UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

"ADMINISTRACIÓN DE SISTEMAS LINUX PARA EMPRESA DEDICADA A LAS TECNOLOGÍAS DE LA INFORMACIÓN"

DESARROLLO DE UN CASO PRÁCTICO

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

JAVIER TAPIA GONZALEZ

ASESOR:

ING. ENRIQUE GARCÍA GUZMÁN

MEXICO, 2012

INDICE

Capítulo I
Introducción

El proyecto de Administración de Sistemas Linux para una empresa dedicada a las Tecnologías de la Información a quien en lo sucesivo se denominara como MEGASOFT S.A. de C.V. fue un proyecto realizado e implementado en el mes de junio del año 2006 en la Universidad TecMilenio, como parte del programa llamado "Centro de Educación Tecnológica en Estándares Abiertos (CETEA)" que fue auspiciado por el gobierno del Distrito Federal, la empresa IBM y la Universidad TecMilenio, teniendo como sede el campus Ferrería de dicha universidad.

El proyecto fue desarrollado en el transcurso de un mes y la finalidad principal fue la de optimizar la administración y funcionamiento de los sistemas de MEGASOFT S.A. de C.V., también fue requisito para la obtener la certificación de Linux Administrator por parte de la empresa IBM y Linux Professional Institud (LPI).

El proyecto involucro conocimientos de programación, administración y planeación de redes tomando en cuenta la prevención en caso de desastre de sistemas.

En el primer capítulo se hace una *introducción al proyecto* indicando el porqué de la necesidad de implementar un nuevo sistema en la empresa MEGASOFT S.A. de C.V. así como el porqué se selecciono como plataforma de desarrollo el sistema operativo Linux, además se especifican los tiempos de entrega y los requerimientos que se debían tomar en cuenta para el desarrollo del proyecto.

En el segundo capítulo se indican los *conceptos básicos* para poder comprender los alcances del proyecto, algunas definiciones que se plantearan serán: Linux, Zona Desmilitarizada de una red (DMZ), servidor de bases de datos, Servidor Web, Mail Server, Gateway, Router, Traducción de direcciones de Red NAT.

En el tercer capítulo *especificaciones y planteamiento* del sistema se define el propósito y alcance del proyecto, se hace una descripción general del sistema indicando los resultados,

funciones y alcance que se cubrieron en base a los requerimientos que solicito MEGASOFT S.A. de C.V. también se mencionan las áreas involucradas en el proyecto, se especifican las funciones de los usuarios, las restricciones que tendrá el sistema y el resultado que se esperaba del sistema.

En el cuarto capítulo *análisis y diseño para la implementación del proyecto* se hace la definición de una solución integral y robusta para la realización del proyecto tomando en cuenta las especificaciones y requerimientos que se hicieron en el capitulo anterior además se define la plataforma y herramientas utilizadas en la implementación del proyecto y el cómo se atenderán todas las necesidades para la realización y puesta en marcha del proyecto.

En el quinto capítulo *realización y puesta* en marcha del proyecto se explicaran y mostraran los archivos de configuración y comandos utilizados para las implementaciones de los servicios de todo el sistema que cubren las especificaciones y requerimientos que el sistema debe cubrir para la puesta en marcha del proyecto.

En el sexto capítulo *conclusiones* se hace un resumen completo de todo el proyecto desde la etapa de análisis hasta etapa de implementación y puesta en marcha del proyecto, indicando los resultados obtenidos y metas alcanzadas en los ámbitos, profesionales y personales.

1.1 Acerca de la empresa.

La empresa MEGASOFT S.A. de C.V. busca siempre estar a la vanguardia tecnológica buscando alternativas de software libre para establecer sistemas con plataformas enfocadas a los estándares abiertos.
A continuación se enuncian la misión y visión de MEGASOFT S.A. de C.V. en las cuales plantean lo antes mencionado.

Misión

"En MEGASOFT buscamos llegar a un gran número de negocios y hacerlos crecer hacia un nuevo mundo de innovación tecnológica.

Estando siempre a la vanguardia para ofrecerle a usted y su empresa mejores alternativas y soluciones con sistemas hechos a la medida para sus negocios.

Contando siempre con personal altamente capacitado y avalado por empresas de nivel internacional que pondrá todos los recursos y conocimientos a el alcance de nuestros clientes."

Visión

"En MEGASOFT tenemos el compromiso de crear sistemas a la medida de su negocio y sus necesidades, que fomenten la productividad y rentabilidad de su Organización, a través de los mejores especialistas en las diferentes herramientas tecnológicas de vanguardia.

Para ello contamos con un equipo de profesionales altamente capacitados por las mejores empresas dentro del área de tecnologías de la información y estándares abiertos."

1.2 Introducción acerca del proyecto

En MEGASOFT S.A. de C.V. se tenía toda la infraestructura de red, sistemas de administración de archivos y administración de usuarios bajo la plataforma del Sistema Operativo Windows en sus versiones XP Professional y 2003 Server.

Para la elaboración del proyecto se opto por la migración de todas las aplicaciones de control de archivos y usuarios a la plataforma con el Sistema Operativo Linux en específico en su versión SuSE 9.3.

Este proyecto tuvo como finalidad brindar una solución bajo la plataforma Linux a la empresa MEGASOFT S.A. de C.V., dedicada a brindar servicios en línea a sus empleados y clientes, dicha empresa cuenta con aproximadamente 200 desarrolladores los cuales algunos son técnicos, programadores y administradores de sistemas ellos después de ver, analizar y atender una demostración del sistema operativo Linux en su versión SuSE 9.3 decidieron

implementarlo en la compañía tomando como base la rentabilidad, escalabilidad y estabilidad del sistema operativo, además de reducir costos y aumentar la eficiencia de sus sistemas.

1.3 Especificaciones generales del sistema.

Después de haber hecho un análisis de las expectativas de la empresa MEGASOFT S.A. de C.V., se hizo un informe global de los requerimientos del sistema que darían una mayor rentabilidad, eficiencia y escalabilidad al sistema de dicha empresa.

A continuación se enlistan los requerimientos que se tomaron en cuenta para la elaboración del sistema.

- El sistema debía tener la habilidad para servir a los empleados de la Empresa dedicada a las Tecnologías de la Información además de facilitar la comunicación a través de toda la red así como la administración centralizada.

- Había que limitar las direcciones IP reales para la conexión de Internet. Debido a que solo un número restringido de ellas tendría acceso a tal recurso, con este requerimiento la empresa buscaba tener menor vulnerabilidad al exponer menos terminales hacia internet.

- Se tenía que hacer posible y transparente para los usuarios la compatibilidad de dos tipos de sistemas operativos algunos usuarios usarían Microsoft Windows y otros Linux SuSE versión 9.3.

- Se debía hacer uso de una Intranet para facilitar la asignación de tareas a la gerencia de proyecto.

- Era necesario un servidor de archivos, de impresión y de correos que diera servicio a los usuarios de la intranet.

- Se elaboraría un sitio Web para los empleados y los usuarios de Internet en donde pudieran hacer consultas laborales como avisos gerenciales, días vacacionales entre algunos otros.

- Había que establecer una estrategia de recuperación del desastre para las fallas del software y del hardware.

    - Se debía implementar un alto sistema de seguridad para controlar:
    - Las peticiones de los usuarios en el sistema.
    - La conexión a Internet.
    - Las acciones de los usuarios en Internet.
    - El control de los usuarios en los servidores de la intranet de MEGASOFT S.A. de C.V.

- Se debía contar con un sistema de respaldo de datos en caso de desastres tanto en hardware o software.

- Se requería un alto grado de rentabilidad y disponibilidad del los servicios implementados en el servidor para garantizar el servicio durante las 24 horas del día los 365 días del año, haciendo posible la escalabilidad del sistema que permitiera hacer mejoras del sistema incorporando en él actualizaciones o implementaciones de nuevos servicios.

Capítulo II
Definiciones importantes

En este capítulo se abordaran las definiciones de todas las herramientas utilizadas para la implementación del sistema, iniciando por definir la plataforma en la que se implementara que es Linux.

Estas definiciones ayudaran a comprender terminologías utilizadas en los capítulos subsecuentes a este.

2.1 Linux

Linux es un sistema operativo derivado de UNIX que manteniendo casi todas las ventajas que este último ofrece, poder ser ejecutado en computadoras personales. Fue desarrollado originalmente por el estudiante finlandés de informática Linus Torvalds, que publicó su código fuente en 1990, en la forma de código abierto. Este hecho, unido a la **estructura modular** del sistema operativo (basado en la integración de componentes de software independientes) generó una nueva visión de desarrollo informático y ha permitido que Linux se haya expandido notablemente, gracias al trabajo, muchas veces voluntario y sin ánimo de lucro de miles de programadores a todo lo largo del mundo. Actualmente están disponibles varias distribuciones de Linux, ofertadas por diversos proveedores, como RedHat, SuSE o Mandrake Inc.

2.1.1 Desarrollo de Linux

La colección de utilidades para la programación de GNU es ciertamente la familia de compiladores más utilizada en GNU/Linux. Tiene capacidad para compilar C, C++, Java, Ada, entre otros muchos lenguajes. Además soporta diversas arquitecturas mediante la compilación cruzada, lo que hace que sea un entorno adecuado para desarrollos heterogéneos.

Hay varios IDEs disponibles para GNU/Linux incluyendo, Anjuta, KDevelop, NetBeans IDE y Eclipse. Además existen editores extensibles como pueda ser Emacs que hoy en día siguen siendo ampliamente utilizados. GNU/Linux también dispone de capacidades para lenguajes de guión (script), aparte de los clásicos lenguajes de programación de shell, la mayoría de las distribuciones tienen instalado Python, Perl, PHP y Ruby.

2.1.2 ¿Por qué usar Linux?

La creciente popularidad de GNU/Linux se debe a las ventajas que presenta ante otros tipos de software. Entre otras razones se debe a su estabilidad, al acceso a las fuentes (lo que permite

personalizar el funcionamiento y auditar la seguridad y privacidad de los datos tratados), a la independencia de proveedor, a la seguridad, a la rapidez con que incorpora los nuevos adelantos tecnológicos (IPv6, microprocesadores de 64 bits), a la escalabilidad (se pueden crear clusters de cientos de computadoras), a la activa comunidad de desarrollo que hay a su alrededor, a su inter operatibilidad y a la abundancia de documentación relativa a los procedimientos.

Hay varias empresas que comercializan soluciones basadas en GNU/Linux por lo tanto es así que GNU/Linux es usado por muchas personas a nivel mundial: IBM, Novell, Red Hat, Rxart, así como miles de PYMES que ofrecen productos o servicios basados en esta tecnología. Dentro del segmento de supercomputadoras, la más grande de Europa se llama *MareNostrum*. Desarrollado por IBM, está basado en un *cluster* GNU/Linux (Presentación de MareNostrum en IBM) y junto con esta muchas más supercomputadoras funcionando con Linux. Linux tiene una amplia cuota en el mercado de servidores de Internet debido, entre otras cosas, a la gran cantidad de soluciones que tiene para este segmento

2.1.3 Editor VI

VI es un editor de texto, fue originalmente escrito por Bill Joy en 1976, tomando recursos de ed y ex, dos editores de texto deficientes para Unix, que trataban de crear y editar archivos, de ahí, la creación de vi. Es un editor de texto que se encuentra en (casi) todo sistema de tipo Unix, de forma que conocer rudimentos de VI es una salvaguarda ante operaciones de emergencia en diversos sistemas operativos.

VI es un editor con dos modos: edición y comandos. En el modo de edición el texto que ingrese será agregado al archivo que este siendo modificado en ese momento, en modo de comandos las teclas que oprima pueden representar algún comando de VI.

Para iniciar a modificar un archivo deberá teclear la tecla ESC seguida de la letra i esto lo dejara en modo de edición, para pasar al modo de comandos es necesario presionar nuevamente la tecla ESC seguida de el comando que desee utilizar por citar algún ejemplo mencionare el comando w que guardara los cambios realizados al archivo hasta ese momento.

2.1.4 Comandos básicos en Linux

Para manejar el entorno Linux lo haremos sobre una terminal a la cual llamaremos consola en esta escribiremos los comandos para realizar acciones especificas que nos permitan hacer el desarrollo del sistema.

En la tabla 1.1 se muestran algunos de los comandos básicos utilizados en Linux:

<table>
<tr><th>Comando</th><th>Acción</th></tr>
<tr><td>Whoami</td><td>Dice que tipo de sesión que se tiene</td></tr>
<tr><td>Pwd</td><td>Indica el directorio en el que se encuentra</td></tr>
<tr><td>Cd</td><td>Lleva al directorio de usuario</td></tr>
<tr><td>cd..</td><td>Va a un directorio atrás</td></tr>
<tr><td>Ls</td><td>Lista los archivos y directorios</td></tr>
<tr><td>clear/cls</td><td>Borrar pantalla</td></tr>
<tr><td>Su</td><td>Cambia la sesión a modo root (se sale con CTRL+d)</td></tr>
<tr><td>ALT+(F1-F6)</td><td>Cambia de terminal desde la 1 hasta la 6</td></tr>
<tr><td>man (comando)</td><td>Muestra la ayuda sobre el comando</td></tr>
<tr><td>cp (origen) (destino)</td><td>Copia archivos</td></tr>
<tr><td>rm (nombre arch)</td><td>Borra un archivo</td></tr>
<tr><td>mv (origen) (destino)</td><td>Mueve archivos</td></tr>
<tr><td>mkdir (nombre)</td><td>Crea un directorio</td></tr>
<tr><td>chmod (nnn) (nombre archivo)</td><td>Cambia los atributos (n son números del 0-7 que representan combinaciones binarias. El primero representa los derechos del propietario, el segundo el del grupo y el tercero es para el resto de usuarios owner/group/other.
<table>
<tr><td></td><td>R</td><td>W</td><td>X</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td>2</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>3</td><td>0</td><td>1</td><td>1</td></tr>
<tr><td>4</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>5</td><td>1</td><td>0</td><td>1</td></tr>
<tr><td>6</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>7</td><td>1</td><td>1</td><td>1</td></tr>
</table>
En donde R= read (lectura)
W= write (escritura)
X= execute (ejecución)</td></tr>
<tr><td>whereis (nombre de archivo)</td><td>Busca un archivo en el sistema(devuelve el nombre de la carpeta donde está)</td></tr>
</table>

cat (nombre de archivo)	Muestra el contenido del archivo por pantalla
ps –ef	Lista los procesos activos
kill (nombre PID)=	Deja de ejecutar el proceso
Logout	cierra la sesión
shutdown -h now	Detiene el sistema (se puede apagar la máquina cuando aparece "the system is halted")
shutdown -r now	Reinicia el sistema

Tabla 1.1
Comandos de editorVI

2.2 Red de computadora

Una red de computadoras (también llamada red informática) es un conjunto de computadoras y/o dispositivos conectados por enlaces de un medio físico (medios guiados) ó inalámbricos (medios no guiados) y que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, chat, juegos), etc.

2.2.1 Zona Desmilitarizada (DMZ)

Una DMZ (del inglés Demilitarized zone) o Zona Desmilitarizada. En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet(Véase figura 2.1). El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ's den servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

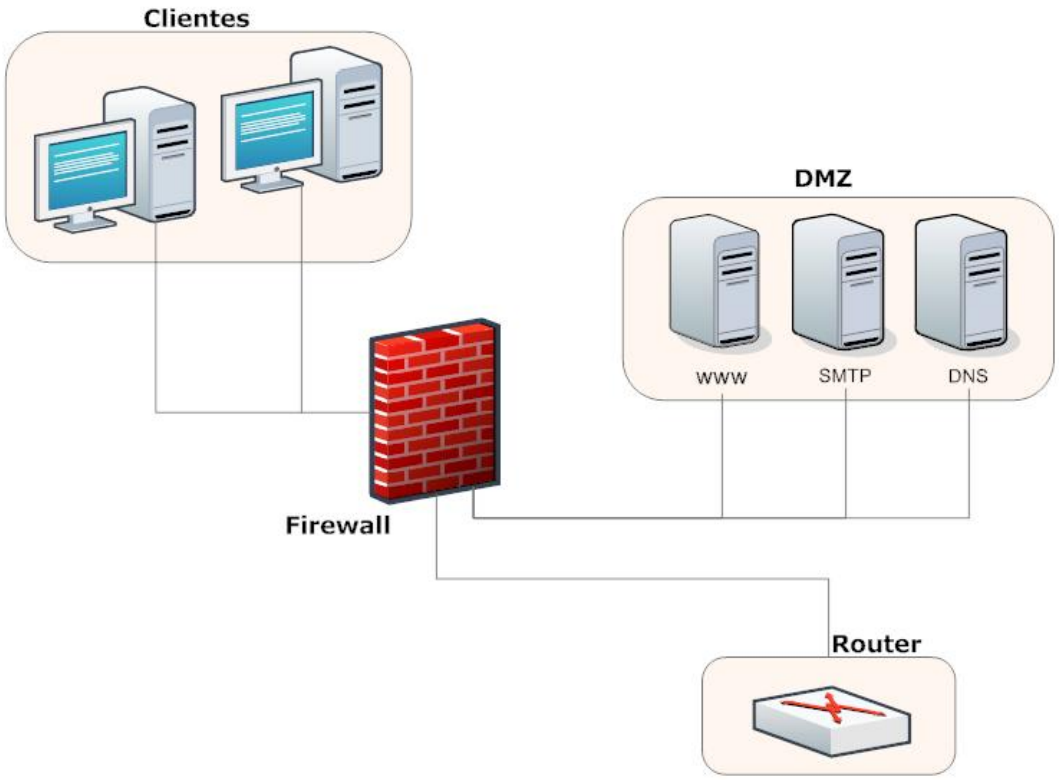

Figura 2.1

Diagrama general de una Zona Desmilitarizada (DMZ)

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama ¿cortafuegos de tres patas? (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

2.2.2 Switch

Un switch es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los data gramas en la red.

