Esta parte suele ser bastante simple, pero existen diferencias entre las diferentes distribuciones de Linux. Los archivos pueden estar en ***/etc*** o en ***/usr/etc*** o incluso en ***/usr/etc/inet.*** En ocasiones se encuentran repartidos por varios directorios y no en uno solo.

Sin embargo esta situación es poco frecuente. Debido a que las instalaciones que actualmente se hacen de Linux incluyen la tarjeta de red.

Es importante señalar que existen tres propuestas de configuración en red. *Dirección IP estática*: Si se elige esta propuesta la información referente a la red se debe de suministrar manualmente; *BOOTP:* la información necesaria de la red se obtiene automáticamente mediante una petición bootp; *DHCP.* la información necesaria se obtiene automáticamente mediante una petición DHCP.

Si elige la opción *BOOTP* o *DHCP* la configuración de su red se realiza automáticamente

Si elige la opción *Dirección IP estática o manual,* se tendrán que especificar todos los datos sobre la red.

Si su red cuenta con más de un servidor de nombres , puede introducir las direcciones IP de estos en los campos Servidor de nombres secundario y Servidor de nombres terciario. Posteriormente elija OK para continuar.

La figura 3 esquematiza las tres propuestas de configuración de red.

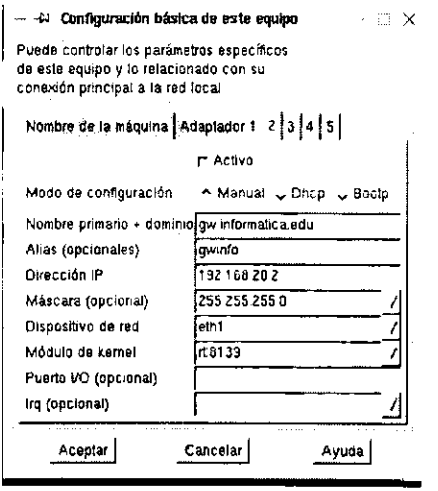

Figura 3. Pantalla que muestra la forma de asignación de direcciones IP.

3.1.2. INSTALACIÓN Y CONFIGURACIÓN DEL MÓDEM O TARJETA DE RED. CONFIGURACIÓN DE LAS TARJETAS DE RED.

La configuración de las tarjetas de red la detecta Linux durante su instalación de esté sistema operativo. En el caso de que las tarjetas no sean detectadas se tendrán que proporcionar los siguientes datos:

- El modelo: Se refiere al modelo de la tarjeta
- El No. de Irq
- El direccionamiento
- La dirección IP: Es la dirección IP asignada al host, está cuenta con un componente del host y un componente de la red.
- La mascara de red
- La dirección del gateway. Es la dirección del host que sirve de puerta de enlace a otras redes.
- El nombre del host: Como su nombre lo indica se refiere al nombre de la maquina .
- El Dominio: Se refiere al dominio al que pertenece la red local.

En la figura 4 se presenta un ejemplo de la configuración de una tarjeta de red.

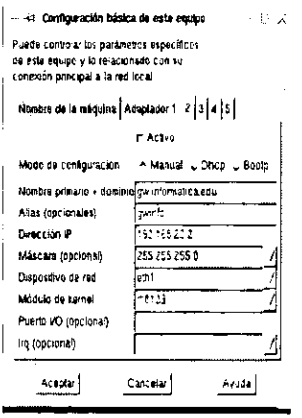

Figura 4. Pantalla que muestra los parámetros de la tarjeta de red a configurar.

El No. de Irq y la dirección de E/S son parámetros opcionales; los demás parámetros son obligatorios.

Cuando se han insertado las tarjetas de red después de la instalación de la distribución, lo primero que se debe hacer es configurarla. Para ello se ejecuta el programa netconf(Network Configurator) y en la solapa INTERFACES se añaden las tarjetas de red. Primeramente preguntará el tipo: PPP, SLIP, PLIP, Ethernet, Arcnet, Token ring, Pocket. También se configurará la dirección IP que se va a utilizar y la máscara de red. Se activara y guardara la configuración. Si es el primer adaptador de red que se instala, por ejemplo: del tipo Ethernet, se llamará eth0, si es el segundo eth1, si es el tercero eth2, etc.

Se ejecutará ***netconf***(Configurador de red), en donde la primera opción es ***Información Básica del Equipo***, aquí se configura el nombre de la máquina y la configuración completa de cada uno de los adaptadores de red, etc. La Figura 5 esquematiza la pantalla a la que se hace referencia.

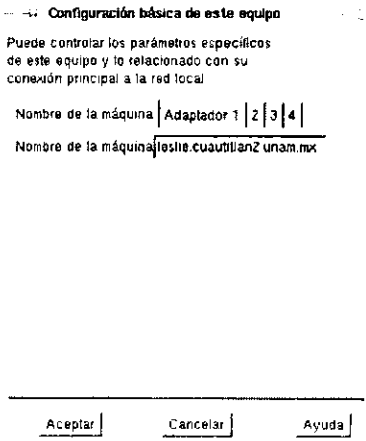

Figura 5. Información Básica del equipo.

Podrá reiniciar su equipo, si lo desea y al arrancar se verán las tarjetas de red y sabrá si están bien ó mal configuradas; Por ejemplo:

```
eth0 [ OK ]
eht1 [ FAILED ]
eht2 [ PASSED ]
eht3 [ FAILED ]
```

En el ejemplo anterior el equipo tiene cuatro tarjetas de red de las cuales sólo dos están físicamente ó están correctamente configuradas.

CONFIGURACIÓN DEL MÓDEM EN FORMA GRÁFICA.

Existen dos clases de módems los internos y los externos, estos últimos no presentan ningún tipo de problemas, en los primeros hay que tener mucho cuidado en que no sean win-módem, ya que estos últimos son módems de bajo rendimiento, que dan pésimos resultados. Es importante señalar que un buen módem no tiene requerimiento de software y hardware.

En el caso de que se utilice una conexión punto a punto se debe de verificar la correcta instalación y configuración del módem en la maquina en donde se va a instalar el servidor proxy. La correcta instalación del hardware es un factor importante para el acceso a Internet.

Para conectar Linux a Internet por medio de un módem, RDSI ó módem ADSL, a través de la línea telefónica, se necesita conectar a un proveedor de acceso a Internet (ISP). Para ello se utilizara el protocolo PPP, el cuál se conoce como protocolo de comunicación en líneas punto a punto. PPP trabaja en diferentes tipos de línea punto a punto entre los que se incluye SONET, X25 y RDSI.

Existen varias formas para la configuración de un módem. Una de ellas es ejecutando el programa ***modemtool***, en el cual se selecciona el puerto en que se encuentra conectado el módem. Normalmente los módem externos utilizan el puerto COM2 ó ttys1 y COM1 ó ttys0, si se trata de un módem interno COM3 ó ttys2 y COM4 ttys3. Se selecciona el puerto y se pulsa Ok. Posteriormente se ejecuta el programa ***kppp*** en el que aparecen las 6 solapas que se muestran en la figura 6.

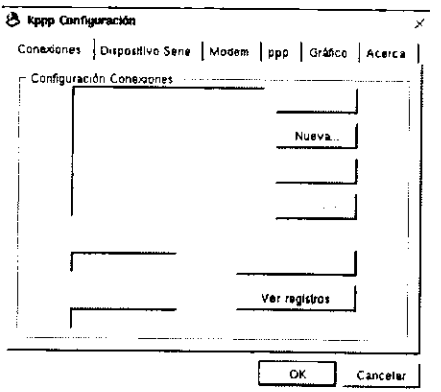

Figura 6. Pantalla de configuración del módem

Si selecciona la solapa módem puede hacer una consulta al módem y comprobar así el funcionamiento. Aquí se pueden configurar parámetros del módem, además de que tiene una consola para comunicación del módem, programación del mismo y consultas. Después se selecciona la solapa ***dispositivos serie*** y ***dispositivos del módem*** en donde se selecciona el puerto que utiliza el módem.