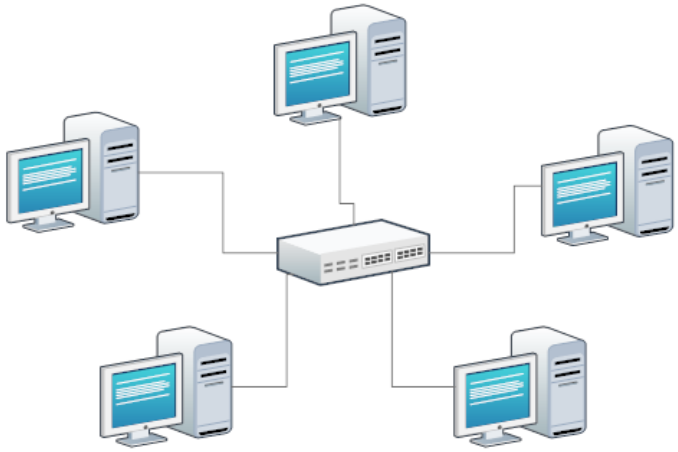

Figura 2.2

Un switch en el centro de una red en estrella.

Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los bridges, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

2.2.3 Router

El router (enrutador o encaminador) es un dispositivo hardware de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en los distintos

interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

2.3 Servidor de archivos (File Server)

Tipo de servidor en una red de computadoras cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este. En principio, cualquier computadora conectada a una red con un software apropiado, puede funcionar como servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente. Esto es que normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

2.4 Servidor de impresión (Print Server)

El servidor de impresión se encarga de gestionar los trabajos de impresión de toda la red, permitiendo que todos los usuarios, independientemente de la ubicación física de su computadora y de la plataforma utilizada, puedan imprimir en una impresora determinada.

Cuando los usuarios de la red quieren imprimir datos en una impresora de red compartida, envían sus datos a un servidor de impresora. Entonces el servidor envía los datos a una impresora compartida.

Un gestor (spooler) de impresión es el software que intercepta un trabajo de impresión que envía una aplicación por ejemplo, un procesador de textos a la impresora, y lo envía a una cola de impresión. Una cola de impresión es un búfer en el que se encuentra el trabajo de impresión hasta que la impresora esté preparada para imprimirlo.

La impresión en red consta de estos cuatro pasos:

- Una aplicación da formato a los datos del documento en una forma que pueda ser utilizada por la impresora y se los envía.
- El redirector del equipo envía los datos a la red, por donde viaja hasta el equipo servidor de impresión.
- El software de gestión de impresión del equipo servidor de impresión coloca los datos en una cola de impresión en el servidor.
- La cola de impresión guarda los datos hasta que la impresora esté preparada para imprimirlos.

Las colas de impresión suelen utilizar memoria RAM para el almacenamiento debido a que pueden mover los datos más rápido que un disco duro. Sin embargo, si se han enviado varios

trabajos a la impresora, la cola se llena, y estos documentos se envían al disco duro del servidor de impresión para que esperen su turno en la cola.

2.5 Servidor de la base de datos (Data base server)

Los Sistemas Gestores de Bases de Datos son un tipo de software muy específico, dedicado a servir de interfaz entre la Base de datos y el usuario, las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta. En los textos que tratan este tema, o temas relacionados, se mencionan los términos SGBD y DBMS, siendo ambos equivalentes, y acrónimos, respectivamente, de Sistema Gestor de Bases de Datos y DataBase Management System, su expresión inglesa.

2.5.1 Sistema de gestión de base de datos MySQL

MySQL es un sistema de gestión de base de datos, multihilo y multiusuario con más de seis millones de instalaciones. MySQL AB desarrolla MySQL como software libre en un esquema de licenciamiento dual. Por un lado lo ofrece bajo la GNU GPL, pero, empresas que quieran incorporarlo en productos privativos pueden comprar a la empresa una licencia que les permita ese uso.Está desarrollado en su mayor parte en ANSI C.

Al contrario de proyectos como el Apache, donde el software es desarrollado por una comunidad pública, y el copyright del código está en poder del autor individual, MySQL está poseído y patrocinado por una empresa privada, que posee el copyright de la mayor parte del código. Esto es lo que posibilita el esquema de licenciamiento anteriormente mencionado. Además de la venta de licencias privativas, la compañía ofrece soporte y servicios. Para sus operaciones contratan trabajadores alrededor del mundo que colaboran vía Internet. MySQL AB fue fundado por David Axmark, Allan Larsson, y Michael Widenius.

2.6 Servidor Web (Web server)

Un servidor web es un programa que implementa el protocolo HTTP (hypertext transfer protocol). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Sin embargo, el hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un formato de archivo y HTTP es un protocolo.

2.7 Servidor de correos (Mail server)

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

SMTP, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.
A diferencia de POP, se establece comunicación con el servidor y se sincronizan los cambios automáticamente.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

2.8 Gateway

Una gateway es un dispositivo, con frecuencia un servidor, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un gateway de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos. En realidad es una puerta de acceso, teniendo lugar una conversión completa de protocolos hasta la capa de aplicación del modelo de referencia OSI.

2.9 Protocolo de Internet

El Protocolo de Internet (IP, de sus siglas en inglés *Internet Protocol*) es un protocolo orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red que se basa en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en

IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del *mejor esfuerzo* (*best effort*), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de como estén de congestianadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits (lo cuál asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670 mil billones de direcciones IP's), muchas más direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

2.9.1 Dirección IP

Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el **protocolo IP** (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una *dirección IP dinámica* (normalmente se abrevia como *IP dinámica*).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una *dirección IP fija* (se aplica la misma reducción por *IP fija* o *IP estática*), es decir, no cambia con el tiempo. Los servidores de correo, dns, ftp públicos, servidores web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación. Las máquinas tienen una gran facilidad para manipular y jerarquizar la información numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP, sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar, tal es el caso URLs y resolución de nombres de dominio DNS.

Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (*Dynamic Host Configuration Protocol*).

2.9.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

DHCP son las siglas en inglés de Protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

2.9.3 Clase de direcciones IP

Hay dos diferentes clases de direcciones IP. Cada clase define la parte de la dirección IP que identifica a la RED y la parte que identifica al número de hosts dentro de esa red.

La comunidad Internet ha definido 5 clases de direcciones para poder acomodar redes de diferentes tamaños. El TCP/IP de Microsoft soporta las clases A, B y C. Estas clases, definen que bits son usados para la red y cuales son usados para identificar el número de host dentro de la red.

Se puede identificar la clase de dirección por el número del primer octeto. Así por ejemplo la clase A, son direcciones del tipo w.x.y.z en donde ‘w’ representa la RED y x.y.z el número de host dentro de la red. En la tabla 1.2 se muestran las clases A, B y C de direcciones IP.

Clase	Rango	N° de Redes	N° de Host Por Red
A	0.0.0.0 - 127.255.255.255	128	16.777.214
B	128.0.0.0 - 191.255.255.255	16.384	65.534
C	192.0.0.0 - 223.255.255.255	2.097.152	254

3 Tabla 1.2

Clase de direcciones IP

2.9.4 Direccionamiento IP y enrutamiento

Quizás los aspectos más complejos de IP son el direccionamiento y el enrutamiento. El direccionamiento se refiere a la forma como se asigna una dirección IP y como se dividen y se agrupan subredes de equipos.

El enrutamiento consiste en encontrar un camino que conecte una red con otra y aunque es llevado a cabo por todos los equipos, es realizado principalmente por enrutadores que no son más que computadores especializados en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos.

2.9.5 Enrutamiento

En comunicaciones, el encaminamiento (a veces conocido por el anglicismo ruteo o enrutamiento) es el mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Asociado al encaminamiento existe el concepto de métrica, que es una medida de lo "bueno" que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, coste, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Si la métrica es el retardo, es mejor un camino cuyo retardo total sea menor que el de otro. Lo ideal en una red es conseguir el encaminamiento óptimo: tener caminos de distancia (o coste, o retardo, o la magnitud que sea, según la métrica) mínimos. Típicamente el encaminamiento es una función implantada en la capa 3(capa de red) del modelo de referencia OSI.

2.9.6 Traducción de dirección de red (NAT)

NAT (Network Address Translation - Traducción de Dirección de Red) es un estándar creado por la Internet Engineering Task Force (IETF) el cual utiliza una o más direcciones IP para conectar varios computadores a otra red (normalmente a Internet), los cuales tienen una dirección IP completamente distinta (normalmente una IP no válida de Internet definida por el RFC 1918). Por lo tanto, se puede utilizar para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino con sus respectivos puertos. Esta combinación de números define una única conexión.

Basicamente el NAT es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP.

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (Destination NAT).

NAT tiene muchas formas de funcionamiento, entre las que destaca.

NAT estático

Realiza un mapeo en el que una dirección IP privada se traduce a una correspondiente dirección IP pública de forma unívoca. Normalmente se utiliza cuando un dispositivo necesita ser accesible desde fuera de la red privada.

NAT dinámico

Una dirección IP privada se traduce a un grupo de direcciones públicas. Por ejemplo, si un dispositivo posee la IP 192.168.10.10 puede tomar direcciones de un rango entre la IP 200.85.67.44 y 200.85.67.99. Implementando esta forma de NAT se genera automáticamente un firewall entre la red pública y la privada, ya que sólo se permite la conexión que se origina desde ésta última.

Sobrecarga

La forma más utilizada de NAT proviene del NAT dinámico, ya que toma múltiples direcciones IP privadas (normalmente entregadas mediante DHCP) y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como PAT (Port Address Translation - Traducción de Direcciones por Puerto), NAT de única dirección o NAT multiplexado a nivel de puerto.

Traslape

Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red. El ruteador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evita los conflictos de direcciones entre las distintas redes.

2.9.6.1 Razones de la creación y utilización de NAT

Con el crecimiento exponencial de Internet, y debido a que se utiliza direccionamiento IPv4, el cual ocupa 32 bits para la asignación de direcciones, dando un máximo de 4.294.967.296 direcciones únicas (2 elevado a 32), llegó el momento en que el número de direcciones no daba abasto para la cantidad de dispositivos conectados. Incluso, el número de direcciones es menor al teórico, por la forma en que se distribuyen las direcciones en clases, otras son reservadas para multicasting, y para usos especiales. Para solucionar esto se diseñó un protocolo que es capaz de asignar un número mayor de direcciones, llamado IPv6, pero tomará muchos años su implantación, por que hay que modificar completamente la infraestructura de Internet.

Finalmente se diseñó NAT, el cual permite a cualquier dispositivo, como un router, actuar como traductor de direcciones IP.

NAT es muy utilizado en empresas y redes caseras, ya que basta tener una sola dirección IP pública para poder conectar una multitud de dispositivos. Los ISP también pueden utilizar NAT para aliviar la escasez de direcciones IP para los usuarios de cable y ADSL, en este caso el ISP le asigna una dirección a cada usuario, usa direcciones no válidas de Internet. Cuando los paquetes de las máquinas de usuario salen del ISP atraviesan una caja NAT que los traduce a la verdadera dirección de Internet del ISP. En el camino de regreso, los paquetes sufren la conversión inversa. En este caso, para el resto de Internet, el ISP y sus usuarios caseros de cable y ADSL se comportan como una compañía grande.

2.10 SAMBA (Programa para la compartición de impresiones entre plataformas Windows y Linux)

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que los equipos con Linux o Mac OS X se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

Entre los sistemas tipo Unix en los que se puede ejecutar Samba, están las distribuciones GNU/Linux, Solaris y las diferentes variantes BSD entre las que podemos encontrar el Mac OS X Server de Apple.

Samba fue desarrollado originalmente para Unix por Andrew Tridgell utilizando un sniffer o capturador de tráfico para entender el protocolo a través de la ingeniería inversa. El nombre viene de insertar dos vocales al protocolo estándar que Microsoft usa para sus redes, el SMB o server message block. En un principio Samba tomó el nombre de smbserver pero tuvieron que cambiarlo por problemas con una marca registrada. Tridgell busco en el diccionario de su máquina Unix alguna palabra que incluyera las letras “s”, “m” y “b” con la orden grep hasta que dio con Samba.

Samba es una implementación de una docena de servicios y una docena de protocolos, entre los que están NetBIOS sobre TCP/IP (NetBT), SMB (también conocido como CIFS), DCE/RPC o más concretamente, MSRPC, el servidor WINS también conocido como el servidor de nombres NetBIOS (NBNS), la suite de protocolos del dominio NT, con su Logon de entrada a dominio, la base de datos del gestor de cuentas seguras (SAM), el servicio Local Security Authority (LSA) o autoridad de seguridad local, el servicio de impresoras de NT y recientemente el Logon de entrada de Active Directory, que incluye una versión modificada de Kerberos y una versión modificada de LDAP. Todos estos servicios y protocolos son frecuentemente referidos de un modo incorrecto como NetBIOS o SMB.

Samba configura directorios Unix/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estás unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux. Por ejemplo, las carpetas home pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin

embargo, deberemos cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente.

La configuración de Samba se consigue editando un solo archivo, accesible en */etc/smb.conf* o en */etc/samba/smb.conf*.

2.11 Servidor HTTP APACHE

El *servidor HTTP Apache* es un servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etcétera), Windows y otras, que implementa el protocolo HTTP/1.1 (RFC 2616) y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que originalmente Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, *a patchy server* (un servidor *parcheado*).

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: en el 2005, Apache es el servidor HTTP más usado, siendo el servidor HTTP del 70% de los sitios web en el mundo y creciendo aún su cuota de mercado.

2.12 PHP

PHP es un lenguaje de programación usado generalmente para la creación de contenido para sitios web. PHP es un acrónimo recurrente que significa "PHP Hypertext Pre-processor" (inicialmente PHP Tools, o, *P*ersonal *H*ome *P*age Tools), y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios Web. Últimamente también para la creación de otro tipo de programas incluyendo aplicaciones con interfaz gráfica usando la biblioteca GTK+.

Capítulo III

Especificaciones y planteamiento del proyecto

3.1 Propósito

El propósito del sistema era dar cumplimiento a todos y cada uno de los requerimientos dados por la empresa MEGA-SOFT S.A. de C.V., dando como resultado la integración de un sistema que fuera altamente funcional, robusto, eficiente, escalable y de vanguardia tecnológica que permitiera administrar los recursos de la empresa.

Para lograr esto se requirió hacer uso de conocimiento de redes, sistemas operativos, administración de centros de cómputo, hardware, software y seguridad de cómputo.

La empresa MEGA-SOFT S.A. de C.V. debía brindar a sus empleados y clientes la seguridad y certeza de contar con la información necesaria o requerida en todo momento, dicho sistema tenía que integrar la disponibilidad de recursos así como también ser eficiente para asegurar la integridad de dicha información, restringiendo algunos usuarios de servicios en especifico como podría ser accesos a Internet, uso de impresoras, acceso y modificación de archivos de configuración del sistema, todo esto enfocado a los usuarios de la intranet que serian los empleados en tanto a los usuarios de Internet es decir los clientes de la empresa, debían de poder acceder al sitio Web y visualizar los servicios ofrecidos por la empresa en todo momento.

3.2 Alcance

El sistema debía abarcar todas las áreas de desarrollo y planificación de sistemas además de las áreas administrativas y clientes, teniendo como metas prioritarias la optimización de recursos y bajo costo del sistema.

La intranet de la empresa debían restringir los permisos de los usuarios para una buena administración de la red así pues algunos usuarios debían poder acceder a Internet, otros más debían poder hacer uso de las impresoras y compartir archivos, en tanto que otros no.

Los clientes debían poder acceder al sitio Web de la empresa en todo momento para poder solicitar servicios u obtener información de la empresa.

3.3 Descripción General

El sistema debía disminuir costos además de mejorar la administración de los recursos de la empresa, brindando eficacia y rapidez a las peticiones de los distintos usuarios.

Se tuvieron que integrar dos tecnologías distintas de manera transparente para los usuarios esto es que sé tenía que hacer la compatibilidad entre dos sistemas operativos distintos (Windows y Linux), para que la compartición de archivos no se viera afectada entre los mismos usuarios, también el uso de dispositivos de la red como las impresoras por citar algunos.

El acceso a Internet tuvo que ser delimitado para ciertos usuarios debido al manejo de información confidencial que maneja la empresa, los usuarios de Internet que no pertenecieran a la empresa debían poder ver la información de la misma sin poder acceder a la información confidencial, para asegurar la integridad de esta.

Otra parte fundamental del sistema fue el tener respaldos de información para la prevención de desastres que pudieran afectar en la perdida de esta misma, esta parte de respaldo de información no debía implicar un costo mayor dentro del sistema, se debía mantener también la escalabilidad que contemplara los respaldos de información, así es que sé pensó en un servidor descentralizado en donde se guardara la información pertinente.

La escalabilidad del sistema debía contemplar el crecimiento de la empresa a un mediano y largo plazo haciendo que la inclusión de más usuarios dentro de la intranet resultara viable y no hubiese necesidad del cambio de la lógica del sistema.

3.4 Resultados del Producto

Al finalizar el sistema se entrego un producto eficiente, robusto, escalable y de bajo costo que da solución a todos y cada uno de los requerimientos solicitados por la empresa MEGA-SOFT S.A. de C. V.

La inclusión de los dos sistemas operativos dentro del sistema fue transparente para los usuarios, estableciendo una alta efectividad en el compartimento de archivos y recursos de la red.
La escalabilidad del sistema fue garantizada de acuerdo al diseño implementado en la red, dando paso también a la seguridad de la información y restricción de permisos hacia los usuarios.

En tanto a la parte Web el sitio de MEGA-SOFT S.A. de C.V. permite a los usuarios acceder a información de la empresa a cualquier hora

3.5 Funciones del Producto

Las funciones que tendría que realizar el sistema serian básicamente el poder brindar acceso a Internet a algunos usuarios de la intranet, compartir archivos entre usuarios no importando el sistema operativo de estos mismos

3.6 Características del usuario

Dentro del sistema se contemplaron tres niveles de usuarios cada uno de ellos con permisos distintos dentro del sistema.

- **Administradores:** estos podrán acceder a los archivos de configuración del sistema, hacer la inclusión de usuarios en la intranet, administrar los dispositivos y archivos del sistema además de delimitar que usuarios podrán salir a Internet y que usuarios no, teniendo también la función de administrar, actualizar y gestionar el sitio Web de la empresa.

- **Usuarios de la intranet (empleados):** este nivel de usuario únicamente hará uso del sistema en su parte de intranet es decir contara con un correo electrónico de la empresa pero no todos tendrá salida a Internet esto para garantizar la seguridad de la información de la empresa, los usuarios que tengan salida a Internet tendrá monitoreado el servicio para evitar saturación en la red por mal uso de este servicio.

- **Clientes:** Estos usuarios únicamente tendrán acceso al sistema en la parte del sitio Web consultando información de la empresa desde el portal de la misma.

3.7 Restricciones

Las restricciones del sistema están enfocadas a los permisos de accesos a los servicios de acuerdo a las jerarquías de usuarios.

Los usuarios con una mayor jerarquía (Administradores) podrán acceder a internet, sin tener restricción en su navegación.

Los usuarios con menor jerarquía n (Empleados) o podrían tener acceso a internet, solo podrán tener acceso a los servicios locales, como son: impresoras en red, navegación dentro de la intranet y uso de correo electrónico.

3.8 Áreas Involucradas

Las áreas involucradas dentro del sistema directamente serán el área de sistema de la empresa MEGA-SOFT S.A. de C.V. la cual deberá hacer el mantenimiento del sistema en el ámbito de sistemas, el área de telecomunicaciones que esta involucrada con el área de redes de la empresa dando soporte a la intranet, diseño gráfico, esta área será la encargada de llevar el mantenimiento del sitio Web.

Capítulo IV

Análisis y diseño para la implementación del proyecto

Como es sabido el diseño de una red es una tarea muy subjetiva. Se tienen que tomar muchos factores en cuenta ya que se pueden elegir diferentes caminos para evaluar las necesidades del negocio y las soluciones del diseño de la red. Desde todos los casos, este proceso puede estar bajo tres fases (*Véase figura 4.1*) y así fue como se planteo para el proyecto.

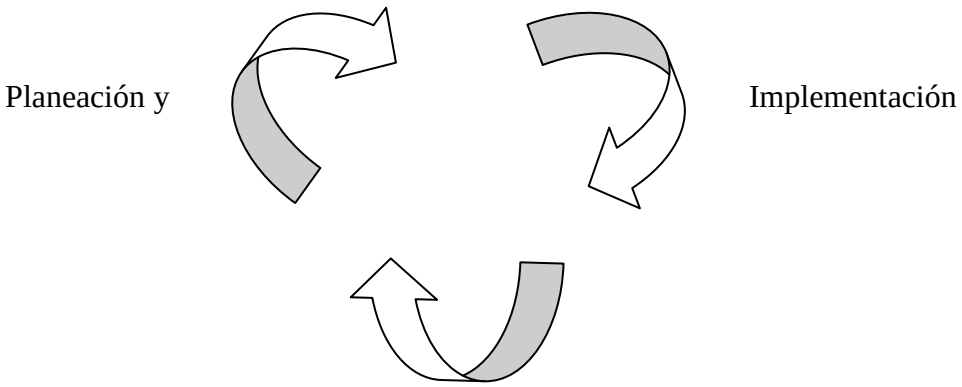

Figura 4.1

En la opción que se eligió para el diseño y análisis del proyecto se puede ver que nunca se romperá el proceso, dándonos así la posibilidad de hacer un sistema que pueda ser modificable durante cualquier etapa del mismo (*Véase figura 4.1*). Se inicio con el diseño, para después darle paso a la implementación y por ultimo al mantenimiento. Dependiendo de los cambios que se fueron efectuando en el mantenimiento se analizaron las nuevas implementaciones que hicieran más robusto el sistema y cubrieran de la mejor manera los requerimientos del mismo.

4.1 Secciones del proyecto para MEGA-SOFT

- **Sección 1:** Diseño de la infraestructura de red.
- **Sección 2:** Sistemas operativos.
- **Sección 3:** Diseño de la seguridad.

4.1.1 Sección 1: Diseño de la infraestructura de red.

En esta sección se baso en la dependencia de los servicios requeridos. Se eligió como protocolo la suite de TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de

Control de Transmisión/Protocolo Internet). Debido a que es el único protocolo que nos permitía cumplir con cada uno de los requerimientos de la empresa MEGA – SOFT.

4.1.1.1 Subredes y routers

Basado en los requerimientos se planeo tener dos zonas desmilitarizadas que contaran con los siguientes servicios cada una de ellas (*Véase Tabla 4.1*).

Además de ello tener dos routers uno para la red interna (Intranet) y el otro para la zona desmilitarizada (DMZ) que tendría la finalidad de proteger la red interna de Internet, evitando que usuarios no reconocidos en la DMZ tuviesen acceso a la misma. (*Véase figura 4.2*).

Quedando estructurado de la siguiente manera.

Equipo	Servicio	Equipo	Servicio
Router-1	IP tables	Router-1	IP tables
Router-2	IP tables	Router-2	IP tables
Dmz02	DNS esclavo Internet web server	intr02	DNS maestro DHCP Mail server
Dmz03	DNS maestro Mail gateway	Intr03	Intranet web server File server Print server Data base Server DNS esclavo

Tabla 4.1

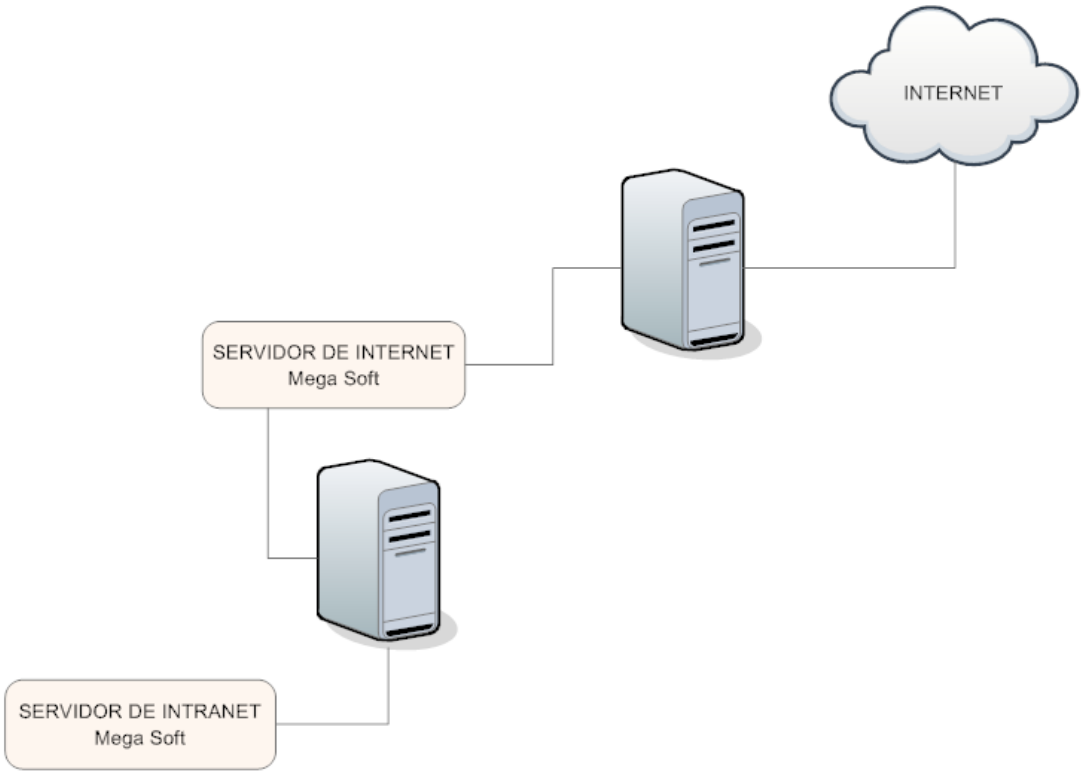
INTERNET
SERVIDOR DE INTERNET
Mega Soft
SERVIDOR DE INTRANET
Mega Soft

Figura 4.2

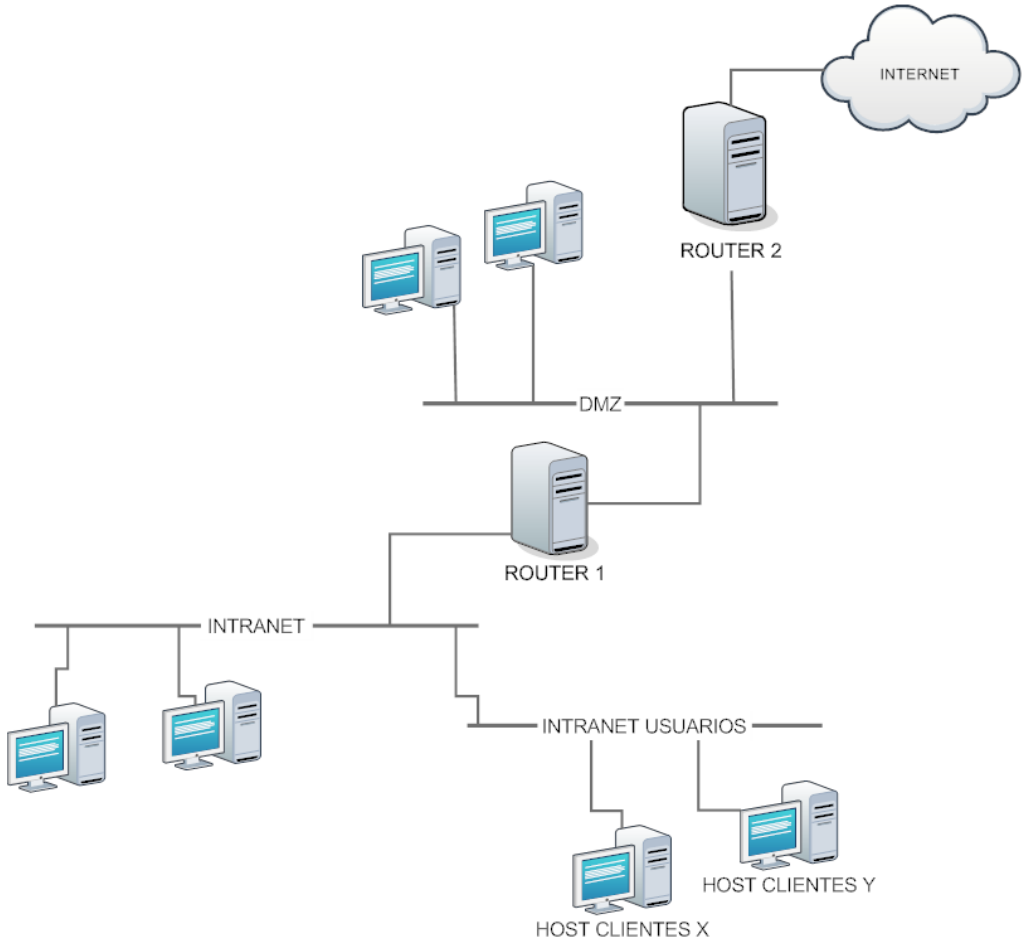

Figura 4.3

Como se ve en el diagrama(*Véase figura 4.3*), se uso una zona desmilitarizada que es la que está apuntando directamente a Internet por medio de un equipo de ruteo, el cual se conecta a un switch en el que se tienen los equipos que brindan el servicio de servidor web, DNS y gateway.

Para la red Interna (Intranet) se tiene el acceso mediante un equipo de ruteo, el cual se conecta por un switch a los equipos de la intranet, dando con ello el paso de la intranet a los servicios de Internet.

Para poder implementar lo anterior, se recurrió al uso de redes clase B, utilizando cinco equipos con los requerimientos mostrados abajo, quedando organizada de la siguiente manera (*Véase Tabla 4.2, 4.3*):

Zona Desmilitarizada:

Equipo	Red	Dirección IP	Máscara	Gateway	Broadcast
Router-1 (eth0)	172.16.16.0	172.16.16.35	255.255.255.0	200.33.146.217	172.16.16.255
Router-1 (eth1)	10.5.0.0	10.5.0.1	255.255.0.0	10.5.0.1	10.5.255.255
dmz02	10.5.0.0	10.5.0.2	255.255.0.0	10.5.0.1	10.5.255.255
dmz03	10.5.0.0	10.5.0.3	255.255.0.0	10.5.0.1	10.5.255.255
Router-2 (eth0)	10.5.0.0	10.5.0.4	255.255.0.0	10.5.0.1	10.5.255.255

Tabla 4.2

Intranet

Equipo	Red	Dirección IP	Máscara	Gateway	Broadcast
Router-2 (eth1)	10.6.0.0	10.6.0.1	255.255.0.0	10.6.0.1	10.6.255.255
intr02	10.6.0.0	10.6.0.2	255.255.0.0	10.6.0.1	10.6.255.255
intr03	10.6.0.0	10.6.0.3	255.255.0.0	10.6.0.1	10.6.255.255

Tabla 4.3

4.1.1.2 Servicio web

MEGASOFT S.A. de C.V. necesitaba el uso de una interfase Web en el orden que facilitara el proceso de recursos de autenticación y acceso a datos. Estos requerimientos necesitaban la implementación de un servidor Web. Utilizamos el servidor Web Apache. Aunque en MEGASOFT S.A. de C.V. se requería de una interfase distinta en donde se pudieran publicar productos o servicios en Internet.

4.1.1.3 Servicio de correo electrónico

El correo electrónico era uno de los requerimientos más importantes en donde se tenía que analizar la rentabilidad. Este servicio podía ser local únicamente para trabajadores de Mega-Soft o para público en general y trabajadores. Basado en los requerimientos y perspectivas de crecimiento que contemplaba MEGASOFT S.A. de C.V. se opto por la implementación de un correo Web únicamente para los empleados de MEGASOFT S.A. de C.V.

4.1.1.4 Servidor de nombres (DNS)

Cuando se diseño la red se identifico la solución para las computadoras locales y servicios en la red, dicha solución fue un servidor de nombres para usuarios locales que solucionaran

pedidos a servicios locales y un servidor de nombres para usuarios en Internet que resolviera a usuarios de Internet.

4.1.1.5 Esquema de direccionamiento

El incremento en la complejidad de la red demuestra la necesidad de automatizar y centralizar el manejo de la configuración del esquema de IP. EL Dynamic Host Configuration Protocol (DHCP) en Linux provee un manejo automático y centralizado de servicio de direcciones IP sobre TCP/IP.

4.1.1.6 Sistema de ruteo

Para la búsqueda de datos y recursos, geográficos distribuidos en la red privada se requería la conectividad entre múltiples localizaciones. El diseño del ruteo en las conexiones de la red privada fue basado en el número de localizaciones. En este proyecto se usaron las características que nos brinda Linux.