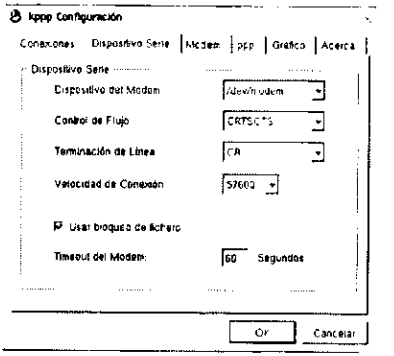

Figura 7. Elementos a configurar en la solapa dispositivo serie.

En control de flujo normalmente es XON/XOFF, en terminación de línea CR/LF y en la velocidad de conexión aquella que sea acorde con el módem. Posteriormente se selecciona la solapa conexiones y se pulsa nuevo. La figura 8 muestra la pantalla que se presenta al seleccionar la solapa conexiones. En la solapa marcar, se introduce el nombre de la conexión y el número de teléfono a donde nos vamos a conectar. En la solapa Dirección IP normalmente se selecciona la IP asignada por el servidor, salvo que se tenga una IP fija en nuestro ISP.

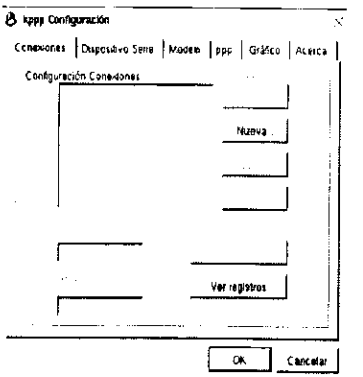

Figura 8. Pantalla que se muestra al seleccionar conexiones.

En la solapa servidor de nombres se completan las IP correspondientes al servidor de nombre ó DNS por ejemplo 10.0.1.1 .Y salvo algún parámetro que en particular sea necesario, por último se entrara a la solapa puerta de enlace en donde se dejara puerta de enlace por defecto. Es importante señalar que la IP del DNS es la que el ISP disponga.

En la pantalla principal del programa kppp se debe introducir el nombre de usuario y la clave para acceder remotamente al servidor. Ya tenemos básicamente configurada la conexión sólo se debe pulsar la opción conectar.

CONFIGURACIÓN DEL MÓDEM EN MODO CONSOLA.

PPPD es la primera posibilidad de conexión a Internet que ofrece Linux. Es una conexión a Internet que gasta pocos recursos y con posibilidad de hacerla desde la consola, sin necesidad de entrar en modo gráfico. Cualquiera que aspire a obtener el máximo rendimiento de la conexión a Internet, lo puede tener por medio de esta posibilidad..

Cuenta con una serie de inconvenientes. El más destacable es la falta total y absoluta de interactividad o de información en pantalla de cómo va la conexión, siendo necesario el uso de otros comandos (como ***ifconfig***) o la observación de archivos históricos (***/var/log/messages)*** para averiguar si la conexión se ha realizado con éxito o ha surgido algún error.

La configuración de pppd se basa en la creación de una serie de archivos los cuales se describen a continuación:

/etc/ppp/options: Configuración de la conexión y del puerto serie
/etc/ppp/marcado : Configuración del módem y marcado del número de teléfono
/etc/ppp/pap-secrets : Claves de acceso para identificación con PAP
/etc/ppp/chap-secrets : Claves de acceso para identificación con CHAP
/etc/resolv.conf : Servidores de nombres (DNS)

Un ejemplo del archivo ***/etc/ppp/options*** es:

```
connect "/usr/sbin/chat -v -f /etc/ppp/marcado"
name mi_login@mi_proveedor
defaultroute
noipdefault
modem
crtscts
asyncmap a0000
mru 576
/dev/ttySx
115200
```

En mi_login@mi_proveedor irá el login y el proveedor (el proveedor sin dominio, por ejemplo: fulanito@arrakis)
Donde pone /dev/ttySx, la 'x' indica el puerto serie: /dev/ttyS0 = COM1, /dev/ttyS1 = COM2, etc.

La velocidad 115200 no es la velocidad del módem, es la velocidad entre el módem y el puerto serie, que no tiene por qué coincidir con la velocidad en el lado de la línea telefónica. La velocidad del módem (33600, 28800...). No hay que ponerla en ningún sitio. Algunos módems no soportan esa velocidad entre el módem y el puerto serie y habrá que probar con 57600 o incluso con 38400.

Si se tiene una UART 16450 o 8250, utilizar 38400 (usar setserial /dev/ttySx para conocer la UART del módem o del puerto serie, donde 'x' indica el puerto serie de la misma forma que antes). Nótese que el valor óptimo es 115200 y conforme menor sea dicho valor, menos rendimiento le sacaremos al módem.

Un ejemplo del archivo ***/etc/ppp/marcado*** es:

```
ABORT "BUSY"
ABORT "NO CARRIER"
ABORT "NO DIALTONE"
ABORT "ERROR"
""
"AT& F" TIMEOUT 5 OK
"ATW1DTnumero_de_telefono" TIMEOUT 100 CONNECT
```

Los ABORT iniciales sirven para que, si el módem encuentra una situación anómala (no hay tono de llamada, comunicando..) y responde alguno de esos mensajes (BUSY, NO CARRIER), el pppd pare y no pierda tiempo hasta fallar el TIMEOUT 100 que sería el que acabase la conexión. El problema es que no todos los módems responden de la misma forma (por ejemplo, puede responder (*NO DIAL TONE* en vez de *NO DIALTONE*) y la correspondencia debe ser exacta. Por tanto, para una configuración correcta, será necesario consultar en el manual del módem cómo son estos mensajes.

El "AT& F" es la cadena de inicialización del módem. La que se indica es de las más estándar. No obstante, en algunos módems puede ser mejor "ATZ" o variantes de "AT& F" (como "AT& F1", "AT& F2"...).

Como referencia, se debe usar aquella que configure el módem para usar control de flujo hardware (RTS/CTS). En caso de no acertar en la configuración del módem, es posible que se produzcan algunos efectos indeseables (el módem no cuelga al cortar la comunicación, conexión lent.).
Una posibilidad es "fusilar" la que use windows. Se puede ver dentro del directorio de windows un archivo llamado modemlog.txt o modemdet.txt.
El número_de_teléfono es precisamente eso. El número de teléfono del nodo que le asigne su proveedor telefónico.

El archivo ***/etc/ppp/pap-secrets y /etc/ppp/chap-secrets***

Existen dos formas posibles de identificación cuando nos conectamos a un proveedor: PAP y CHAP. PAP es la más sencilla y CHAP es muy usada. En caso de que cuente con las dos opciones es recomendable que use PAP, ya que como se explico es la más sencilla de usar.

El formato de ambos archivos es el mismo:

---

*mi_login@mi_proveedor * password*

---

mi_login@mi_proveedor debe ser exactamente lo mismo que se puso como parámetro de la opción 'name' en /etc/ppp/options. Los campos van separador por tabuladores no por espacios.

Si se dispone de más cuentas con otros proveedores, se pueden añadir nuevas líneas con el mismo formato.

Si sabes que su proveedor usa PAP, grábelo como pap-secrets. Si usa CHAP, grábelo como chap-secrets. Si no sabes cual usa, puedes hacer prueba-y-error o crear los dos, o crear uno sólo y hacer un enlace simbólico de uno al otro. Por ejemplo, si ha creado chap-secrets, para hacer un enlace desde pap-secrets se haría:

cd /etc/ppp

ln -s chap-secrets pap-secrets

Esto en teoría haría que pppd y tu proveedor se pusieran de acuerdo para elegir PAP o CHAP según prefieran. Un ejemplo del archivo ***/etc/resolv.conf :***

Aquí irían las direcciones de los DNS primario y secundario. El formato es muy sencillo:

---

nameserver DNS_primario

nameserver DNS_secundario

Por ejemplo, nameserver 195.5.65.2

En lugar de DNS_primario y DNS_secundario, se pondrán las direcciones numéricas de los DNS primario y secundario respectivamente. Los DNS primarios y secundarios se deberán de preguntar al proveedor y este tendrá que proporcionarlos, ya que no son secretos.

Si no se cuenta con DNS_secundario se puedes ahorrar la segunda línea.

Una vez creados los scripts, la conexión se efectuaría al escribir ***pppd o /usr/sbin/pppd.***

Para comprobar si la conexión tiene éxito, se puede usar el comando ***/sbin/ifconfig*** y ver si al cabo de un minuto o dos aparece un bloque nuevo ppp0.

Otra forma es consultando periódicamente el archivo ***/var/log/messages*** hasta ver si aparece lo siguiente:

Local IP address xxx.xxx.xxx.xxx

Remote IP address yyy.yyy.yyy.yyy

Lo cual indicaría una conexión con éxito. Una forma de hacer esto sería con la orden ***tail -f /var/log/messages*** y pulsar Ctrl+C cuando veamos que la conexión ha funcionado o fallado. La desconexión se realizaría introduciendo la orden ***killall pppd.***

Los archivos descritos se deben crear desde cero con un editor de Linux, ya que crearlos con un editor de DOS o de Windows, o con operaciones de cortar-y-pegar en Windows añade un carácter no visible al final de cada línea que Linux confundiría con un carácter normal, inutilizando los scripts.

3.2 CONFIGURACIÓN DE LOS CLIENTES

3.2.1 INSTALACIÓN Y CONFIGURACIÓN DEL PROTOCOLO TCP/IP EN LOS CLIENTES.

Los proxy son instalados para el acceso a Internet y a la red local al mismo tiempo. Los clientes del servidor que quieran acceder a Internet, realizan sus peticiones al servidor proxy, pues es el único que dispone de acceso al exterior. El servidor proxy realiza la conexión con el sitio indicado y cuando el servidor remoto le contesta, devuelve la información al cliente de la red interna que había solicitado la conexión. Es importante señalar que el servidor proxy dará servicio a todos los clientes de la red privada sin importar la plataforma que utilicen(windowsx, linux o unix).

CLIENTES LINUX.

- Si los clientes cuentan con Linux y el kernel ha sido compilado con soporte para TCP/IP, entonces la instalación y configuración es correcta. Esto incluye clientes como telnet y ftp, comandos de administración como ifconfig y route (que suelen estar en el directorio */etc*) y archivos de configuración de red, como */etc/hosts*.

- En caso se contrario se procederá a seguir lo explicado en el punto 3.1.1. Una vez hecho esto, se procede a modificar los archivos de configuración que usa NET-4. Esta parte suele ser bastante simple, pero existen desacuerdos entre las diferentes distribuciones de Linux. Los archivos pueden estar en */etc* o en */usr/etc* o incluso en */usr/etc/inet*. A veces los archivos están también repartidos por varios directorios y no en uno sólo.

CLIENTES UNIX.

- Si los clientes cuentan con unix y el kernel soporta el protocolo TCP/IP, entonces la instalación y configuración es correcta. Ya que contiene comandos de administración como ifconfig, route, telnet y gated. Además de que contiene clientes telnet y ftp.

- Los archivos de configuración que usa TCP/IP se encuentran ubicados en los directorios ***/etc, etc/host, /usr/, etc/ptotocols o*** incluso en ***etc/services.***

CLIENTES WINDOWS 9X.

Para configurar el protocolo TCP/IP en los clientes windows95. Se deben de seguir los siguientes puntos.

1. Haga doble click en el escritorio ***MI PC*** (figura 9), situado en el escritorio de windows.

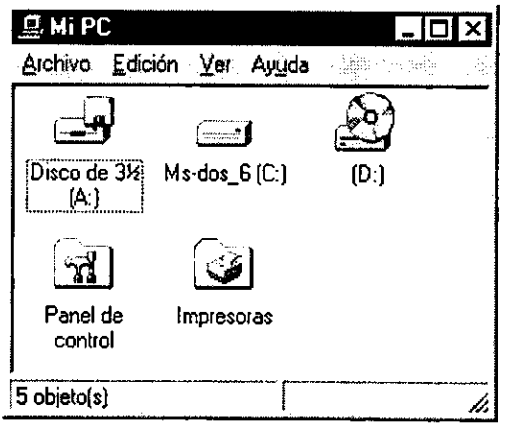

Figura 9. MI PC

2. Haga doble click en el icono ***Panel de Control*** (figura 10) y seleccione el icono ***RED***

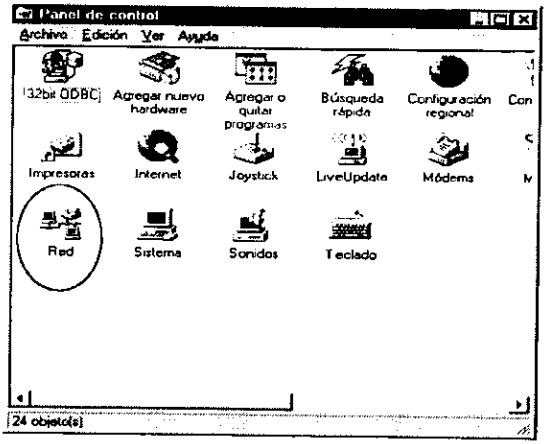

Figura 10. Panel de control

3. En la ventana ***seleccione protocolo de red(figura 11)***, elija en la primera columna **fabricantes**, la opción Microsoft y en la segunda columna **Protocolos de red**, la opción **TCP/IP.** Haga clic en el botón Aceptar para retornar la ventana **Red.**

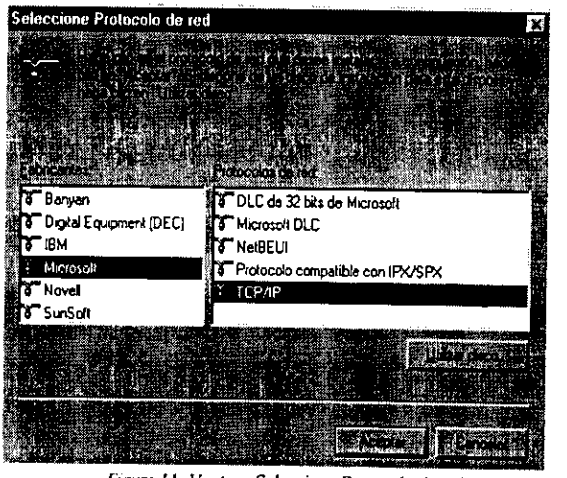

Figura 11. Ventana Seleccione Protocolo de red.

4. En la ventana ***Red*** (figura 12), verifique que solo haya un elemento TCP/IP. Si encuentra más de uno utilice el botón quitar para retirar los sobrantes. Después marque la línea TCP/IP y haga clic en propiedades. Es importante verificar que si se tiene una tarjeta de red, sólo haya un elemento TCP/IP.