4.1.1.7 Sistema de archivos e impresión

Una de las principales razones de la popularidad de las redes es el servicio de archivos e impresiones. Estos dos servicios fueron incorporados como un solo servicio en un servidor. Basado en los requerimientos en donde se especifico que se tendrían dos tipos de sistemas operativos, se contemplo la solicitud desde un sistema Linux a un sistema Windows y viceversa, para poder hacer posible la conexión entre estos dos sistemas fue necesario la implementación del servidor SAMBA que nos da dicha solución.

4.1.2 Sección 2: Sistemas operativos.

Para la implementación de los sistemas operativos se considero que en la actualidad la mayoría de las computadoras usadas en las empresas cuentan con el sistema operativo Windows además que los usuarios están acostumbrados al ambiente que el sistema operativo Windows les ofrece así como también la compatibilidad de la mayoría de la paquetería de software.

Una parte importante era la seguridad que tenían que brindar los servidores así es que en ese aspecto se utilizo el sistema operativo Linux el cual brinda una mayor seguridad debido a que Linux fue diseñado como un sistema operativo multiusuario, y como tal los archivos "importantes" están protegidos aun cuando la identidad de un usuario se vea comprometida.

En base a lo expuesto anteriormente los sistemas operativos que se utilizaron en el proyecto para la implementación del proyecto en la empresa MEGASOFT S.A. de C.V. fueron:

- Windows XP Professional Edition
- Linux en su versión SUsE 9.3

Los equipos que utilizaron Windows XP fueron básicamente el de los usuarios de la red interna (Intranet) de MEGA – SOFT y para los equipos que actuaron como routeadores y servidores se uso el sistema operativo Linux en su versión SUsE 9.3

4.1.2.1 Requerimientos del sistema.

Las especificaciones técnicas de los equipos fueron las siguientes:

- Procesador Pentium IV 3.2 Ghz
- Disco duro de 80 Gb
- Memoria RAM 2 Gb
- Unidad de CD-ROM
- Monitor
- Teclado
- Mouse
- Tarjetas de red 10/100 Base T
- 2 Switch (mínimo)
- Impresora

4.1.3 Sección 3: Diseño de la seguridad.

La nuevas prácticas comerciales están abonando el campo para una multitud de cambios en todas las facetas de la redes de las empresas. El término seguridad de red de empresa se está generalizando a medida que las empresas tratan de entender y enfrentarse a los riesgos asociados al desarrollo rápido de las aplicaciones y prácticas comerciales que se implementan en las infraestructuras de las redes de empresa. La seguridad de red es una cuestión compleja, debido en parte a la abundancia de tecnologías de seguridad, muchas de las cuales solucionan problemas de seguridad similares y que existen como ciclo evolutivo hacia una estrategia de seguridad más general.

Recientemente los mecanismos que implementan la seguridad en la redes de empresa se han simplificado, aunque las tecnologías subyacentes sigan siendo complejas.

Este documento hace hincapié en la protección de la infraestructura corporativa. En un entorno de networking ideal, la seguridad estaría basada en hosts, y todos los servicios de seguridad se implementarían entre el emisor y el destinatario de la información.

Dentro de MEGASOFT S.A. de C.V. se desarrolló la gestión a cualquier combinación de las siguientes funciones:

- Infraestructura de networking.
- Requisitos de escritorio.
- Requisitos de seguridad.

El grupo de infraestructura de networking diseña y pone en práctica el diseño de la red corporativa. El grupo de requisitos de escritorio define las especificaciones de todas las computadoras de escritorio (PC y estaciones de trabajo) y de las aplicaciones que soportan. El grupo de requisitos de seguridad evalúa los riesgos de seguridad y crea normas de seguridad adecuada para que sean implementadas.

4.1.3.1 Seguridad física

Para asegurar que ninguna persona no autorizada tenga acceso al equipo de cómputo se tuvo que:

- Asegurar puertas
- Códigos de acceso
- Control de entradas del personal
- Protección del cableado físico
- Supresor de corriente
- Sistema de alarmas de fuego
- Aire acondicionado
- Respaldos

4.1.3.2 Seguridad de red

Para el sistema de red se aseguro que ningún usuario no permitido pudiera acceder al sistema desde:

- Internet
- Intranet

4.1.3.3 Autenticación

Se determinó que todos los usuarios se identificarían por medio de

- Usuario y password.
- Criptografía de llave pública.

Capítulo V

Realización y puesta en marcha del sistema

5.1 Archivo de configuración para el DNS

Este archivo está ubicado en el directorio /etc es el archivo de configuración principal de DNS ya que contiene la ubicación y parámetros de los demás archivos de configuración.

Este archivo contiene dos tipos de secciones:

Opciones "options": Indica el directorio donde se encuentran otros archivos de configuración y algunas otras opciones.

Zonas "zone": Pueden existir varias zonas por archivo, estas zonas definen los dominios (mega-soft.com.mx) y redes "networks" (10.6.0.0) sobre los que se mantiene información

Para acceder a este archivo y modificarlo primero deberemos escribir en la consola la siguiente instrucción:

vi /etc/named.conf, esta línea al ser ejecutada abrirá el archivo:

```
# Copyright (c) 2001-2004 SuSE Linux AG, Nuernberg, Germany.
# All rights reserved.
#
# Author: Frank Bodammer, Lars Mueller <lmuelle@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the name server BIND 9.  It works as
# a caching only name server without modification.
#
# A sample configuration for setting up your own domain can be found in
# /usr/share/doc/packages/bind/sample-config.
#
# A description of all available options can be found in
# /usr/share/doc/packages/bind/misc/options.

options {

        # The directory statement defines the name server's working directory

        directory "/var/lib/named";

        # Write dump and statistics file to the log subdirectory.  The
        # pathenames are relative to the chroot jail.
```

```
        dump-file "/var/log/named_dump.db";
        statistics-file "/var/log/named.stats";

        # The forwarders record contains a list of servers to which queries
        # should be forwarded.  Enable this line and modify the IP address to
        # your provider's name server.  Up to three servers may be listed.

        #forwarders { 192.0.2.1; 192.0.2.2; };

        # Enable the next entry to prefer usage of the name server declared in
        # the forwarders section.

        #forward first;

        # The listen-on record contains a list of local network interfaces to
        # listen on.  Optionally the port can be specified.  Default is to
        # listen on all interfaces found on your system.  The default port is
        # 53.

        #listen-on port 53 { 127.0.0.1; };

        # The listen-on-v6 record enables or disables listening on IPv6
        # interfaces.  Allowed values are 'any' and 'none' or a list of
        # addresses.

        listen-on-v6 { any; };

        # The next three statements may be needed if a firewall stands between
        # the local server and the internet.

        #query-source address * port 53;
        #transfer-source * port 53;
        #notify-source * port 53;

        # The allow-query record contains a list of networks or IP addresses
        # to accept and deny queries from. The default is to allow queries
        # from all hosts.

        #allow-query { 127.0.0.1; };

        # If notify is set to yes (default), notify messages are sent to other
        # name servers when the the zone data is changed.  Instead of setting
        # a global 'notify' statement in the 'options' section, a separate
        # 'notify' can be added to each zone definition.

        notify no;
};

# To configure named's logging remove the leading '#' characters of the
```

```
# following examples.
#logging {
#       # Log queries to a file limited to a size of 100 MB.
#       channel query_logging {
#               file "/var/log/named_querylog"
#                       versions 3 size 100M;
#               print-time yes;                 // timestamp log entries
#       };
#       category queries {
#               query_logging;
#       };
#
#       # Or log this kind alternatively to syslog.
#       channel syslog_queries {
#               syslog user;
#               severity info;
#       };
#       category queries { syslog_queries; };
#
#       # Log general name server errors to syslog.
#       channel syslog_errors {
#               syslog user;
#               severity error;
#       };
#       category default { syslog_errors;  };
#
#       # Don't log lame server messages.
#       category lame-servers { null; };
#};

# The following zone definitions don't need any modification.  The first one
# is the definition of the root name servers.  The second one defines
# localhost while the third defines the reverse lookup for localhost.

zone "." in {
        type hint;
        file "root.hint";
};

zone "mega-soft.com.mx" in {
        type master;
        file "master/named.mega-soft.com.mx";
};

zone "0.6.10.in-addr.arpa" in {
        type master;
        file "master/named.10.6.0";
};
```

```
zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

# Include the meta include file generated by createNamedConfInclude.  This
# includes all files as configured in NAMED_CONF_INCLUDE_FILES from
# /etc/sysconfig/named

include "/etc/named.conf.include";

# You can insert further zone records for your own domains below or create
# single files in /etc/named.d/ and add the file names to
# NAMED_CONF_INCLUDE_FILES.
# See /usr/share/doc/packages/bind/README.SUSE for more details.
```

5.2 Archivo de nombres de zona

Este archivo es llamado en el archivo named.conf debe ser creado en la ruta /var/lib/named/master

Para crear este archivo se debe introducir la siguiente línea en la consola del servidor:

vi /var/lib/named/master/named.mega-soft.com.mx una vez ejecutada la línea se editara el archivo de la siguiente manera:

```
$TTL 86400
@               IN SOA          intr02.mega-soft.com.mx.    root.intr02.mega-
soft.com.mx. (
                                2006061502  ; serial
                                28800       ; refresh
                                7200        ; retry
                                604800      ; expire
                                86400 )             ; minimum TTL

mega-soft.com.mx.   IN NS       dmz03.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr01.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr02.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr03.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr04.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr05.mega-soft.com.mx.
```

```
mega-soft.com.mx.    IN NS     intr06.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr07.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr08.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr09.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr10.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr12.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr13.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr14.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr15.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr16.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr17.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr18.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr19.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr20.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr21.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr22.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr23.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr24.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr25.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr26.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr27.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr28.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr29.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr30.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr31.mega-soft.com.mx.
mega-soft.com.mx.    IN MX     10 intr02.mega-soft.com.mx.

dmz03        IN A        10.5.0.3
intr01       IN A        10.6.0.1
intr02       IN A        10.6.0.2
intr03       IN A        10.6.0.3
intr04       IN A        10.6.0.4
intr05       IN A        10.6.0.5
intr06       IN A        10.6.0.6
intr07       IN A        10.6.0.7
intr08       IN A        10.6.0.8
intr09       IN A        10.6.0.9
intr10       IN A        10.6.0.10
intr11       IN A        10.6.0.11
intr12       IN A        10.6.0.12
intr13       IN A        10.6.0.13
intr14       IN A        10.6.0.14
intr15       IN A        10.6.0.15
intr16       IN A        10.6.0.16
intr17       IN A        10.6.0.17
intr18       IN A        10.6.0.18
intr19       IN A        10.6.0.19
intr20       IN A        10.6.0.20
intr21       IN A        10.6.0.21
```

```
intr22          IN A          10.6.0.22
intr23          IN A          10.6.0.23
intr24          IN A          10.6.0.24
intr25          IN A          10.6.0.25
intr26          IN A          10.6.0.26
intr27          IN A          10.6.0.27
intr28          IN A          10.6.0.28
intr29          IN A          10.6.0.29
intr30          IN A          10.6.0.30
intr31          IN A          10.6.0.31
```

5.3 Archivo de zona IP

El archivo de zona ip contiene información sobre un espacio de nombres particular y son almacenados en el directorio de trabajo named, por defecto que en este caso es /lib/named/mster/ y debe ser nombrado de acuerdo a la opción file en la declaración zone.

Para crear el archivo de zona ip se debe ejecutar la siguiente línea en la consola:

vi /var/lib/named/mster/named.10.6.0

```
$TTL 86400
@       IN      SOA    intr02.mega-soft.com.mx. root.intr02.mega-soft.com.mx (
                                        2006061501    ;       serial
                                        28800         ;       refresh
                                        7200          ;       retry
                                        604800        ;       expire
                                        86400  )      ;       minimum TTL
      IN      NS      intr01.mega-soft.com.mx.
      IN      NS     intr02.mega-soft.com.mx.
      IN      NS     intr03.mega-soft.com.mx.
      IN      NS     intr04.mega-soft.com.mx.
      IN      NS     intr05.mega-soft.com.mx.
      IN      NS     intr06.mega-soft.com.mx.
      IN      NS     intr07.mega-soft.com.mx.
      IN      NS     intr08.mega-soft.com.mx.
      IN      NS     intr09.mega-soft.com.mx.
      IN      NS     intr10.mega-soft.com.mx.
      IN      NS     intr11.mega-soft.com.mx.
      IN      NS     intr12.mega-soft.com.mx.
      IN      NS     intr13.mega-soft.com.mx.
      IN      NS     intr14.mega-soft.com.mx.
      IN      NS     intr15.mega-soft.com.mx.
      IN      NS     intr16.mega-soft.com.mx.
      IN      NS     intr17.mega-soft.com.mx.
      IN      NS     intr18.mega-soft.com.mx.
```

```
        IN      NS      intr19.mega-soft.com.mx.
        IN      NS      intr20.mega-soft.com.mx.
        IN      NS      intr21.mega-soft.com.mx.
        IN      NS      intr22.mega-soft.com.mx.
        IN      NS      intr23.mega-soft.com.mx.
        IN      NS      intr24.mega-soft.com.mx.
        IN      NS      intr25.mega-soft.com.mx.
        IN      NS      intr26.mega-soft.com.mx.
        IN      NS      intr27.mega-soft.com.mx.
        IN      NS      intr28.mega-soft.com.mx.
        IN      NS      intr29.mega-soft.com.mx.
        IN      NS      intr30.mega-soft.com.mx.
        IN      NS      intr31.mega-soft.com.mx.

1       IN      PTR     intr01.mega-soft.com.mx
2       IN      PTR     intr02.mega-soft.com.mx
3       IN      PTR     intr03.mega-soft.com.mx
4       IN      PTR     intr04.mega-soft.com.mx
5       IN      PTR     intr05.mega-soft.com.mx
6       IN      PTR     intr06.mega-soft.com.mx
7       IN      PTR     intr07.mega-soft.com.mx
8       IN      PTR     intr08.mega-soft.com.mx
9       IN      PTR     intr09.mega-soft.com.mx
10      IN      PTR     intr10.mega-soft.com.mx
11      IN      PTR     intr11.mega-soft.com.mx
12      IN      PTR     intr12.mega-soft.com.mx
13      IN      PTR     intr13.mega-soft.com.mx
14      IN      PTR     intr14.mega-soft.com.mx
15      IN      PTR     intr15.mega-soft.com.mx
16      IN      PTR     intr16.mega-soft.com.mx
17      IN      PTR     intr17.mega-soft.com.mx
18      IN      PTR     intr18.mega-soft.com.mx
19      IN      PTR     intr19.mega-soft.com.mx
20      IN      PTR     intr20.mega-soft.com.mx
21      IN      PTR     intr21.mega-soft.com.mx
22      IN      PTR     intr22.mega-soft.com.mx
23      IN      PTR     intr23.mega-soft.com.mx
24      IN      PTR     intr24.mega-soft.com.mx
25      IN      PTR     intr25.mega-soft.com.mx
26      IN      PTR     intr26.mega-soft.com.mx
27      IN      PTR     intr27.mega-soft.com.mx
28      IN      PTR     intr28.mega-soft.com.mx
29      IN      PTR     intr29.mega-soft.com.mx
30      IN      PTR     intr30.mega-soft.com.mx
31      IN      PTR     intr31.mega-soft.com.mx
```

5.4 Archivo host

El archivo hosts de un servidor es usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP. Este es uno de los diferentes métodos que usa el sistema operativo para resolver nombres de dominios.

Editar archivo hosts el cual se encuentra en la ruta:

vi /etc/hosts

```
#
# hosts       This file describes a number of hostname-to-address
#             mappings for the TCP/IP subsystem.  It is mostly
#             used at boot time, when no name servers are running.
#             On small systems, this file can be used instead of a
#             "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
10.6.0.2        intr02.mega-soft.com.mx intr02
```

Cambiar hostname con el siguiente comando.

```
Hostname intr02.mega-soft.com.mx
```

vi /etc/HOSTNAME

```
intr02.mega-soft.com.mx
```

vi /etc/resolv.conf

```
nameserver 10.6.0.2
nameserver 10.5.0.3
search mega-soft.com.mx mega-soft.com.mx
```

Iniciar el servicio de servidor de nombres

El servidor de nombres puede iniciarse desde la línea de comandos como superusuario root mediante el comando:

```
rcnamed start
```

5.5 Archivo para la configuración de DHCP

Se tendrá que editar el archivo de configuración para el rango de IP`s dinámicas de la dirección 10.6.0.50 a la 10.6.0.150.