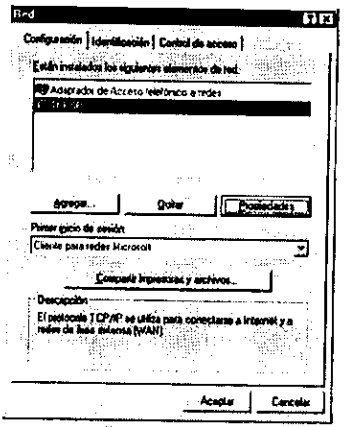

Figura 12. Ventana Red

5. En la pantalla ***Propiedades de TCP/IP*** (figura 13), verifique que este activa la opción **Obtener una dirección IP automáticamente**. Posteriormente haga clic en la pestaña **Configuración DNS.** La cuál se encuentra situada en la parte superior derecha.

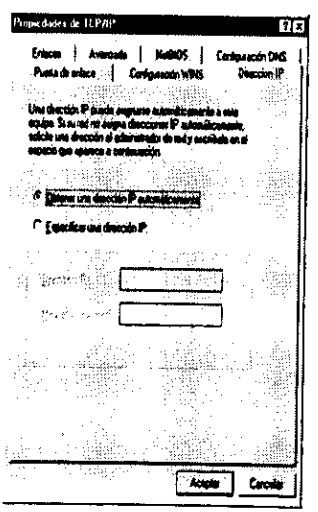

Figura 13. Pantalla Propiedades de TCP/IP

6. En la pantalla **Propiedades de TCP/IP** verifique que este activa la resolución WINS(figura 14). Presione el botón aceptar.

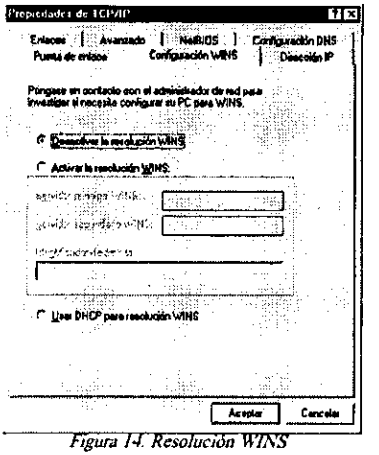

Figura 14. Resolución WINS

7. Al regresar a la pantalla de ***Red*** (figura 15), haga nuevamente click en el botón **Aceptar.** El sistema iniciara el proceso de instalación del TCP/IP. Si windows le pide el CD de instalación del Sistema Operativo, insértelo, de lo contrario iniciará la instalación del protocolo automáticamente. Después de terminado este proceso reinicie su PC.

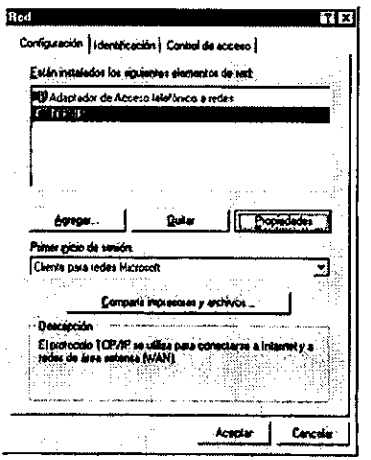

Figura 15. Pantalla RED

3.2.2 CONFIGURACIÓN DEL ACCESO A INTERNET.

Una vez instalada y configurada la tarjeta de red o el módem dependiendo del caso, el siguiente paso es hacer la configuración del acceso a Internet. La configuración del acceso a Internet con un computadora Linux se puede hacer de dos formas; 1) Configuración en modo X Window; y 2) Configuración en modo consola, las cuales se explican a continuación:

1°.- CONFIGURACIÓN EN MODO X-WINDOW.

Toda la configuración en modo gráfico se hará con los programas (Netconfig) ***netconf*** ó ***netcfg***. Después de la configuración de los dispositivos de red, llega el momento de la configuración de las IP , dominios, etc. En el programa ***netcfg*** se configura el ***hostname*** ó nombre del equipo, el ***dominio*** al que pertenece, la dirección IP y la máscara de red que tiene asignada cada una de las tarjetas de red que se tengan configuradas.

También se puede configurar la dirección del ***gateway*** ó puerta de enlace, en el caso de que para tener acceso a Internet exista un ***gateway*** ó una computadora que sirva de puerta de enlace. Con el programa ***netconf***, se puede configurar todo más detalladamente. Por ejemplo en la opción *NFS: FILESYSTEM EXPORTADOR* que se encuentra en la opción *Tareas como servidor* (figura 18), especificamos los directorios que se deseen compartir en la red.

Al ejecutar el programa ***netconf*** aparecerá una pantalla de configuración (Figura 16).

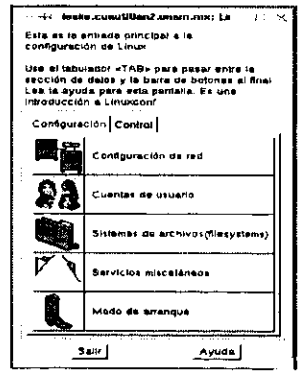

Figura 16. Pantalla de opciones de configuración.

Al seleccionar la opción *Configuración de la red* mostrara tres solapas: *Tareas como cliente, Tareas como servidor Y Misc .*

La solapa ***Tareas como cliente*** tiene las opciones que se muestran en la figura 17.

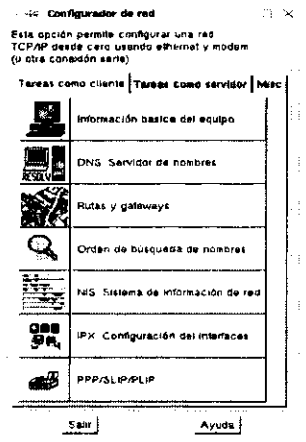

Figura 17. Tareas como Cliente

La solapa ***Tareas como servidor*** tiene las opciones que se muestran en la figura 18.

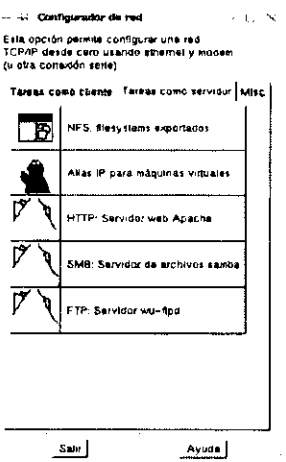

Figura 18. Tareas como Servidor

Por último la solapa ***Misc*** cuenta con utilidades de red que se muestran en la figura 19:

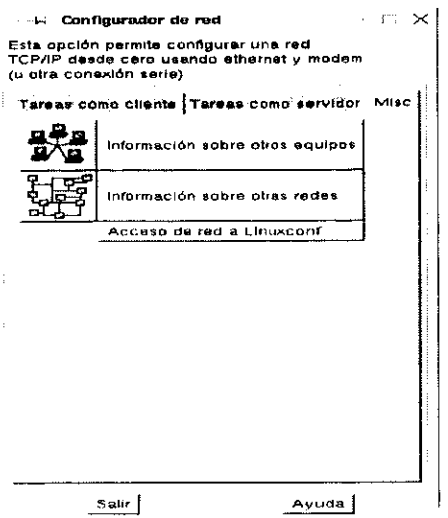

Figura 19. Utilidades con las que cuenta la opción MISC.

2°.- CONFIGURACIÓN DE LA RED EN MODO CONSOLA.

Para configurar la red en modo consola, lo primero que se debe hacer es configurar las tarjetas de red en modo consola. En el caso que durante la instalación de Linux no se hayan instalado las tarjetas de red, se tendrán que configurar introduciendo todos los datos con la ayuda del programa ***netconf*** en modo consola. Posteriormente se configurara la IP, mascara de red, etc.

Cuando se instala Linux, localiza la tarjeta de red durante la misma instalación, los datos que nos pide son el nombre del equipo y el dominio. De cualquier forma, en modo consola se puede utilizar el programa ***netconf*** ó ***netconfig***, pero también se puede hacer de la siguiente manera:

Primeramente se desactiva la interfaz (sí esta se encuentra activa debido a una configuración anterior)

por ejemplo:

ifdown eth0

Se configura de nuevo con una dirección correspondiente al rango de la red local, por ejemplo:

ifconfig eth0 10.0.0.4 netmask 255.0.0.0.

Posteriormente se añade la IP del ***gateway*** en el caso que sea necesario por ejemplo:

route add default gw 10.0.0.1 dev eth0

route -v

Por último se configura el navegador en el caso que estemos conectados a través de otra máquina, que sea la que conecta a Internet con un módem ó con RDSI, módem ADSL, etc y que tenga instalado un servidor proxy para dar servicio a toda la red local. Para ello se ejecutará el Netscape Navigator y en el menú se escogerá la opción ***edit***, en donde en la parte de abajo se encuentra la opción ***preferencias y advanced.***

Se seleccionará la solapa ***advanced***, que es en donde se encuentra la opción ***proxies*** en donde al entrar esta la opción de configurar manualmente las opciones del proxy. En ellas se pondrán los siguientes datos: el nombre DNS en el caso que corresponda a una IP del que hace de servidor proxy ó directamente su número de IP.

Por ejemplo:

Servicio	Servidor Proxy	Puerto
HTTP	10.0.0.1	80
FTP	10.0.0.1	21

A partir de aquí cuando se habrá el navegador. automáticamente buscará Internet en la computadora de la red local que da ó hace de servidor proxy, y se tendrá Internet en la PC.

3.2.3 ASIGNACIÓN DE LAS DIRECCIONES IP A LAS ESTACIONES DE TRABAJO.

Antes de instalar el servidor proxy, hay que asegurarse de que se encuentre instalado el protocolo TCP/IP en la red local. La instalación del protocolo no es necesaria en todas las maquinas que conforman a la red LAN, sino únicamente en aquellas que utilizarán el servicio de Internet y en la que se va a instalar el proxy.

Al instalar el protocolo TCP/IP, se deberá asignar direcciones IP a las estaciones de trabajo de la Red Local, las direcciones que se le asignen a los puestos de trabajo deberán de estar comprendidas en la subred de ***clase C*** 192.168.x.x, ya que este rango de direcciones IP esta reservado para el uso de intranets, además de que proporciona un espacio seguro de direcciones. Es importante señalar que se le debe asignar una dirección diferente a cada conexión de la Red local. Se recomienda que al servidor proxy se le asigne la dirección IP 192.168.0.1, ya que esta es más fácil de recordar.

3.2.4 COMPROBACIÓN DE LA INSTALACIÓN Y CONFIGURACIÓN DEL PROTOCOLO TCP/IP.

Para comprobar si esta instalado el soporte TCP/IP se tiene que introducir el siguiente comando en la línea de mandatos:

cat /proc/net/dev

Si no se generan errores y la salida se parece a la que se muestra a continuación, entonces el núcleo esta configurado correctamente.

```
Inter-   Receive                Transmit
Face |packets errs drop fifo frame|packets errs drop fifo colls carrier
  lo    0    0    0    0    0    0    0    0    0    0
dummy  No statistics available
Plip0  No statistics available
Plip1  No statistics available
Plip2  No statistics available
Eth0   No statistics available
Eth1   No statistics available
Eth2   No statistics available
Eth3   No statistics available
Ppp0     0    0    0    0    0      0    0    0    0    0    0
```

El TCP/IP es un paquete necesario, puede estar seguro de que está instalado, si los siguientes archivos **rc.inet1** y **rc.inet2** se encuentran en el directorio **/etc/rc.d.** Estos son los archivos de configuración durante el arranque del sistema. Para comprobar la configuración del protocolo TCP/IP, se procede a arrancar la computadora y se introduce el siguiente comando en la línea de mandatos.

Ping -c 4 hansolo.starwars.com

Si todo esta correcto la pantalla mostrará la siguiente salida.

```
PING hansolo.starwars.com (127.0.0.1) 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=255 time=0.3 ms
--- hansolo.starwars.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
Round-trip min/avg/max = 0.3/0.3/0.4 ms
```

Si la salida recibida no se parece a esta o se obtienen mensajes de error, significa que algunos de los pasos de configuración no se realizaron correctamente.

3.3. CONFIGURACIÓN DEL SOCKET.

El programa socks necesita dos archivos de configuración distintos. En uno se le indica que accesos están permitidos, y en el otro se le dirigen las peticiones al servidor proxy apropiado. El archivo de control de acceso debe residir en el servidor, y el archivo de ruteo debe de residir en todas las maquinas.

Algo importante que hay que señalar es que el servidor proxy se debe de añadir al ***etc/inetd.conf.*** mediante la siguiente línea:

socks streams tcp nowait nobody /usr/local/etc/sockd sockd.

3.3.1 EL ARCHIVO DE CONTROL DE ACCESO (sockd.conf).

El archivo de control de acceso es el **sockd.conf,** este deberá contener dos tipos de líneas: las de permiso, que contienen ***"permit"*** y las de prohibición que contienen ***"deny"***. Cada línea tendrá las tres palabras siguientes:

- El identificador (permit/deny)
- La dirección IP
- El modificador de dirección

El identificador es permit o deny

La dirección IP se compone de cuatro octetos según la típica notación de puntos.
por ejemplo:

192.168.2.0

El modificador de direcciones es también un número de cuatro octetos. Esta funciona como un mascara de red. Se debe de ver como 32 bits. Si el bit es uno, el bit correspondiente de la dirección que se comprueba debe coincidir con el bit correspondiente del campo de dirección IP.
La siguiente línea permitirá las direcciones IP comprendidas desde la 192.168.2.0 hasta la 192.168.2.255.

permit 192.168.2.0 255.255.255.0

Primero se deben de permitir todas las direcciones que se quieran permitir, y después se prohibirán el resto.
Por ejemplo:

permit 192.168.2.0 255.255.255.0
deny 0.0.0.0 0.0.0.0

El ejemplo anterior permite todas las líneas comprendidas en el rango 192.168.2.xxx

3.3.2 EL ARCHIVO DE RUTEO (socks.conf)

El archivo de ruteo de socks tiene le nombre de **socks.conf**, este archivo tiene la función de decir al cliente de socks cuando usar socks y cuando no.

Existen tres tipos de entradas:

- deny
- direct
- sockd

deny le indica a socks que peticiones debe de rechazar, esta entrada tiene los siguientes campos, identificador, dirección y modificador. Dado que esto también es manejado por el archivo de control de acceso **sockd.conf**, el modificador se pone a 0.0.0.0, si uno quiere impedirse así mismo conectarse a un sitio determinado, se puede hacer especificándolo aquí.

La entrada ***direct*** indica para que direcciones no se debe usar socks. Es decir aquellas direcciones a las que se puede llegar sin usar el servidor proxy. Esta entrada también contiene tres campos identificador, dirección y modificador.

Un ejemplo de esta entrada es el siguiente:

direct 192.168.2.0 255.255.255.0

Con esa entrada se accedería a cualquier maquina de la red protegida.

La entrada **sockd** señala cuál es la máquina en la que se ejecuta el servidor socks. Su sintaxis es la siguiente:

sockd @= <lista de servidores> <dirección Ip> <modificador>

@ = permite poner las direcciones IP de una lista de servidores proxy. La dirección IP y el modificador especifican a que direcciones se va a través de los servidores.

3.4 CONFIGURACIÓN DEL SERVIDOR PROXY

El servidor se instalará en una pc que contenga el Sistema Operativo Linux, a esta se le adaptará una segunda tarjeta de red. Es decir el Servidor tendrá dos tarjetas de red, con una se comunicará a la red local y con la otra establecerá comunicación con la red privada.