Este archivo se encuentra en la siguiente direccion /etc/dhcpd.conf

```
option domain-name "mega-soft.com.mx";
option domain-name-servers 10.6.0.2;
max-lease-time 7200;
# if you do not use dynamical DNS updates:
#
# this statement is needed by dhcpd-3 needs at least this statement.
# you have to delete it for dhcpd-2, because it does not know it.
#
# if you want to use dynamical DNS updates, you should first read
# read /usr/share/doc/packages/dhcp-server/DDNS-howto.txt
ddns-update-style none;
ddns-updates off;
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;
# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;
default-lease-time 600;
# This is a very basic subnet declaration.
subnet 10.6.0.0 netmask 255.255.0.0 {
  option routers 10.6.0.1;
```

```
  option subnet-mask 255.255.0.0;
  range 10.6.0.50 10.6.0.150;
  default-lease-time 14400;
  max-lease-time 172800;
}
```

Iniciar el servicio con el comando:

```
rcdhcpd start
```

5.6 Configuración del Mail server

Se tendrá que editar el archivo named ubicado en esta dirección:

/var/lib/named/master/named.mega-soft.com.mx

```
$TTL 86400
@               IN SOA          intr02.mega-soft.com.mx.    root.intr02.mega-
soft.com.mx. (
                                2006061502  ; serial
                                28800       ; refresh
                                7200        ; retry
                                604800      ; expire
                                86400 )             ; minimum TTL

mega-soft.com.mx.   IN NS       dmz03.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr01.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr02.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr03.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr04.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr05.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr06.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr07.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr08.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr09.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr10.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr12.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr13.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr14.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr15.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr16.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr17.mega-soft.com.mx.
mega-soft.com.mx.   IN NS       intr18.mega-soft.com.mx.
```

```
mega-soft.com.mx.    IN NS     intr19.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr20.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr21.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr22.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr23.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr24.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr25.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr26.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr27.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr28.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr29.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr30.mega-soft.com.mx.
mega-soft.com.mx.    IN NS     intr31.mega-soft.com.mx.
mega-soft.com.mx.    IN MX     10 intr02.mega-soft.com.mx.

dmz03        IN A        10.5.0.3
intr01       IN A        10.6.0.1
intr02       IN A        10.6.0.2
intr03       IN A        10.6.0.3
intr04       IN A        10.6.0.4
intr05       IN A        10.6.0.5
intr06       IN A        10.6.0.6
intr07       IN A        10.6.0.7
intr08       IN A        10.6.0.8
intr09       IN A        10.6.0.9
intr10       IN A        10.6.0.10
intr11       IN A        10.6.0.11
intr12       IN A        10.6.0.12
intr13       IN A        10.6.0.13
intr14       IN A        10.6.0.14
intr15       IN A        10.6.0.15
intr16       IN A        10.6.0.16
intr17       IN A        10.6.0.17
intr18       IN A        10.6.0.18
intr19       IN A        10.6.0.19
intr20       IN A        10.6.0.20
intr21       IN A        10.6.0.21
intr22       IN A        10.6.0.22
intr23       IN A        10.6.0.23
intr24       IN A        10.6.0.24
intr25       IN A        10.6.0.25
intr26       IN A        10.6.0.26
intr27       IN A        10.6.0.27
intr28       IN A        10.6.0.28
intr29       IN A        10.6.0.29
intr30       IN A        10.6.0.30
intr31       IN A        10.6.0.31
```

Se realizara una prueba de conexión ingresando el siguiente comando en la consola:

```
Dig @intr02.mega-soft.com.mx
```

Editar el archivo main.cf del servicio Postfix.

Postfix es un servicio de servidor de correo de software libre / código abierto, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail.

```
# ------------------------------------------------------------------
# NOTE: Many parameters have already been added to the end of this file
#       by SuSEconfig.postfix. So take care that you don't uncomment
#       and set a parameter without checking whether it has been added
#       to the end of this file.
# ------------------------------------------------------------------
#
# Global Postfix configuration file. This file lists only a subset
# of all 300+ parameters. See the postconf(5) manual page for a
# complete list.
#
# The general format of each line is: parameter = value. Lines
# that begin with whitespace continue the previous line. A value can
# contain references to other $names or ${name}s.
#
# NOTE - CHANGE NO MORE THAN 2-3 PARAMETERS AT A TIME, AND TEST IF
# POSTFIX STILL WORKS AFTER EVERY CHANGE.

# SOFT BOUNCE
#
# The soft_bounce parameter provides a limited safety net for
# testing.  When soft_bounce is enabled, mail will remain queued that
# would otherwise bounce. This parameter disables locally-generated
# bounces, and prevents the SMTP server from rejecting mail permanently
# (by changing 5xx replies into 4xx replies). However, soft_bounce
# is no cure for address rewriting mistakes or mail routing mistakes.
#
#soft_bounce = no

# LOCAL PATHNAME INFORMATION
#
# The queue_directory specifies the location of the Postfix queue.
# This is also the root directory of Postfix daemons that run chrooted.
# See the files in examples/chroot-setup for setting up Postfix chroot
```

```
# environments on different UNIX systems.
#
queue_directory = /var/spool/postfix

# The command_directory parameter specifies the location of all
# postXXX commands.
#
command_directory = /usr/sbin

# The daemon_directory parameter specifies the location of all Postfix
# daemon programs (i.e. programs listed in the master.cf file). This
# directory must be owned by root.
#
daemon_directory = /usr/lib/postfix

# QUEUE AND PROCESS OWNERSHIP
#
# The mail_owner parameter specifies the owner of the Postfix queue
# and of most Postfix daemon processes.  Specify the name of a user
# account THAT DOES NOT SHARE ITS USER OR GROUP ID WITH OTHER ACCOUNTS
# AND THAT OWNS NO OTHER FILES OR PROCESSES ON THE SYSTEM.  In
# particular, don't specify nobody or daemon. PLEASE USE A DEDICATED
# USER.
#
mail_owner = postfix

# The default_privs parameter specifies the default rights used by
# the local delivery agent for delivery to external file or command.
# These rights are used in the absence of a recipient user context.
# DO NOT SPECIFY A PRIVILEGED USER OR THE POSTFIX OWNER.
#
#default_privs = nobody

# INTERNET HOST AND DOMAIN NAMES
#
# The myhostname parameter specifies the internet hostname of this
# mail system. The default is to use the fully-qualified domain name
# from gethostname(). $myhostname is used as a default value for many
# other configuration parameters.
#

#myhostname = intr02.mega-soft.com.mx
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
```

```
#

mydomain = mega-soft.com.mx

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
#
# For the sake of consistency between sender and recipient addresses,
# myorigin also specifies the default domain name that is appended
# to recipient addresses that have no @domain part.
#

#myorigin = $myhostname

myorigin = $mydomain

# RECEIVING MAIL

# The inet_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on.  By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#

#inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost

# The proxy_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on by way of a
# proxy or network address translation unit. This setting extends
# the address list specified with the inet_interfaces parameter.
#
# You must specify your proxy/NAT addresses when your system is a
# backup MX host for other domains, otherwise mail delivery loops
# will happen when the primary MX host is down.
#
#proxy_interfaces =
```

```
#proxy_interfaces = 1.2.3.4

# The mydestination parameter specifies the list of domains that this
# machine considers itself the final destination for.
#
# These domains are routed to the delivery agent specified with the
# local_transport parameter setting. By default, that is the UNIX
# compatible delivery agent that lookups all recipients in /etc/passwd
# and /etc/aliases or their equivalent.
#
# The default is $myhostname + localhost.$mydomain.  On a mail domain
# gateway, you should also include $mydomain.
#
# Do not specify the names of virtual domains - those domains are
# specified elsewhere (see VIRTUAL_README).
#
# Do not specify the names of domains that this machine is backup MX
# host for. Specify those names via the relay_domains settings for
# the SMTP server, or use permit_mx_backup if you are lazy (see
# STANDARD_CONFIGURATION_README).
#
# The local machine is always the final destination for mail addressed
# to user@[the.net.work.address] of an interface that the mail system
# receives mail on (see the inet_interfaces parameter).
#
# Specify a list of host or domain names, /file/name or type:table
# patterns, separated by commas and/or whitespace. A /file/name
# pattern is replaced by its contents; a type:table is matched when
# a name matches a lookup key (the right-hand side is ignored).
# Continue long lines by starting the next line with whitespace.
#
# See also below, section "REJECTING MAIL FOR UNKNOWN LOCAL USERS".
#

#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
#         mail.$mydomain, www.$mydomain, ftp.$mydomain

# REJECTING MAIL FOR UNKNOWN LOCAL USERS
#
# The local_recipient_maps parameter specifies optional lookup tables
# with all names or addresses of users that are local with respect
# to $mydestination, $inet_interfaces or $proxy_interfaces.
#
# If this parameter is defined, then the SMTP server will reject
# mail for unknown local users. This parameter is defined by default.
#
# To turn off local recipient checking in the SMTP server, specify
```

```
# local_recipient_maps = (i.e. empty).
#
# The default setting assumes that you use the default Postfix local
# delivery agent for local delivery. You need to update the
# local_recipient_maps setting if:
#
# - You define $mydestination domain recipients in files other than
#   /etc/passwd, /etc/aliases, or the $virtual_alias_maps files.
#   For example, you define $mydestination domain recipients in
#   the $virtual_mailbox_maps files.
#
# - You redefine the local delivery agent in master.cf.
#
# - You redefine the "local_transport" setting in main.cf.
#
# - You use the "luser_relay", "mailbox_transport", or "fallback_transport"
#   feature of the Postfix local delivery agent (see local(8)).
#
# Details are described in the LOCAL_RECIPIENT_README file.
#
# Beware: if the Postfix SMTP server runs chrooted, you probably have
# to access the passwd file via the proxymap service, in order to
# overcome chroot restrictions. The alternative, having a copy of
# the system passwd file in the chroot jail is just not practical.
#
# The right-hand side of the lookup tables is conveniently ignored.
# In the left-hand side, specify a bare username, an @domain.tld
# wild-card, or specify a user@domain.tld address.
#
#local_recipient_maps = unix:passwd.byname $alias_maps
#local_recipient_maps = proxy:unix:passwd.byname $alias_maps
#local_recipient_maps =

# The unknown_local_recipient_reject_code specifies the SMTP server
# response code when a recipient domain matches $mydestination or
# ${proxy,inet}_interfaces, while $local_recipient_maps is non-empty
# and the recipient address or address local-part is not found.
#
# The default setting is 550 (reject mail) but it is safer to start
# with 450 (try again later) until you are certain that your
# local_recipient_maps settings are OK.
#
unknown_local_recipient_reject_code = 550

# TRUST AND RELAY CONTROL

# The mynetworks parameter specifies the list of "trusted" SMTP
# clients that have more privileges than "strangers".
#
```

```
# In particular, "trusted" SMTP clients are allowed to relay mail
# through Postfix.  See the smtpd_recipient_restrictions parameter
# in postconf(5).
#
# You can specify the list of "trusted" network addresses by hand
# or you can let Postfix do it for you (which is the default).
#
# By default (mynetworks_style = subnet), Postfix "trusts" SMTP
# clients in the same IP subnetworks as the local machine.
# On Linux, this does works correctly only with interfaces specified
# with the "ifconfig" command.
#
# Specify "mynetworks_style = class" when Postfix should "trust" SMTP
# clients in the same IP class A/B/C networks as the local machine.
# Don't do this with a dialup site - it would cause Postfix to "trust"
# your entire provider's network.  Instead, specify an explicit
# mynetworks list by hand, as described below.
#
# Specify "mynetworks_style = host" when Postfix should "trust"
# only the local machine.
#
#mynetworks_style = class
#mynetworks_style = subnet
#mynetworks_style = host

# Alternatively, you can specify the mynetworks list by hand, in
# which case Postfix ignores the mynetworks_style setting.
#
# Specify an explicit list of network/netmask patterns, where the
# mask specifies the number of bits in the network part of a host
# address.
#
# You can also specify the absolute pathname of a pattern file instead
# of listing the patterns here. Specify type:table for table-based lookups
# (the value on the table right-hand side is not used).
#
#mynetworks = 168.100.189.0/28, 127.0.0.0/8
#mynetworks = $config_directory/mynetworks
#mynetworks = hash:/etc/postfix/network_table

# The relay_domains parameter restricts what destinations this system will
# relay mail to.  See the smtpd_recipient_restrictions description in
# postconf(5) for detailed information.
#
# By default, Postfix relays mail
# - from "trusted" clients (IP address matches $mynetworks) to any destination,
# - from "untrusted" clients to destinations that match $relay_domains or
#   subdomains thereof, except addresses with sender-specified routing.
# The default relay_domains value is $mydestination.
```

```
#
# In addition to the above, the Postfix SMTP server by default accepts mail
# that Postfix is final destination for:
# - destinations that match $inet_interfaces or $proxy_interfaces,
# - destinations that match $mydestination
# - destinations that match $virtual_alias_domains,
# - destinations that match $virtual_mailbox_domains.
# These destinations do not need to be listed in $relay_domains.
#
# Specify a list of hosts or domains, /file/name patterns or type:name
# lookup tables, separated by commas and/or whitespace.  Continue
# long lines by starting the next line with whitespace. A file name
# is replaced by its contents; a type:name table is matched when a
# (parent) domain appears as lookup key.
#
# NOTE: Postfix will not automatically forward mail for domains that
# list this system as their primary or backup MX host. See the
# permit_mx_backup restriction description in postconf(5).
#
#relay_domains = $mydestination

# INTERNET OR INTRANET

# The relayhost parameter specifies the default host to send mail to
# when no entry is matched in the optional transport(5) table. When
# no relayhost is given, mail is routed directly to the destination.
#
# On an intranet, specify the organizational domain name. If your
# internal DNS uses no MX records, specify the name of the intranet
# gateway host instead.
#
# In the case of SMTP, specify a domain, host, host:port, [host]:port,
# [address] or [address]:port; the form [host] turns off MX lookups.
#
# If you're connected via UUCP, see also the default_transport parameter.
#
#relayhost = $mydomain
#relayhost = [gateway.my.domain]
#relayhost = [mailserver.isp.tld]
#relayhost = uucphost
#relayhost = [an.ip.add.ress]

# REJECTING UNKNOWN RELAY USERS
#
# The relay_recipient_maps parameter specifies optional lookup tables
# with all addresses in the domains that match $relay_domains.
#
# If this parameter is defined, then the SMTP server will reject
# mail for unknown relay users. This feature is off by default.
```

```
#
# The right-hand side of the lookup tables is conveniently ignored.
# In the left-hand side, specify an @domain.tld wild-card, or specify
# a user@domain.tld address.
#
#relay_recipient_maps = hash:/etc/postfix/relay_recipients

# INPUT RATE CONTROL
#
# The in_flow_delay configuration parameter implements mail input
# flow control. This feature is turned on by default, although it
# still needs further development (it's disabled on SCO UNIX due
# to an SCO bug).
#
# A Postfix process will pause for $in_flow_delay seconds before
# accepting a new message, when the message arrival rate exceeds the
# message delivery rate. With the default 100 SMTP server process
# limit, this limits the mail inflow to 100 messages a second more
# than the number of messages delivered per second.
#
# Specify 0 to disable the feature. Valid delays are 0..10.
#
#in_flow_delay = 1s

# ADDRESS REWRITING
#
# The ADDRESS_REWRITING_README document gives information about
# address masquerading or other forms of address rewriting including
# username->Firstname.Lastname mapping.

# ADDRESS REDIRECTION (VIRTUAL DOMAIN)
#
# The VIRTUAL_README document gives information about the many forms
# of domain hosting that Postfix supports.

# "USER HAS MOVED" BOUNCE MESSAGES
#
# See the discussion in the ADDRESS_REWRITING_README document.

# TRANSPORT MAP
#
# See the discussion in the ADDRESS_REWRITING_README document.

# ALIAS DATABASE
#
# The alias_maps parameter specifies the list of alias databases used
# by the local delivery agent. The default list is system dependent.
#
# On systems with NIS, the default is to search the local alias
```

```
# database, then the NIS alias database. See aliases(5) for syntax
# details.
#
# If you change the alias database, run "postalias /etc/aliases" (or
# wherever your system stores the mail alias file), or simply run
# "newaliases" to build the necessary DBM or DB file.
#
# It will take a minute or so before changes become visible.  Use
# "postfix reload" to eliminate the delay.
#
#alias_maps = dbm:/etc/aliases
#alias_maps = hash:/etc/aliases
#alias_maps = hash:/etc/aliases, nis:mail.aliases
#alias_maps = netinfo:/aliases

# The alias_database parameter specifies the alias database(s) that
# are built with "newaliases" or "sendmail -bi".  This is a separate
# configuration parameter, because alias_maps (see above) may specify
# tables that are not necessarily all under control by Postfix.
#
#alias_database = dbm:/etc/aliases
#alias_database = dbm:/etc/mail/aliases
#alias_database = hash:/etc/aliases
#alias_database = hash:/etc/aliases, hash:/opt/majordomo/aliases

# ADDRESS EXTENSIONS (e.g., user+foo)
#
# The recipient_delimiter parameter specifies the separator between
# user names and address extensions (user+foo). See canonical(5),
# local(8), relocated(5) and virtual(5) for the effects this has on
# aliases, canonical, virtual, relocated and .forward file lookups.
# Basically, the software tries user+foo and .forward+foo before
# trying user and .forward.
#
#recipient_delimiter = +

# DELIVERY TO MAILBOX
#
# The home_mailbox parameter specifies the optional pathname of a
# mailbox file relative to a user's home directory. The default
# mailbox file is /var/spool/mail/user or /var/mail/user.  Specify
# "Maildir/" for qmail-style delivery (the / is required).
#
#home_mailbox = Mailbox
#home_mailbox = Maildir/

# The mail_spool_directory parameter specifies the directory where
# UNIX-style mailboxes are kept. The default setting depends on the
# system type.
```

```
#
#mail_spool_directory = /var/mail
#mail_spool_directory = /var/spool/mail

# The mailbox_command parameter specifies the optional external
# command to use instead of mailbox delivery. The command is run as
# the recipient with proper HOME, SHELL and LOGNAME environment settings.
# Exception:  delivery for root is done as $default_user.
#
# Other environment variables of interest: USER (recipient username),
# EXTENSION (address extension), DOMAIN (domain part of address),
# and LOCAL (the address localpart).
#
# Unlike other Postfix configuration parameters, the mailbox_command
# parameter is not subjected to $parameter substitutions. This is to
# make it easier to specify shell syntax (see example below).
#
# Avoid shell meta characters because they will force Postfix to run
# an expensive shell process. Procmail alone is expensive enough.
#
# IF YOU USE THIS TO DELIVER MAIL SYSTEM-WIDE, YOU MUST SET UP AN
# ALIAS THAT FORWARDS MAIL FOR ROOT TO A REAL USER.
#
#mailbox_command = /some/where/procmail
#mailbox_command = /some/where/procmail -a "$EXTENSION"

# The mailbox_transport specifies the optional transport in master.cf
# to use after processing aliases and .forward files. This parameter
# has precedence over the mailbox_command, fallback_transport and
# luser_relay parameters.
#
# Specify a string of the form transport:nexthop, where transport is
# the name of a mail delivery transport defined in master.cf.  The
# :nexthop part is optional. For more details see the sample transport
# configuration file.
#
# NOTE: if you use this feature for accounts not in the UNIX password
# file, then you must update the "local_recipient_maps" setting in
# the main.cf file, otherwise the SMTP server will reject mail for
# non-UNIX accounts with "User unknown in local recipient table".
#
#mailbox_transport = lmtp:unix:/file/name
#mailbox_transport = cyrus

# The fallback_transport specifies the optional transport in master.cf
# to use for recipients that are not found in the UNIX passwd database.
# This parameter has precedence over the luser_relay parameter.
#
# Specify a string of the form transport:nexthop, where transport is
```

```
# the name of a mail delivery transport defined in master.cf.  The
# :nexthop part is optional. For more details see the sample transport
# configuration file.
#
# NOTE: if you use this feature for accounts not in the UNIX password
# file, then you must update the "local_recipient_maps" setting in
# the main.cf file, otherwise the SMTP server will reject mail for
# non-UNIX accounts with "User unknown in local recipient table".
#
#fallback_transport = lmtp:unix:/file/name
#fallback_transport = cyrus
#fallback_transport =

# The luser_relay parameter specifies an optional destination address
# for unknown recipients.  By default, mail for unknown@$mydestination,
# unknown@[$inet_interfaces] or unknown@[$proxy_interfaces] is returned
# as undeliverable.
#
# The following expansions are done on luser_relay: $user (recipient
# username), $shell (recipient shell), $home (recipient home directory),
# $recipient (full recipient address), $extension (recipient address
# extension), $domain (recipient domain), $local (entire recipient
# localpart), $recipient_delimiter. Specify ${name?value} or
# ${name:value} to expand value only when $name does (does not) exist.
#
# luser_relay works only for the default Postfix local delivery agent.
#
# NOTE: if you use this feature for accounts not in the UNIX password
# file, then you must specify "local_recipient_maps =" (i.e. empty) in
# the main.cf file, otherwise the SMTP server will reject mail for
# non-UNIX accounts with "User unknown in local recipient table".
#
#luser_relay = $user@other.host
#luser_relay = $local@other.host
#luser_relay = admin+$local

# JUNK MAIL CONTROLS
#
# The controls listed here are only a very small subset. The file
# SMTPD_ACCESS_README provides an overview.

# The header_checks parameter specifies an optional table with patterns
# that each logical message header is matched against, including
# headers that span multiple physical lines.
#
# By default, these patterns also apply to MIME headers and to the
# headers of attached messages. With older Postfix versions, MIME and
# attached message headers were treated as body text.
#
```

```
# For details, see "man header_checks".
#
#header_checks = regexp:/etc/postfix/header_checks

# FAST ETRN SERVICE
#
# Postfix maintains per-destination logfiles with information about
# deferred mail, so that mail can be flushed quickly with the SMTP
# "ETRN domain.tld" command, or by executing "sendmail -qRdomain.tld".
# See the ETRN_README document for a detailed description.
#
# The fast_flush_domains parameter controls what destinations are
# eligible for this service. By default, they are all domains that
# this server is willing to relay mail to.
#
#fast_flush_domains = $relay_domains

# SHOW SOFTWARE VERSION OR NOT
#
# The smtpd_banner parameter specifies the text that follows the 220
# code in the SMTP server's greeting banner. Some people like to see
# the mail version advertised. By default, Postfix shows no version.
#
# You MUST specify $myhostname at the start of the text. That is an
# RFC requirement. Postfix itself does not care.
#
#smtpd_banner = $myhostname ESMTP $mail_name
#smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)

# PARALLEL DELIVERY TO THE SAME DESTINATION
#
# How many parallel deliveries to the same user or domain? With local
# delivery, it does not make sense to do massively parallel delivery
# to the same user, because mailbox updates must happen sequentially,
# and expensive pipelines in .forward files can cause disasters when
# too many are run at the same time. With SMTP deliveries, 10
# simultaneous connections to the same domain could be sufficient to
# raise eyebrows.
#
# Each message delivery transport has its XXX_destination_concurrency_limit
# parameter.  The default is $default_destination_concurrency_limit for
# most delivery transports. For the local delivery agent the default is 2.

#local_destination_concurrency_limit = 2
#default_destination_concurrency_limit = 20

# DEBUGGING CONTROL
#
# The debug_peer_level parameter specifies the increment in verbose
```

```
# logging level when an SMTP client or server host name or address
# matches a pattern in the debug_peer_list parameter.
#
debug_peer_level = 2

# The debug_peer_list parameter specifies an optional list of domain
# or network patterns, /file/name patterns or type:name tables. When
# an SMTP client or server host name or address matches a pattern,
# increase the verbose logging level by the amount specified in the
# debug_peer_level parameter.
#
#debug_peer_list = 127.0.0.1
#debug_peer_list = some.domain

# The debugger_command specifies the external command that is executed
# when a Postfix daemon program is run with the -D option.
#
# Use "command .. & sleep 5" so that the debugger can attach before
# the process marches on. If you use an X-based debugger, be sure to
# set up your XAUTHORITY environment variable before starting Postfix.
#
debugger_command =
	PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
	xxgdb $daemon_directory/$process_name $process_id & sleep 5

# If you can't use X, use this to capture the call stack when a
# daemon crashes. The result is in a file in the configuration
# directory, and is named after the process name and the process ID.
#
# debugger_command =
#	PATH=/bin:/usr/bin:/usr/local/bin; export PATH; (echo cont;
#	echo where) | gdb $daemon_directory/$process_name $process_id 2>&1
#	>$config_directory/$process_name.$process_id.log & sleep 5
#
# Another possibility is to run gdb under a detached screen session.
# To attach to the screen sesssion, su root and run "screen -r
# <id_string>" where <id_string> uniquely matches one of the detached
# sessions (from "screen -list").
#
# debugger_command =
#	PATH=/bin:/usr/bin:/sbin:/usr/sbin; export PATH; screen
#	-dmS $process_name gdb $daemon_directory/$process_name
#	$process_id & sleep 1

# INSTALL-TIME CONFIGURATION INFORMATION
#
# The following parameters are used when installing a new Postfix version.
#
# sendmail_path: The full pathname of the Postfix sendmail command.
```

```
# This is the Sendmail-compatible mail posting interface.
#
sendmail_path = /usr/sbin/sendmail

# newaliases_path: The full pathname of the Postfix newaliases command.
# This is the Sendmail-compatible command to build alias databases.
#
newaliases_path = /usr/bin/newaliases

# mailq_path: The full pathname of the Postfix mailq command.  This
# is the Sendmail-compatible mail queue listing command.
#
mailq_path = /usr/bin/mailq

# setgid_group: The group for mail submission and queue management
# commands.  This must be a group name with a numerical group ID that
# is not shared with other accounts, not even with the Postfix account.
#
setgid_group = maildrop

# html_directory: The location of the Postfix HTML documentation.
#
html_directory = /usr/share/doc/packages/postfix/html

# manpage_directory: The location of the Postfix on-line manual pages.
#
manpage_directory = /usr/share/man

# sample_directory: The location of the Postfix sample configuration files.
# This parameter is obsolete as of Postfix 2.1.
#
sample_directory = /usr/share/doc/packages/postfix/samples

# readme_directory: The location of the Postfix README files.
#
readme_directory = /usr/share/doc/packages/postfix/README_FILES
inet_protocols = all
biff = no
mail_spool_directory = /var/mail
canonical_maps = hash:/etc/postfix/canonical
virtual_maps = hash:/etc/postfix/virtual
relocated_maps = hash:/etc/postfix/relocated
transport_maps = hash:/etc/postfix/transport
sender_canonical_maps = hash:/etc/postfix/sender_canonical
masquerade_exceptions = root
masquerade_classes = envelope_sender, header_sender, header_recipient
myhostname = intr02.mega-soft.com.mx
program_directory = /usr/lib/postfix
```

```
# inet_interfaces = 127.0.0.1 ::1
inet_interfaces = all

masquerade_domains =
mydestination = $myhostname, localhost.$mydomain, $mydomain
defer_transports =
disable_dns_lookups = no
relayhost = dmz03.mega-soft.com.mx
mailbox_command =
mailbox_transport =
smtpd_sender_restrictions = hash:/etc/postfix/access
smtpd_client_restrictions =
smtpd_helo_required = no
smtpd_helo_restrictions =
strict_rfc821_envelopes = no
smtpd_recipient_restrictions = permit_mynetworks,reject_unauth_destination
smtp_sasl_auth_enable = no
smtpd_sasl_auth_enable = no
smtpd_use_tls = no
smtp_use_tls = no
alias_maps = hash:/etc/aliases
mailbox_size_limit = 0
message_size_limit = 10240000
```