A los adaptadores de red se les configuraran los siguientes datos:

Adaptador 1

Nombre primario + dominio	leslie.cuautilan2.unam.mx	
Alias	leslie:	Nombre asignado arbitrariamente.
Dirección IP	132.248.102.146:	Asignada por el administrador de la red.
Mascara opcional	255.255.255.0:	Alcance de la red
Dispositivo de red	eth0:	El primer dispositivo ethernet del equipo.
Módulo de kernel	3c50x	Corresponde a una tarjeta 3com etherlink III 10/100

Adaptador 2

Nombre primario + dominio	gw.informatica.edu
Alias	gwinfo
Dirección IP	192.168.20.1
Mascara opcional	255.255.255.0
Dispositivo de red	eth1
Módulo de kernel	rtl8139

La dirección del gateway es la siguiente *132.248.102.254*

La dirección de los servidores de nombres son las siguientes:

- *132.248.102.1*
- *132.248.204.1*

El archivo de control de acceso residirá en el servidor. Los parámetros de configuración son los siguientes:

permit	***192.168.20.1***	***255.255.255.0***
deny	***0.0.0.0***	***0.0.0.0***

Esto permitirá el acceso de cualquier máquina de la red privada hacia el servidor.

Se debe de utilizar dos concentradores en uno se conectará la red Local y en el otro se conectara toda la red privada.

Los archivos de configuración que se bajen por medio del ftp se tendrán que descomprimir y compilar, ya que algunos makefiles son correctos y algunos no. Estos archivos como ya se menciono en el capitulo dos se encuentran en la siguiente dirección ftp.
ftp://sunsite.unc.edu/pub/Linux/system network/misc/socks-linux-src.tgz

Es importante recordar que la llamada al servidor Proxy se hará en el archivo ***etc/inetd.conf*** mediante la siguiente línea:

socks streams tcp nowait nobody /usr/local/etc/sockd sockd.

Otro aspecto a considerar es que se tienen que agregar los siguientes parámetros al archivo **etc/services:**

socks	***1080/tcp***
ghoper	***70/tcp***
www	***80/tcp***

Para poder acceder a los archivos de configuración es necesario que se cuente con una cuenta de superusuario, ya que esta permite que se tenga una serie de privilegios para modificar, borrar y actualizar archivos de configuración del sistema.

3.5 CONFIGURACIÓN DEL CLIENTE.

Cada cliente tendrá un adaptador con la siguiente configuración:

Cliente 1

Adaptador 1

Nombre primario + dominio	est1.informatica.edu	
Alias	est1:	Primera estación de la red privada
Dirección IP	192.168.20.2 :	Dirección IP de la red detrás del Proxy
Mascara opcional	255.255.255.0	
Dispositivo de red	eth0:	El primer dispositivo ethernet del equipo.
Módulo de kernel	3c50x	Corresponde a una tarjeta 3com etherlink III 10/100

Cliente 2

Adaptador 1

Nombre primario + dominio	est2.informatica.edu
Alias	est2
Dirección IP	192.168.20.3
Mascara opcional	255.255.255.0
Dispositivo de red	eth0
Módulo de kernel	3c50x

La IP del gateway para los clientes es el 192.168.20.1(***gw.informatica.edu***)

La dirección de los servidores de nombres son las siguientes:

- *132.248.102.1*
- *132.248.204.1*

Es importante señalar que el módulo de kernel es distinto en cada cliente, ya que aquí se configura la marca y modelo de la tarjeta de red. Otro aspecto a considerar es que todos los clientes de la red privada deberán pertenecer al dominio ***informatica.edu***

En los clientes deberá existir el archivo de ruteo ***(socks.conf)*** este archivo contendrá la siguiente configuración:

direct 132.248.102.146
sockd @=192.168.20.1 255.255.255.0

Con esto se establece para qué máquinas no se debe de usar el servidor socks, además de que se indica cuál es la dirección IP válida del servidor Proxy, así como a que direcciones se va a través del servidor Proxy

Es importante mencionar que no se deberá restringir ningún tipo de servicio a los clientes, ya que únicamente se utilizará como caché.

3.6 CONFIGURACIÓN DE LAS APLICACIONES

Para que las aplicaciones funcionen correctamente con el servidor proxy es necesario configurarlas. Será necesario tener dos telnets uno para la comunicación directa y otro para la comunicación a través del servidor proxy.

Una vez configuradas las aplicaciones se debe de cambiar el nombre a todos los programas de la red protegida y sustituirlos por los configurados. Así "telnet" pasara a ser "telnet.orig", "finger" a "finger.orig", etc. Esto se debe de dar a conocer al archivo socks en el archivo ***include/socks.h***

3.7 CONFIGURACIÓN DEL CORTAFUEGOS.

La configuración del cortafuegos depende en gran medida del que se haya elegido. Para ejecutar las reglas del script correctamente se deben tener dos datos: la dirección IP de la interfaz por el que nos conectamos a Internet y el nombre de ese interfaz.

Si suponemos que la conexión es mediante PPP con asignación dinámica de IP, por lo que recibimos la IP y el nombre del interfaz del programa PPP que al establecer la conexión pasa esa información en dos variables de entorno que son $IFNAME e $IPLOCAL (man pppd).

La ejecución del script es invocada en ***/etc/ppp/ip-up.local.***

En Caso de tener conexión directa o IP fija, la llamada a ***rc.firewall*** debe realizarse en otro sitio (por ejemplo ***/etc/rc.d/rc.local***) y estos datos, se deberán de asignar manualmente. También se tendrá que modificar esto en el caso de que la conexión sea mediante DHCP (acceso a Internet por cable).

El archivo ***/etc/ppp/ip-up.local*** se encarga de realizar las acciones que se puedan necesitar una vez que se establezca la conexión PPP. Por ejemplo, registrar conexiones, o establecer las reglas del cortafuegos.

En el siguiente ejemplo se invocara en él la llamada a un script /etc/rc.d/rc.firewall en el que se incluyen las reglas de filtrado de paquetes.