Después de editar el archivo anterior se deben realizar las siguientes acciones.

Reiniciar postfix

```
Rcpostfix restart
```

Configurar Stunnel

Stunnel puede ser utilizado para proveer conexiones cifradas seguras para clientes o servidores que no utilizan TLS o SSL de forma nativa. Corre en una gran variedad de sistemas operativos, incluyendo a la mayoría de los basados en el sistema operativo Linux.

Para proveer de una conexión SSL segura a un servidor de correo SMTP existente, Stunnel deberá mapear el puerto 443 de SSL al puerto 25 del servidor de correo.

Crear certificado

```
Openssl req –newkey rsa 1024 –keyout stunnel.pem –nodes –x509 –days 365 –out stunnel.pem
```

Se debe modificar el archivo stunnel.conf tecleando vi stunnel.conf en la consola de usuario:

```
# Sample stunnel configuration file
# Copyright by Michal Trojnara 2002
# --with changes for SuSE package

# client = yes | no
# client mode (remote service uses SSL)
# default: no (server mode)
client = no

#
# chroot + user (comment out to disable)
#
chroot = /var/lib/stunnel/
setuid = stunnel
setgid = nogroup
# note about the chroot feature and the "exec" keyword to start other services...
# while the init script /etc/init.d/stunnel will copy the binaries and libraries
# into the chroot jail, more files might be needed in the jail (configuration
# files etc.)

pid = /var/run/stunnel.pid

#
# debugging
#
#debug = 7
#output = stunnel.log

# Workaround for Eudora bug
#options = DONT_INSERT_EMPTY_FRAGMENTS

#
# Authentication stuff
#
#verify = 2
# don't forget about c_rehash CApath
# it is located inside chroot jail:
#CApath = /certs
# or simply use CAfile instead:
#CAfile = /etc/stunnel/certs.pem

cert = /etc/stunnel/stunnel.pem

#
# Examples for service-level configuration:
#
```

```
[pop3s]
accept  = 995
connect = 110

# [imaps]
# accept  = 993
# connect = 143

# [imaps]
# accept = 993
# exec = /usr/sbin/imapd
# execargs = imapd
# pty = no

# [ssmtp]
# accept  = 465
# connect = 25

# [s1]
# accept  = 5000
# connect = mail.example.com:110
# delay = yes

# [s2]
# accept  = 5001
# connect = mail.example.com:25

# [https]
# accept  = 443
# connect = 80
# TIMEOUTclose = 0

# [swat]
# accept  = 902
# connect = 901

#
# mysql over stunnel example:
#
# [mysqls]                          ← on the server
#       accept = 3307
#       connect = localhost:mysql
#
# client = yes                      ← on the client
# [mysqls]
#       accept = 3307
#       connect = remote-mysql-server.example.com:3307
#
```

```
# Hint. Use the mysql client with "-h 127.0.0.1", not "-h localhost", because
# "localhost" will mean it will go through the local socket and ignore the port.

#
# pppd over stunnel example:
# (note: read http://sites.inka.de/sites/bigred/devel/tcp-tcp.html , and
# look for better alternatives like cipe or openvpn.)
#
# [ppp]                         ← on the server
# accept = 2020
# exec = /usr/sbin/pppd
# execargs = pppd local
# # the pty option doesn't work in chroot jail without further efforts
# #pty = yes
#
#
# [ppp]                         ← on the "client"
# connect = host.example.com:2020
# exec = /usr/sbin/pppd
# execargs = pppd local nodeflate nobsdcomp 192.168.20.20:192.168.20.21
# # the pty option doesn't work in chroot jail without further efforts
# #pty = yes
```