#!/bin/sh
/etc/rc.d/rc.firewall

```
#!/bin/sh
#-------------------------------------------------------------------------------
#                CONFIGURACIÓN DEL CORTAFUEGOS
#-------------------------------------------------------------------------------
# Incluir la llamada a este script en /etc/ppp/ip-up.local
#-------------------------------------------------------------------------------
```

```
# Variables de entorno activadas por pppd al establecer la comunicación
#--------------------------------------------------------------------------------------------------
# IPLOCAL <- dirección IP del interface ppp
# IFNAME <- nombre del interface local
# Asignaciones locales
LOCALNET="192.168.0.0/24"
IPADDR=$IPLOCAL
TODAS="0.0.0.0/0"
# Nombres de Interfaz
PPP=$IFNAME
ETH="eth0"
LO="lo"
# Direcciones
LOOPBACK="127.0.0.1/32"
CLASE_A="10.0.0.0/8"
CLASE_B="172.16.0.0/16"
CLASE_C="192.168.0.0/16"
MULTICAST="240.0.0.0/3"
BROADCAST_0="0.0.0.0"
BROADCAST_1="255.255.255.255"
# Puertos conocidos
ROOT="0:1023"          # Puertos reservados a root
NO_ROOT="1024:65535"   # puertos no root
NFS="2049"             # (TCP/UDP) NFS
OPENWINDOWS="2000"     # (TCP) OpenWindows
XWINDOWS="6000:6001"   # (TCP) X Window
PORTS="1020:1023"      # Rango de puertos de SSH
PORTS="6667"           # Puertos del servidor IRC
#--------------------------------------------------------------------------------------------------
# Limpiamos las reglas anteriores
#--------------------------------------------------------------------------------------------------
/sbin/ipchains -F
```

```
#------------------------------------------------------------------------------
# Establecer la política por defecto
#     Permitir entrada
#     Permitir salida
#     Denegar IP Forward
#------------------------------------------------------------------------------
/sbin/ipchains -P input   ACCEPT
/sbin/ipchains -P forward DENY
/sbin/ipchains -P output  ACCEPT
#------------------------------------------------------------------------------
#              Spoofing y direcciones ilegales
#------------------------------------------------------------------------------
# Evitar que entren paquetes de fuera indicando como dirección de origen  nuestra IP
/sbin/ipchains -A input -i $PPP -s $IPADDR -j DENY
# Evitar que lleguen de fuera paquetes con origen o destino 127.0.0.1
/sbin/ipchains -A input -i $PPP -s $LOOPBACK -j DENY
/sbin/ipchains -A input -i $PPP -d $LOOPBACK -j DENY
# Evitar que lleguen de fuera paquetes con origen o destino  de direcciones  reservadas #para
redes privadas
/sbin/ipchains -A input -i $PPP -s $CLASE_A -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_A -j DENY
/sbin/ipchains -A input -i $PPP -s $CLASE_B -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_B -j DENY
/sbin/ipchains -A input -i $PPP -s $CLASE_C -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_C -j DENY
# Evitar que salgan hacia el exterior paquetes cuyo destino   sea nuestra  propia IP
/sbin/ipchains -A output -i $PPP -d $IPADDR -j REJECT
# Evitar que salgan paquetes con origen o destino 127.0.0.1
/sbin/ipchains -A output -i $PPP -s $LOOPBACK -j REJECT
/sbin/ipchains -A output -i $PPP -d $LOOPBACK -j REJECT
# Evitar que salgan paquetes con origen o destino a   direcciones reservadas
# para redes privadas
/sbin/ipchains -A output -i $PPP -s $CLASE_A -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_A -j REJECT
```

```
/sbin/ipchains -A output -i $PPP -s $CLASE_B -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_B -j REJECT
/sbin/ipchains -A output -i $PPP -s $CLASE_C -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_C -j REJECT
# Denegar paquetes de broadcast de fuera
/sbin/ipchains -A input -i $PPP -s $BROADCAST_1 -j DENY
/sbin/ipchains -A input -i $PPP -d $BROADCAST_0 -j DENY
#-----------------------------------------------------------------------------------------------
# Poner aquí los servicios explícitamente permitidos
# auth (identd) 113, ctcp (irc) (59)
#-----------------------------------------------------------------------------------------------
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR  59 -j ACCEPT
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 113 -j ACCEPT
#-----------------------------------------------------------------------------------------------
# Rechazar acceso del exterior a servicios de nuestra máquina  Echa un vistazo con
#"netstat -a" para ver qué puertos  tienes abiertos por encima  del 1023 y por tanto
# deberíass cerrar
#-----------------------------------------------------------------------------------------------
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $ROOT -l -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $ROOT -l -j
DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $NFS -j DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $NFS -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR
$OPENWINDOWS -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $XWINDOWS
-j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $SSH -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $IRCD -j
DENY
```

```
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3128 -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3130 -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 8080 -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1024 -j DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1024 -j DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1026 -j DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1119 -j DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3401 -j DENY
#-----------------------------------------------
# Forward con enmascaramiento para la red local
#-----------------------------------------------
/sbin/ipchains -A forward -s $LOCALNET  -j MASQ
```

4. CONCLUSIONES

Los servidores Proxy son una alternativa viable para las dependencias que hacen uso frecuente de Internet, por ejemplo las Universidades. En este caso los servidores proxy son muy útiles ya que además de que el acceso a Internet es más rápido, se optimizan las direcciones IP. Es decir solamente se utiliza una dirección IP que pertenezca al dominio de la Universidad y las direcciones de la red privada pertenecerán a la subclase C. Además trae como consecuencia que el acceso al Internet sea mucho más rápido ya que como se ha venido mencionando el proxy almacena en el caché del disco las páginas ya visitadas, y no es necesario salir a buscarlas nuevamente hacia el Internet en caso de que otra persona las quiera consultar.

Otro beneficio que trae el uso del servidor proxy es que evitará que haya tráfico en la red general de la Facultad de Estudios Superiores Cuautitlán, esto gracias al manejo de dos concentradores, que como ya se explicó en uno se conectará toda la red local y en el otro sólo la red privada.

Por otra parte en las empresas los servidores proxy, además de optimizar las direcciones IP, también sirven como dispositivo de seguridad. Ya que no permiten que nadie del exterior acceda a la red privada. Esto puede ocasionar ventajas y desventajas para las empresas, por el lado de las ventajas no podrán filtrarse los hackers para saquear información importante de la empresa. Por el lado de las desventajas en caso de que alguien tenga que hacer un trabajo importante para la empresa y la información se encuentre en su red privada, no podrá acceder a su red privada.

Es importante resaltar que en el caso de las Universidades no es necesario restringir ningún tipo de servicio, ya que solamente se utiliza como caché de páginas Web. Sin embargo en el caso de las empresas si es necesario restringir los servicios, ya que como mencioné también sirve como un dispositivo de seguridad para estas. En cualquiera de las dos dependencias la configuración de un Proxy trae beneficios y perjuicios, sin embargo, la configuración de este dispositivo es un factor que debe de evaluar la dependencia que desee configurarlo

APÉNDICE 1

GLOSARIO

ADSL: Es una nueva tecnología de modems que convierte el par trenzado de la línea telefónica en el acceso a multimedia y en alta velocidad para la comunicación de datos.

Autenticación: Es un método utilizado en la criptografía en el cuál añade al final de la información un a firma electrónica , la cual se crea encriptando la información con la clave secreta. El receptor de la información puede probar a desencriptar esta firma con la llave pública del emisor. Si logra desencriptar la información, esto prueba que el emisor es la persona a la que realmente se le envío la información ya que el sólo posee su clave secreta y solo puede firmar.

Caché de disco: Capacidad para almacenar en disco las páginas visitadas en Internet

DNS: Sistema de nombres de dominio

DHCP: Protocolo diseñado para asignar dinámicamente la Internet en una RED TCP/IP

Firewalls: Mejor conocido como Pared cortafuegos, es una aplicación que filtra los intentos de establecimiento de conexión a partir de criterios definidos

FSF: Free Software Foundation. (Fundación de software Libre)

Gateway: Es un dispositivo compuesto por hardware y software el cuál sirve como puerta de enlace hacia otras redes.

GPL	Licencia Pública General
Hackers:	Los hackers son personas muy inteligentes, los cuáles se encuentran en la red, siempre atacando la seguridad de la información.
Internet	Conjunto de redes independientes de área local y área extensa que se encuentran conectadas entre sí, permitiendo el intercambio de datos y constituyendo por lo tanto una red mundial
Intranet	Es una red construida dentro de una red local, perteneciente a la subclase "C"
IP	Internet Protocol. Protocolo utilizado en conjunto con el TCP en el Internet
ISP:	Proveedor de servicio de Internet
Kernel:	Núcleo del sistema operativo Linux
LAN:	Red de área Local abarcar en su transmisión de 1m hasta un Kilómetro de distancia. Este tipo de redes por lo regular se instalan en edificios, escuelas, oficinas. Estas son consideradas como redes de alta velocidad.
Linux:	Sistema Operativo compatible con unix . Tiene dos características peculiares; la primera es que es libre y la segunda es que viene acompañado del código fuente

Módem:	Es un dispositivo de entrada - salida que convierte la información en impulsos sonoros que pueden ser transmitidos a través de línea telefónica, o viceversa, convertir las señales analógicas en digitales para que la computadora pueda interpretarlas.
PPP:	Es un protocolo de comunicación entre dos usando una interface serial. Este protocolo se encuentra documentado en el RFC 1661.este protocolo se ha diseñado para controlar el transporte de paquetes en enlaces simples entre máquinas de la misma jerarquía.
Proxy:	Aplicación que se encarga de mediar el tráfico que existe entre una red protegida y el Internet.
RDSI:	Red digital de servicios integrados. Es una tecnología que convierte las señales analógicas en digitales, trabaja a 128 kbps por segundo.
TCP/IP:	Formado por dos protocolos el TCP y el IP. Es el protocolo común utilizado por todas las computadoras que se conectan al Internet.