Tambien se debe modificar el archivo Access del servicio Postfix

vi access

```
# ACCESS(5)                                   ACCESS(5)
#
# NAME
#       access - Postfix access table format
#
# SYNOPSIS
#       postmap /etc/postfix/access
#
#       postmap -q "string" /etc/postfix/access
#
#       postmap -q - /etc/postfix/access <inputfile
#
# DESCRIPTION
#       The  optional  access(5)  table  directs  the Postfix SMTP
#       server to selectively reject or accept mail. Access can be
#       allowed  or  denied for specific host names, domain names,
#       networks, host addresses or mail addresses.
#
#       For an example, see the EXAMPLE section at the end of this
```

```
#       manual page.
#
#       Normally,  the access(5) table is specified as a text file
#       that serves as  input  to  the  postmap(1)  command.  The
#       result,  an  indexed file in dbm or db format, is used for
#       fast searching by the mail  system.  Execute  the  command
#       "postmap  /etc/postfix/access"  in  order  to  rebuild the
#       indexed file after changing the access table.
#
#       When the table is provided via other means  such  as  NIS,
#       LDAP  or  SQL,  the  same lookups are done as for ordinary
#       indexed files.
#
#       Alternatively, the table can be  provided  as  a  regular-
#       expression map where patterns are given as regular expres-
#       sions, or lookups can be directed to TCP-based server.  In
#       that  case,  the  lookups are done in a slightly different
#       way as described below under "REGULAR  EXPRESSION  TABLES"
#       and "TCP-BASED TABLES".
#
# TABLE FORMAT
#       The input format for the postmap(1) command is as follows:
#
#       pattern action
#            When pattern matches a mail address, domain or host
#            address, perform the corresponding action.
#
#       blank lines and comments
#            Empty  lines and whitespace-only lines are ignored,
#            as are lines whose first  non-whitespace  character
#            is a `#'.
#
#       multi-line text
#            A  logical  line starts with non-whitespace text. A
#            line that starts with whitespace continues a  logi-
#            cal line.
#
# EMAIL ADDRESS PATTERNS
#       With lookups from indexed files such as DB or DBM, or from
#       networked tables such as NIS, LDAP or  SQL,  patterns  are
#       tried in the order as listed below:
#
#       user@domain
#            Matches the specified mail address.
#
#       domain.tld
#            Matches  domain.tld  as the domain part of an email
#            address.
#
```

```
#           The pattern domain.tld also matches subdomains, but
#           only when the string smtpd_access_maps is listed in
#           the Postfix  parent_domain_matches_subdomains  con-
#           figuration  setting  (note that this is the default
#           for some versions of Postfix).  Otherwise,  specify
#           .domain.tld  (note  the  initial  dot)  in order to
#           match subdomains.
#
#       user@  Matches all mail addresses with the specified  user
#           part.
#
#       Note:  lookup  of  the null sender address is not possible
#       with some types of lookup table. By default, Postfix  uses
#       <> as  the  lookup  key  for such addresses. The value is
#       specified with the smtpd_null_access_lookup_key  parameter
#       in the Postfix main.cf file.
#
# EMAIL ADDRESS EXTENSION
#       When a mail address localpart contains the optional recip-
#       ient delimiter (e.g., user+foo@domain), the  lookup  order
#       becomes:  user+foo@domain, user@domain, domain, user+foo@,
#       and user@.
#
# HOST NAME/ADDRESS PATTERNS
#       With lookups from indexed files such as DB or DBM, or from
#       networked  tables  such as NIS, LDAP or SQL, the following
#       lookup patterns are examined in the order as listed:
#
#       domain.tld
#           Matches domain.tld.
#
#           The pattern domain.tld also matches subdomains, but
#           only when the string smtpd_access_maps is listed in
#           the Postfix  parent_domain_matches_subdomains  con-
#           figuration setting.  Otherwise, specify .domain.tld
#           (note the initial dot) in  order  to  match  subdo-
#           mains.
#
#       net.work.addr.ess
#
#       net.work.addr
#
#       net.work
#
#       net    Matches  the specified IPv4 host address or subnet-
#           work. An IPv4 host address is a  sequence  of  four
#           decimal octets separated by ".".
#
#           Subnetworks  are  matched  by repeatedly truncating
```

```
#           the last ".octet" from the remote IPv4 host address
#           string  until a match is found in the access table,
#           or until further truncation is not possible.
#
#           NOTE 1: The information in the access map should be
#           in canonical form, with unnecessary null characters
#           eliminated.  Address information must  not  be
#           enclosed with "[]" characters.
#
#           NOTE  2:  use the cidr lookup table type to specify
#           network/netmask  patterns.  See  cidr_table(5)  for
#           details.
#
#       net:work:addr:ess
#
#       net:work:addr
#
#       net:work
#
#       net    Matches  the specified IPv6 host address or subnet-
#           work. An IPv6 host address is a sequence  of  three
#           to  eight hexadecimal octet pairs separated by ":".
#
#           Subnetworks are matched  by  repeatedly  truncating
#           the  last  ":octetpair"  from  the remote IPv6 host
#           address string until a match is found in the access
#           table, or until further truncation is not possible.
#
#           NOTE 1: the truncation and comparison are done with
#           the string representation of the IPv6 host address.
#           Thus, not all the ":" subnetworks will be tried.
#
#           NOTE 2: The information in the access map should be
#           in canonical form, with unnecessary null characters
#           eliminated.  Address information must  not  be
#           enclosed with "[]" characters.
#
#           NOTE  3:  use the cidr lookup table type to specify
#           network/netmask  patterns.  See  cidr_table(5)  for
#           details.
#
#           IPv6 support is available in Postfix 2.2 and later.
#
# ACCEPT ACTIONS
#       OK     Accept the address etc. that matches the pattern.
#
#       all-numerical
#           An all-numerical result is treated as OK. This for-
#           mat  is generated by address-based relay authoriza-
```

```
#           tion schemes.
#
# REJECT ACTIONS
#       4NN text
#
#       5NN text
#           Reject the address etc. that matches  the  pattern,
#           and respond with the numerical three-digit code and
#           text. 4NN means "try again later", while 5NN  means
#           "do not try again".
#
#       REJECT optional text...
#           Reject  the  address etc. that matches the pattern.
#           Reply with $reject_code optional text...  when  the
#           optional  text is specified, otherwise reply with a
#           generic error response message.
#
#       DEFER_IF_REJECT optional text...
#           Defer the request if some later  restriction  would
#           result in a REJECT action. Reply with "450 optional
#           text... when the optional text is specified, other-
#           wise reply with a generic error response message.
#
#           This feature is available in Postfix 2.1 and later.
#
#       DEFER_IF_PERMIT optional text...
#           Defer the request if some later  restriction  would
#           result  in a an explicit or implicit PERMIT action.
#           Reply with "450 optional text... when the  optional
#           text  is  specified, otherwise reply with a generic
#           error response message.
#
#           This feature is available in Postfix 2.1 and later.
#
# OTHER ACTIONS
#       restriction...
#           Apply the named UCE restriction(s) (permit, reject,
#           reject_unauth_destination, and so on).
#
#       DISCARD optional text...
#           Claim successful delivery and silently discard  the
#           message.   Log the optional text if specified, oth-
#           erwise log a generic message.
#
#           Note: this action currently affects all  recipients
#           of the message.
#
#           This feature is available in Postfix 2.0 and later.
#
```

```
#       DUNNO  Pretend that the lookup key  was  not  found.  This
#            prevents  Postfix  from  trying  substrings  of the
#            lookup key (such as a subdomain name, or a  network
#            address subnetwork).
#
#            This feature is available in Postfix 2.0 and later.
#
#       FILTER transport:destination
#            After the message is queued, send the  entire  mes-
#            sage through the specified external content filter.
#            The transport:destination syntax  is  described  in
#            the  transport(5)  manual  page.   More information
#            about external content filters is  in  the  Postfix
#            FILTER_README file.
#
#            Note:  this  action  overrides  the  main.cf  con-
#            tent_filter  setting,  and  currently  affects  all
#            recipients of the message.
#
#            This feature is available in Postfix 2.0 and later.
#
#       HOLD optional text...
#            Place the message on the hold queue, where it  will
#            sit  until someone either deletes it or releases it
#            for delivery.  Log the optional text if  specified,
#            otherwise log a generic message.
#
#            Mail  that  is  placed on hold can be examined with
#            the postcat(1) command, and  can  be  destroyed  or
#            released with the postsuper(1) command.
#
#            Note:  use  "postsuper -r" to release mail that was
#            kept on hold for a significant fraction  of  $maxi-
#            mal_queue_lifetime  or  $bounce_queue_lifetime,  or
#            longer.
#
#            Note: this action currently affects all  recipients
#            of the message.
#
#            This feature is available in Postfix 2.0 and later.
#
#       PREPEND headername: headervalue
#            Prepend the specified message header  to  the  mes-
#            sage.  When this action is used multiple times, the
#            first prepended header appears  before  the  second
#            etc. prepended header.
#
#            Note:  this action does not support multi-line mes-
#            sage headers.
```

```
#
#           This feature is available in Postfix 2.1 and later.
#
#       REDIRECT user@domain
#           After  the  message  is queued, send the message to
#           the  specified  address  instead  of  the  intended
#           recipient(s).
#
#           Note:  this action overrides the FILTER action, and
#           currently affects all recipients of the message.
#
#           This feature is available in Postfix 2.1 and later.
#
#       WARN optional text...
#           Log a warning with the optional text, together with
#           client information and  if  available,  with  helo,
#           sender, recipient and protocol information.
#
#           This feature is available in Postfix 2.1 and later.
#
# REGULAR EXPRESSION TABLES
#       This section describes how the table lookups  change  when
#       the table is given in the form of regular expressions. For
#       a description of regular expression lookup  table  syntax,
#       see regexp_table(5) or pcre_table(5).
#
#       Each  pattern  is  a regular expression that is applied to
#       the entire string being looked up. Depending on the appli-
#       cation,  that  string  is  an  entire  client hostname, an
#       entire client IP address, or an entire mail address. Thus,
#       no  parent  domain  or  parent  network  search  is  done,
#       user@domain mail addresses are not broken  up  into  their
#       user@ and domain constituent parts, nor is user+foo broken
#       up into user and foo.
#
#       Patterns are applied in the  order  as  specified  in  the
#       table,  until  a  pattern is found that matches the search
#       string.
#
#       Actions are the same as with indexed  file  lookups,  with
#       the  additional feature that parenthesized substrings from
#       the pattern can be interpolated as $1, $2 and so on.
#
# TCP-BASED TABLES
#       This section describes how the table lookups  change  when
#       lookups are directed to a TCP-based server. For a descrip-
#       tion  of  the  TCP  client/server  lookup  protocol,   see
#       tcp_table(5).   This  feature  is  not available up to and
#       including Postfix version 2.2.
```

```
#
#       Each lookup operation uses the entire query  string  once.
#       Depending  on  the  application,  that string is an entire
#       client hostname, an entire client IP address, or an entire
#       mail  address.   Thus,  no parent domain or parent network
#       search is done, user@domain mail addresses are not  broken
#       up  into  their user@ and domain constituent parts, nor is
#       user+foo broken up into user and foo.
#
#       Actions are the same as with indexed file lookups.
#
# EXAMPLE
#       The following example uses an indexed file,  so  that  the
#       order  of  table entries does not matter. The example per-
#       mits access by the client at address 1.2.3.4  but  rejects
#       all  other  clients  in 1.2.3.0/24. Instead of hash lookup
#       tables, some systems use dbm.  Use the  command  "postconf
#       -m"  to  find  out  what lookup tables Postfix supports on
#       your system.
#
#       /etc/postfix/main.cf:
#          smtpd_client_restrictions =
#             check_client_access hash:/etc/postfix/access
#
#       /etc/postfix/access:
#          1.2.3   REJECT
#          1.2.3.4 OK
#
#       Execute the command "postmap /etc/postfix/access" after
#       editing the file.
#
# BUGS
#       The table format does not understand quoting  conventions.
#
# SEE ALSO
#       postmap(1), Postfix lookup table manager
#       smtpd(8), SMTP server
#       postconf(5), configuration parameters
#       transport(5), transport:nexthop syntax
#
# README FILES
#       Use  "postconf  readme_directory" or "postconf html_direc-
#       tory" to locate this information.
#       SMTPD_ACCESS_README, built-in SMTP server access control
#       DATABASE_README, Postfix lookup table overview
#
# LICENSE
#       The Secure Mailer license must be  distributed  with  this
#       software.
```

```
#
# AUTHOR(S)
#       Wietse Venema
#       IBM T.J. Watson Research
#       P.O. Box 704
#       Yorktown Heights, NY 10598, USA
#
#
#                                       ACCESS(5)
mega-soft.com.mx RELAY
```

5.7 Archivos para la configuración del servicio File server

Se realizo el backup de /etc/samba/smb.conf

Se inicio el archivo de smb.conf desde cero y este es el contenido actual:

```
[global]
        netbios name = intr03
        workgroup = MEGA-SOFT
        security = user
        local master = yes
        printing = cups
        load printers = no
        encrypt passwords = yes
        smb passwd file = /etc/samba/smbpasswd

[homes]
        path = /home/%U
        comment = Home Directory of %U
        browsable = no
        writable = yes
        valid users = %S

[mp370]
        path = /var/spool/samba
        writable = no
        guest ok = yes
        printable = yes
```

Se crearon 5 usuarios para fines de prueba nombrados cliente[n] dentro del grupo users:

useradd –m –c “Samba Cliente [n]” –g users cliente[n]

Se agregan los usuarios creados anteriormente a Samba:

smbpasswd –a cliente[n]

Se agrega al usuario guest para los usuarios que no se autentifiquen como usuarios validos

useradd guest
smbpasswd –a guest

Se dan de alta los clientes[n] como usuarios de Windows

Se mapea el grupo “Print Operators” de windows al grupo “lp” de linux

Net groupmap add unixgroup=”lp” ntgroup=”Print Operators”

Se crea un directorio para los drivers de la impresora, con la siguiente estructura:

```
mkdir /etc/samba/drivers--+
                          +--W32X86
                          +--WIN40
                          +--W32ALPHA
                          +--W32MIPS
                          +--W32PPC
```

Se instalo la impresora en samba seleccionando los drivers adecuados en CUPS en el puerto 631 del local host, en los clientes, se configuró en CUPS para ver la impresora de samba.

5.8 Archivos de configuración para el servicio DNS Slave de la Intranet

Se crearon y modificaron los siguientes archivos:

vi /etc/named.conf

```
options {
        directory "/var/lib/named";
};

zone "mega-soft.com.mx" IN {
        type slave;
        file "slave/named.mega-soft.com.mx.bak";
        masters {
                10.6.0.2;
        };
};
```

```
zone "0.6.10.in-addr.arpa" IN {
        type slave;
        file "slave/named.10.6.0.bak";
        masters {
                10.6.0.2;
        };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr-arpa" IN {
        type master;
        file "127.0.0.zone";
};
```

vi /var/lib/named/localhost.zone

```
$TTL 1W
@               IN SOA  @   root (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

                IN NS           @
                IN A            127.0.0.1
```

vi /var/lib/named/127.0.0.zone

```
$TTL 1W
@               IN SOA          localhost.   root.localhost. (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

                IN NS           localhost.
```

```
        IN PTR      localhost.
```

Se realizo el backup de /etc/hosts

Se modificó el archivo /etc/hosts y quedó con el siguiente contenido

vi /etc/hosts

```
127.0.0.1       localhost
10.6.0.3        intr03.mega-soft.com.mx intr03
```

Se modifico el nombre del host por:

```
hostname intr03.mega.soft.com.mx
```

Se crea el archivo /etc/resolv.conf

vi /etc/resolv.conf

```
nameserver 10.6.0.2
nameserver 10.6.0.3
domain mega-soft.com.mx
```

Se corre el demonio named

```
rcnamed start
```

5.9 APACHE en la Intranet

Se descargo el Apache server

```
httpd-2.0.58.tar.gz
```

Se descomprimió éste, en el siguiente directorio:

```
cd /usr/src
```

Utilizando el siguiente comando:

```
tar -zxvf /root/lx25/httpd-2.0.58.tar.gz
```

Se direcciona la instalación

```
./configure –prefix=/user/local/apache2 --enable --module=so
```

Se compila el código ingresando el comando

```
make
```

Se instalo el servidor

```
make install
```

Se levanto el servicio

```
cd /usr/local/apache2/bin
./apachectl start
```

Una vez funcionando se agrego a la configuración la página Web en el siguiente directorio:

```
cd /srv/www/htdocs
```

Y por ultimo en el archivo de configuración de YAST se direcciona al archivo “index.html” y se reinicio el servicio.

5.10 Archivos para la configuración del Servidor de bases de datos

Se creó el siguiente archivo en esta dirección /srv/www/htdocs/mysql_php_test.php

```
<html>
<head>
	<title>MySQL - PHP Test</title>
</head>
<body>
	<center><h1>MySQL - PHP Test</h1></center>
	<br />
	<?
		$host = 'localhost';
		$usuario = 'root';
		$pass = '';
		$db = 'megasoft';

		//Realizamos la conexión a mysql
		$conn = mysql_pconnect($host,$usuario,$pass) or die('<br /><h3>Error al
conectarse a		MySQL: </h3>'. mysql_error($conn));

		//Seleccionamos la base de datos
		mysql_select_db($db,$conn) or die('<br /><h3>Error al conectarse a la base de
datos:		</h3>'. mysql_error($conn));

		//La consulta
		$query = 'SELECT * FROM usuarios';
		$res = mysql_query($query,$conn) or die('<br /><h3>Error al realizar la consulta:
</h3>'.		mysql_error($conn));

		//Imprimimos los datos
		echo '<br />Integrantes del Proyecto: '. mysql_affected_rows($conn);
		echo '<br /><table border="1">';
		echo '<tr><th>Nombre</th>';
		echo '<th>Apellido Paterno</th>';
		echo '<th>Apellido Materno</th>';
		echo '<th>Email</th></tr>';
		while($fila = mysql_fetch_array($res, MYSQL_ASSOC))
		{
			echo '<tr><td>'.$fila['nombre'].'</td>';
			echo '<td>'.$fila['aPaterno'].'</td>';
			echo '<td>'.$fila['aMaterno'].'</td>';
			echo '<td>'.$fila['email'].'</td></tr>';
		}
		echo '</table>';

	?>
</body>
```

```
</html>
```

Creación de la base de datros en SQL

vi /srv/www/htdocs/megasoft_db.sql

```
CREATE DATABASE megasoft;
USE megasoft;
CREATE TABLE usuarios (
	idUsuario int NOT NULL AUTO_INCREMENT PRIMARY KEY,
	nombre varchar(40) NOT NULL,
	aPaterno varchar(40) NOT NULL,
	aMaterno varchar(40) NOT NULL,
	email varchar(50) NOT NULL
	)TYPE=INNODB;
INSERT INTO usuarios VALUES (1,'Jose
Manuel','Aguilar','Argandar','jmargandar@hotmail.com');
INSERT INTO usuarios VALUES (2,'Itzel','Ramirez','Islas','itzelislas@hotmail.com');
INSERT INTO usuarios VALUES (3,'Indira
Maribel','Rodriguez','Monterrubio','indira_agp@hotmail.com');
INSERT INTO usuarios VALUES
(4,'Yaroslaf','Albarran','Fernandez','yaros_albarran@hotmail.com');
INSERT INTO usuarios VALUES (5,'Javier','Tapia','Gonzalez','javier.tapia.6@gmail.com');
INSERT INTO usuarios VALUES (6,'Jose
Rafael','Campos','Padron','contacto@rafa.com.mx');
INSERT INTO usuarios VALUES (7,'Jonathan','Zertuche','Oñate','jonathan@hotmail.com');
```

5.11 Archivos de configuración para el servicio de DNS esclavo

Se crearon y modificaron los siguientes archivos para generar el DNS de esclavo al principio del capitulo se realizo el mismo procedimiento pero para el DNS master:

vi /etc/named.conf

```
options {
	directory "/var/lib/named";
};

zone "mega-soft.com.mx" IN {
	type slave;
	file "slave/named.mega-soft.com.mx.bak";
	masters {
		10.5.0.3;
	};
```

```
};

zone "0.5.10.in-addr.arpa" IN {
        type slave;
        file "slave/named.10.5.0.bak";
        masters {
                10.5.0.3;
        };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr-arpa" IN {
        type master;
        file "127.0.0.zone";
};
```

vi /var/lib/named/localhost.zone

```
$TTL 1W
@               IN SOA  @   root (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

                IN NS           @
                IN A            127.0.0.1
```

vi /var/lib/named/127.0.0.zone

```
$TTL 1W
@               IN SOA          localhost.   root.localhost. (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

                IN NS           localhost.
```

```
1          IN PTR       localhost.
```

Se realizo el backup de /etc/hosts

Se modificò el archivo /etc/hosts y quedò con el siguiente contenido

vi /etc/hosts

```
127.0.0.1       localhost
10.5.0.2        dmz02.mega-soft.com.mx intr03
```

Se modifico el nombre del host por:

```
hostname dmz03.mega.soft.com.mx
```

Se crea el archivo /etc/resolv.conf

vi /etc/resolv.conf

```
nameserver 10.5.0.3
nameserver 10.5.0.2
domain mega-soft.com.mx
```

Se corre el demonio named

```
rcnamed start
```

5.12 Archivo para la implementacion de Internet web server

Se descargo el Apache server 2.0.58 :

```
httpd-2.0.58.tar.gz
```

Se descomprimió éste, en el siguiente directorio:

```
cd /usr/src
```

```
tar -zxvf /root/lx25/httpd-2.0.58.tar.gz
```

Se direcciona la instalación:

```
./configure –prefix=/user/local/apache2 --enable --module=so
```

Se compilo el código:

```
make
```

Se instalo el servidor:

```
make install
```

Se levanto el servicio:

```
cd /usr/local/apache2/bin

./apachectl start
```

Una vez funcionando se agrego a la configuración la página WEB en el siguiente directorio:

```
cd /usr/local/apache2/htdocs
```

Y por ultimo en el archivo de configuración de YAST se direcciona a el archivo “index.html” y se reinicia el servicio.

5.13 Configuración de DNS en la Zona Desmilitarizada:

Modificación del archivo named.conf:

```
options {
        directory  “var/lib/named”;
};

zone  “mega-soft.com.mx” in {
```

```
                        type master;
                        file  "master/named.mega-soft.com.mx";
};

zone "10.5.0.in-addr.arpa" in {
                        type master;
                        file "master/named.10.5.0";
};

zone "localhost" in {
                        type master;
                        file "localhost.zone";

};

zone "0.0.127.in-addr.arpa" in {
                        type master;
                        file "127.0.0.zone";
};
```

Creación del archivo de nombre de la zona "/var/lib/named/master/named.mega-soft.com.mx", que incluye todos los equipos del dominio mega-soft.com.mx asociando a cada uno con su dirección IP.

```
$TTL 86400
@       IN      SOA    intr03.mega-soft.com.mx. root.intr03.mega-soft.com.mx (
                                        2006061501    ;       serial
                                        28800         ;       refresh
                                        7200          ;       retry
                                        604800        ;       expire
                                        86400  )      ;       minimum TTL
      IN     NS      intr01.mega-soft.com.mx.
      IN     NS     intr02.mega-soft.com.mx.
      IN     NS     intr03.mega-soft.com.mx.
      IN     NS     intr04.mega-soft.com.mx.
      IN     NS     intr05.mega-soft.com.mx.
      IN     NS     intr06.mega-soft.com.mx.
      IN     NS     intr07.mega-soft.com.mx.
      IN     NS     intr08.mega-soft.com.mx.
      IN     NS     intr09.mega-soft.com.mx.
      IN     NS     intr10.mega-soft.com.mx.
      IN     NS     intr11.mega-soft.com.mx.
      IN     NS     intr12.mega-soft.com.mx.
      IN     NS     intr13.mega-soft.com.mx.
      IN     NS     intr14.mega-soft.com.mx.
      IN     NS     intr15.mega-soft.com.mx.
```

```
        IN      NS      intr16.mega-soft.com.mx.
        IN      NS      intr17.mega-soft.com.mx.
        IN      NS      intr18.mega-soft.com.mx.
        IN      NS      intr19.mega-soft.com.mx.
        IN      NS      intr20.mega-soft.com.mx.
        IN      NS      intr21.mega-soft.com.mx.
        IN      NS      intr22.mega-soft.com.mx.
        IN      NS      intr23.mega-soft.com.mx.
        IN      NS      intr24.mega-soft.com.mx.
        IN      NS      intr25.mega-soft.com.mx.
        IN      NS      intr26.mega-soft.com.mx.
        IN      NS      intr27.mega-soft.com.mx.
        IN      NS      intr28.mega-soft.com.mx.
        IN      NS      intr29.mega-soft.com.mx.
        IN      NS      intr30.mega-soft.com.mx.
        IN      NS      intr31.mega-soft.com.mx.

1       IN      PTR     intr01.mega-soft.com.mx
2       IN      PTR     intr02.mega-soft.com.mx
3       IN      PTR     intr03.mega-soft.com.mx
4       IN      PTR     intr04.mega-soft.com.mx
5       IN      PTR     intr05.mega-soft.com.mx
6       IN      PTR     intr06.mega-soft.com.mx
7       IN      PTR     intr07.mega-soft.com.mx
8       IN      PTR     intr08.mega-soft.com.mx
9       IN      PTR     intr09.mega-soft.com.mx
10      IN      PTR     intr10.mega-soft.com.mx
11      IN      PTR     intr11.mega-soft.com.mx
12      IN      PTR     intr12.mega-soft.com.mx
13      IN      PTR     intr13.mega-soft.com.mx
14      IN      PTR     intr14.mega-soft.com.mx
15      IN      PTR     intr15.mega-soft.com.mx
16      IN      PTR     intr16.mega-soft.com.mx
17      IN      PTR     intr17.mega-soft.com.mx
18      IN      PTR     intr18.mega-soft.com.mx
19      IN      PTR     intr19.mega-soft.com.mx
20      IN      PTR     intr20.mega-soft.com.mx
21      IN      PTR     intr21.mega-soft.com.mx
22      IN      PTR     intr22.mega-soft.com.mx
23      IN      PTR     intr23.mega-soft.com.mx
24      IN      PTR     intr24.mega-soft.com.mx
25      IN      PTR     intr25.mega-soft.com.mx
26      IN      PTR     intr26.mega-soft.com.mx
27      IN      PTR     intr27.mega-soft.com.mx
28      IN      PTR     intr28.mega-soft.com.mx
29      IN      PTR     intr29.mega-soft.com.mx
30      IN      PTR     intr30.mega-soft.com.mx
31      IN      PTR     intr31.mega-soft.com.mx
```

Creación de los archivos de zona IP "/var/lib/named/master/named.10.5.0" que contiene los equipos de la red 10.5.0.0 asociando la dirección IP con el nombre de cada equipo.
Verificación la existencia y el contenido de los archivos de la zona local:
Modificación del archivo resolv.conf estableciendo el nombre del dominio y la dirección IP del servidor de nombres de la siguiente manera:
Iniciar el demonio named y verificar que inicie de forma correcta.
Modificar el archivo boot.local para iniciar el servicio al encender el equipo.

5.14 Archivos para la implementación del Router DMZ

Encriptados para poner el password para poder iniciar el boot con una opción especifica.

```
#grub
grub> md5crypt
password $24asFG$SAas212$yuKLOPJspofT7A1s
grub> quit

EDITAMOS EL ARCHIVO DESPUES DE LA LINEA DE (timeout):

password $24asFG$SAas212$yuKLOPJspofT7A1s
```

Se guarda el archivo

Script de configuracion de ipv4 (sysctl.conf)

```
# Disable response to broadcasts.
# You don't want yourself becoming a Smurf amplifier.
net.ipv4.icmp_echo_ignore_broadcasts = 1
# enable route verification on all interfaces
net.ipv4.conf.all.rp_filter = 1
# enable ipV6 forwarding
#net.ipv6.conf.all.forwarding = 1

net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ratelimit = 1
net.ipv4.icmp_ratemask = 6168
net.ipv4.ip_default_tt1 = 255
net.ipv4.ip_local_port_range = 1024 32000
net.ipv4.ip_no_pmtu_disc = 1
net.ipv4.ipfrag_high_thresh = 262144
net.ipv4.ipfrag_low_thresh = 196608
net.ipv4.ipfrag_time = 30
```

```
net.ipv4.tcp_keepalive_probes = 5
net.ipv4.tcp_kepalive_time = 600
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_retries1 = 3
net.ipv4.tcp_fin_timeuot = 30
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.log_martians = 1
```

Script para dar de baja las reglas predefinidas de iptables (iptables_rules_server.down)

```
iptables -X
iptables -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Script para dar de baja y levantar las targetas de red realizamos este script llamado (tarjetas)

```
ifdown eth0
ifdown eth1
ifconfig eth0 10.5.0.1 netmask 255.255.0.0
route add -net 10.6.0.0 netmask 255.255.0.0 gw 10.5.0.4
ifconfig eth1 172.16.16.35 netmask 255.255.255.0
route add default gw 172.16.16.1
```

Script para determinar las acciones de inicio, parada, restaurar, estatus, salvar y panico (/etc/init.d/iptables)

```
#! /bin/sh
#
# init.d/iptables
#
### BEGIN INIT INFO
# Provides:       iptables
# Required-Start: $network
# Required-Stop:
# Default-Start:  3 5
# Default-Stop:   0 1 2 4 6
# Short-Description: Starts iptables
```

```
# Description:  Starts iptables rules from /etc/sysconfig/iptables
### END INIT INFO

. /etc/rc.status
rc_reset

SYSCONFIG_FILE="/etc/sysconfig/iptables"

[ -x /usr/sbin/iptables ] || exit 0

case "$1" in
	start)
		if [ ! -f $SYSCONFIG_FILE ]; then
			echo "SYSCONFIG_FILE not present. Exiting."
			exit 0

		fi
		echo -n "Flushing current iptables rules "
		for i in filter nat mangle
		do
			iptables -t $i -F
			iptables -t $i -X
			iptables -t $i -Z
		done
		rc_status -v
		echo -n "Applying iptables rules "
		/usr/sbin/iptables-restore < $SYSCONFIG_FILE
		rc_status -v
		;;
	stop)
		echo -n "Flushing current iptables rules "
		for i in filter nat mangle
		do
			iptables -t $i -F
			iptables -t $i -X
			iptables -t $i -Z
		done
		rc_status -v
		echo -n "Setting all default policies to ACCEPT "
		iptables -t filter -P INPUT ACCEPT
		iptables -t filter -P OUTPUT ACCEPT
		iptables -t filter -P FORWARD ACCEPT
		iptables -t nat -P PREROUTING ACCEPT
		iptables -t nat -P POSTROUTING ACCEPT
		iptables -t nat -P OUTPUT ACCEPT
		iptables -t mangle -P PREROUTING ACCEPT
		iptables -t mangle -P POSTROUTING ACCEPT
		iptables -t mangle -P INPUT ACCEPT
		iptables -t mangle -P OUTPUT ACCEPT
```

```
        iptables -t mangle -P FORWARD ACCEPT
        rc_status -v
        ;;
    restart)
        $0 stop
        $0 start
        rc_status
        ;;
    status)
        iptables -t filter --list
        iptables -t nat --list
        iptables -t mangle --list
        ;;
    panic)
        echo -n "Changing all policies to DROP "
        iptables -t filter -P INPUT DROP
        iptables -t filter -P OUTPUT DROP
        iptables -t filter -P FORWARD DROP
        iptables -t nat -P PREROUTING DROP
        iptables -t nat -P POSTROUTING DROP
        iptables -t nat -P OUTPUT DROP
        iptables -t mangle -P PREROUTING DROP
        iptables -t mangle -P POSTROUTING DROP
        iptables -t mangle -P INPUT DROP
        iptables -t mangle -P OUTPUT DROP
        iptables -t mangle -P FORWARD DROP
        rc_status -v
        echo -n "Flushing all rules "
        for i in filter nat mangle
        do
            iptables -t $i -F
            iptables -t $i -X
            iptables -t $i -Z
        done
        rc_status -v
        ;;
    save)
        echo -n "Saving rules to $SYSCONFIG_FILE "
        touch $SYSCONFIG_FILE
        chmod 600 $SYSCONFIG_FILE
        /usr/sbin/iptables-save > $SYSCONFIG_FILE 2>/dev/null
        rc_status -v
        ;;
    *)
        echo "Usage: $0 {start|stop|restart|status|panic|save}"
        exit 1
        ;;
esacc_exit
```

5.15 Configuración de NAT para IPTABLES (iptables_nat_up)

Para que el sistema pudiera actuar como gateway y proporcionar el acceso de Internet a múltiples anfitriones en una red local se realizo la configuración mostrada a continuación en el servidor.

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
iptables -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1  -j ACCEPT
```

La definición de las rutas quedo establecida de la siguiente manera:

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.16.16.0	*	255.255.255.0	U	0	0	0	eth1
10.6.0.0	10.5.0.4	255.255.0.0	UG	0	0	0	eth0
10.5.0.0	*	255.255.0.0	U	0	0	0	eth0
loopback	*	255.0.0.0	U	0	0	0	lo
Default	172.16.16.1	0.0.0.0	UG	0	0	0	eth1

Capítulo VI

Conclusiones

Al finalizar el desarrollo y la implementación del sistema en la empresa MEGA-SOFT S.A. de C.V. concluyo que se entrego un sistema integral de alta rentabilidad y robustez. Dando a la empresa y al cliente la satisfacción total en cada uno de sus ámbitos esto debido al cumplimiento de todos y cada uno de los requerimientos solicitados.

Con la implementación del sistema la empresa cuenta ya con la administración y gestión de sus recursos informáticos, haciendo posible la diferenciación de usuarios y la protección ante ataques informáticos que pudiesen presentarse, todo esto es posible por la arquitectura con la que fue diseñado el sistema.

Las regalas de negocio establecidas en el sistema permitieron otorgar permisos de navegación solo a ciertos usuarios, esto deriva en el mejor aprovechamiento de los sistemas y equipos de computo haciendo que los recursos humanos tengan mayor productividad laboral evitando pérdidas de tiempo en navegaciones de internet innecesarias o no relacionadas con su área de trabajo, además de que con esta medida se hace la prevención de ataques informáticos evitando posibles vulnerabilidades que pudiesen darse al exponer a todos los usuarios hacia servicios externos de internet.

Como en toda empresa se busco garantizar la rentabilidad del sistema pensando en el costo – beneficio del mismo, logrando minimizar al máximo los costes de desarrollo, utilizando tecnologías vanguardistas que permiten hacer más fácil el mantenimiento y sustentabilidad del sistema debido a que estas tecnologías son fácilmente escalables en torno a actualizaciones y parches informáticos.

El proceso involucrado desde el análisis, desarrollo y mantenimiento del sistema siempre fue orientado a la búsqueda de la integración de nuevas tecnologías de software libre garantizando un sistema de calidad y bajo costo para la empresa siendo este último punto primordial para la misma, ya que MEGA-SOFT S.A. de C.V. requería el tener un sistema completo de bajo costo pero que garantizara la estabilidad y robustez del mismo.

Profesionalmente haber realizado la implementación de este sistema en la empresa MEGA-SOFT S.A. DE C.V. me aportó gran experiencia ayudándome a reforzar y poner en práctica conocimientos adquiridos en el aula durante mis años de estudio, además de que utilice mi capacidad de planificación, organización y dirección del funcionamiento de un sistema informático.

Hacer uso de tecnologías de software libre a mi parecer me da oportunidades de desarrollo en el ámbito laboral enfocados a innovaciones tecnológicas esto puede darme como resultado alcanzar posiciones de mayor responsabilidad y retos profesionales, al iniciar mi desarrollo profesional enfocado a estas tecnologías libres puedo brindar soluciones de bajo costo de acuerdo a las expectativas de la cualquier empresa.

A mi parecer dos de las más grandes ventajas que provee el software libre de estándares abiertos son el bajo costo y la innovación tecnología que provee, ya que el desarrollo y crecimiento del mismo no está en manos de una empresa especializada sino en las comunidades informáticas, que enriquecen los desarrollos con experiencias e ideas innovadoras.

Personalmente me gustaría mencionar que el desarrollo de este proyecto fue de gran satisfacción para mí, ya que fue desarrollado en el ámbito tecnológico que mas me agrada el cual es el de la tecnología de software libre, por los motivos expuestos en párrafos anteriores.

Este proyecto también me deja una gran satisfacción personal al poder verlo concluido y con resultados exitosos, ya que fue el primer proyecto profesional en el que participe y sin lugar a dudas cambio en demasía la visión que tenia de un desarrollo profesional antes de terminar mis estudios.

Bibliografía

- Linux Power User
  Course code QLX02
  IBM

- Linux System Administration I: Implementation
  Course code QLX03
  IBM

- Linux Network Administration I: TCP/IP
  TCP/IP services
  Course code QLX07
  IBM

- Linux Network Administration II: Network security and firewalls
  Course code QLX24
  IBM

- Linux as a Webserver (Apache)
  Course code QLX25
  IBM