APÉNDICE 2

INDICE DE FIGURAS.

Pagina

Figura 1. Componentes del S.O. Linux 9
Figura 2. Funcionamiento del servidor Proxy 27
Figura 3. Pantalla que muestra la forma de asignación de direcciones IP 39
Figura 4. Pantalla que muestra los parámetros de la tarjeta de red a configurar 40
Figura 5. Información básica del equipo 41
Figura 6. Pantalla de configuración del módem 42
Figura 7. Elementos a configurar en la solapa dispositivo serie 43
Figura 8 Pantalla que se muestra al seleccionar conexiones 43
Figura 9. Mi PC 50
Figura 10. Panel de control 51
Figura 11. Ventana Seleccione Protocolo de red 51
Figura 12. Ventana Red 52
Figura 13. Pantalla propiedades TCP/IP 52
Figura 14. Resolución WINS 53
Figura 15. Pantalla RED 53
Figura 16. Pantalla opciones de configuración 54
Figura 17. Tareas como cliente 55
Figura 18. Tareas como servidor 55
Figura 19. Utilidades con las que cuenta la opción MISC 56

BIBLIOGRAFIA

1. J. Blanco Vicente, Linux, Instalación, administración y uso del sistema, Alfaomega Grupo Editor, México 1997, pp. 320.
2. Raya, José Luis, Domine TCP/IP, Alfaomega Grupo Editor, México 1998, pp.334
3. Comer E. Douglas, Redes Globales de Información con Internet y TCP/IP, Prentice-Hall Hispanoamericana, 3ª edición.
4. Siyan Karanjit, Firewalls y la Seguridad en Internet, Prentice-Hall Hispanoamericana, 2ª edición, México 1997.
5. Andrew, S, Tanenbaum, Redes de ordenadores, Prentice Hall Hispanoamericana, 2ª edición, México 1994, pp 736.
6. Cruz Sánchez Claudia, Tesis: Redes Privadas Virtuales con Linux, México 1998.
7. Uyless Black, Redes de Computadoras: Protocolos, normas e interfaces, Alfaomega Grupo Editor, México 1997, pp 585.
8. José Luis Raya Cabra, Redes locales y TCP/IP, Alfaomega Grupo Editor, México 1997, pp 185.
9. Kevin Stoltz, Todo sobre las redes de computadoras, Prentice-Hall Hispanoamericana, México 1995, pp 518.
10. Anonymous, Maximum Linux Security, SAMS, U.S.A 1999, PP. 743.
11. Stefan Strobel, Linux: unleashing the workstation in your pc, Springer, 3 rd edition, pp.587.
12. Evi Nemeth, Unix system Administration Handbook, Prentice Hall Software Series, 1989, pp.593

REFERENCIAS ELECTRONICAS.

12. http://www.linux.org.sv/Articulos/suarticulo06.htm
13. http://www.unp.edu.pe/ingindustrial/daiinfo/seminario/Linux01.html
14. http://www.jinet.prohosting.com/linux/0003.html
15. http://www.jinet.prohosting.com/linux/0004.html
16. http://www.docs.cn.va.8101/linux.howto/spanish-howto-2.html
17. http://www.nukers.com/info/aa0011.shtml
18. http://www.geocities.com/siliconvalley/circuit/3770/linux.html
19. http://www.acbius.com/enlaces.html
20. http://www.es.linuxstart.com/documentation/howtows.html
21. http://www.linux.es.com/docs/howto/traslation/es/cortafuegos-como
22. http://www.linux.focus.org/castellano/january1998/article8.htm
23. http://acer.com.mx/~nmendiz/guia-rapida-ip-masquerading-en-redhat-linux.html
24. http://www.cecafi.una.mx/internt/x3histo.html
25. http://www.cecafi.una.mx/internt/x4despu.html
26. http://www.cecafi.una.mx/internt/x6direc.html
27. http://www.infosel.com.mx/infoweb/internet/internet.html
28. http://www.monografiaas.com/trabajos/internet/internet1.shtml
29. http://www.geocities.com/sylonvaley/Bay/8259/parte1/html
30. http://www.geocities.com/sylonvaley/Bay/8259/parte2/html
31. http://www.geocities.com/sylonvaley/Bay/8259/parte3/html
32. http://www.geocities.com/sylonvaley/Bay/8259/parte4/html
33. http://www.geocities.com/cristian-t/2.html
34. http://www.geocities.com/cristian-t/4.html
35. http://www.maestrosdelweb.org/editorial/computacion/linux.asp
36. http://www.linux.es.com/que_es.html
37. http://www.linux.es.com/primeros-pasos.html
38. http://www.perso.wanadoo.es/aemulus/linux/ppal.html
39. http://www.geocities.com.sunsetstrip/stage19012/linux.html

40. http://co.worldonline.es/jkaydr77/lipp/lipp5.html
41. http://www.linux.kipelhouse.com
42. http://gaceta.piensa.com
43. http://www.fastlink.net.uy/inmyhouse/3.html
44. http://www.terra.es/personal/rigrasan
45. http://inet.prohosting.com
46. http://piramide.unizar.es/linux/introducción.html
47. http://www.croftj.net/~barreiro/spain/linux.txt
48. http://www.gut.uc3m.es/~israelgc/2.html
49. http://www.ciberdroide.com/misc/novato/curso/intro.html
50. http://metalab.unc.edu/pub/linux/docs/howto/other-formats/html-single/spanish-howto.html
51. http://www.adpsoft.com/linux.html
52. http://www.linuxperu.net/historia.html
53. http://cu.fi.udc.es/Gipol/links
54. http://memebers.es.triped.de/preguntas/linux.html
55. http://www4.uji.es/~al019803/tcp/ip.html
56. http://members.es.triped.de/janjo/janjo1.html
57. http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
58. http://www.insflug.org/como/redes.en.linux-como/redes-en-linux-como.html
59. http://lucas.hispalinux.es/com_insflug/comos/cortafuegos-como/cortafuegos-como2.html
60. http://lucas.hispalinux.es/com_insflug/comos/cortafuegos-como/cortafuegos-como3.html
61. http://lucas.hispalinux.es/com_insflug/comos/cortafuegos-como/cortafuegos-como4.html
62. http://lucas.hispalinux.es/com_insflug/comos/cortafuegos-como/cortafuegos-como5.html
63. http://lucas.hispalinux.es/com_insflug/comos/cortafuegos-como/cortafuegos-como6.html
64. http://www.solnet.com.pe/capitulo3.html
65. http://tid.telfonia.es/infovia/interconexión.rals/escenario4/solucion-proxy_cap005.html#ref0070
66. http://www.linuxylinux.com/segu/segu.htm
67. http://www.estrelladigitales/ciberestrella/secciones/como/como44.html
68. http://squid.nlanr.net/squid

69. http: segurinet.com gsal default.htm
70. http: lasalle.es/benicarlo/monograficos/ired.html
71. http: viared.cl home.html
72. http: web.jet.es s.romero articulos.html