PRÁCTICA EMPRESARIAL
TELEBUCARAMANGA S.A. E.S.P.

LUIS ENRIQUE CORZO PARRA

ID: 69926

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA Y ADMINISTRACIÓN

ESCUELA DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2008

PRÁCTICA EMPRESARIAL

TELEBUCARAMANGA S.A. E.S.P.

CONTENIDO

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: Práctica Empresarial, Telebucaramanga S.A. E.S.P.

AUTOR(ES): Luis Enrique Corzo Parra

FACULTAD: Facultad de Ingeniería Electrónica

DIRECTOR(A): Ing. Alex Alberto Monclou Salcedo

RESUMEN

El objetivo principal de la practica es aprovechar el software de distribución libre Linux/CentOS 5.1, para la implementación de servidores en una red, tales como, servidor Firewall para dar seguridad y restricción a los accesos no autorizados en la red, servidor Proxy para hacer Cache y filtrado de contenido, servidor DHCP para el direccionamiento automático entre los equipos que se conectan a la red, servidor DNS para reconocer la red y cada equipo de la red por un Nombre de Dominio, servidor Web para ofrecer a la red su propio sito web o website, todo esto con el fin de brindar y obtener un mejor rendimiento en la calidad, control y seguridad en el servicio de comunicación entre la red.

PALABRAS CLAVES: Linux Centos servidores Firewall Proxy DNS DHCP WEB

V°B° DIRECTOR DE TRABAJO DE GRADO

SUMMARY OF WORK DEGREE

TITLE: Practical Business Telebucaramanga S.A. E.S.P.

AUTHOR(S): Luis Enrique Corzo Parra

FACULTY: Facultad de Ingeniería Electrónica

DIRECTOR: Ing. Alex Alberto Monclou Salcedo

SUMMARY

The principal objetive of the practice, is to exploit the free software distribution Linux-CentOS 5.1, to implement servers network, such as, Firewall server, for the security and restriction to access not authorized network, Proxy server, to cache and content filter, DHCP server, for automatic routing among computers that connect to the network, DNS server, to recognize the network and each computer on the network by a Domain Name, Web server, to provide to network their own website, all this in order to offer and get the best performance in quality, control and security in the service comunication to network.

KEY WORDS: Linux Centos server Firewall Proxy DNS DHCP WEB.

V°B° DIRECTOR OF WORK DEGREE

2. **INTRODUCCION**

En el desarrollo de la práctica se contemplan las actividades características que intervienen en la elaboración y montaje de una red ***LAN*** *(Local Area Network o Red de Área Local),* instalaciones de cada uno de sus componentes, tanto *Hardware* como *Software*, dando a conocer la importancia del equipo principal de la red, *el Servidor*, su configuración, especificaciones técnicas y las clases de servidores que puede contener una red, para ofrecer la mejor calidad y seguridad en la comunicación entre cada uno de los equipos que la componen.

En la implementación del *Servidor* se lleva a cabo el uso de un *Sistema Operativo de Software Libre* como lo es *LINUX*, optando por la distribución *CentOs versión 5.1,* el cual ofrece gran variedad de poderosas herramientas y programas para la implementación de servidores, totalmente configurables a necesidad del usuario. De esta manera se logra mostrar, especificar y conocer las ventajas y utilidades del uso de software libre, así como también la manera de comenzar a interactuar con el sistema operativo *Linux*, que cada día tienes más acogida en el mundo de la informática así como en los grandes fabricantes de equipos de cómputo, como estaciones de trabajo, equipos portátiles y computadoras personales.

3. **GENERALIDADES DE LA EMPRESA**

Telebucaramanga es una compañía que brinda servicios de telecomunicaciones en Colombia, específicamente en el departamento de Santander. Su objetivo fundamental se basa en proporcionar soluciones de telecomunicaciones que se ajusten a las condiciones socioeconómicas y culturales de las personas a las cuales ofrece sus servicios, buscando garantizarles una vida más productiva y acercarlos con el mundo.
Actualmente *Telebucaramanga* cuenta con 35000 usuarios de internet banda ancha con velocidades desde 250Kbps hasta 4Mbps, distribuidos en el área metropolitana de Bucaramanga y 1200 usuarios de conexiones LAN to LAN para lo cual se dispone de 6 grupos de trabajo conformado por funcionarios y estudiantes en práctica quienes atienden las diferentes solicitudes de los clientes, como puede observarse la cantidad de usuarios conduce a disponer de personal capacitado y capacitar los nuevos miembros del equipo con el objetivo que le colaboren en la tarea de implementación y mantenimiento de los usuarios de nuestra red .

La subgerencia técnica y operativa tiene bajo su responsabilidad todos los aspectos técnicos de soporte y mantenimiento de la red de telecomunicaciones de Bucaramanga, bajo su responsabilidad se encuentra las direcciones de conmutación, transmisión, red externa y dirección de proyectos dentro de la cual trabaja *la red multiservicios*.

La red multiservicios se encarga de la gestión operación y mantenimiento de los usuarios de la plataforma de Internet conmutado y banda ancha, así como de los enlaces LAN to LAN, áreas a las cuales está asignado el estudiante en práctica.

El estudiante en práctica tiene como funciones:

Analizar, configurar e implementar soluciones de datos para enlaces punto a punto y punto-multipunto.

Analizar y configurar conexiones de Internet banda ancha desde 256Kbps a 4Mbps.

Solucionar problemas de enlaces de datos punto a punto y punto-multipunto.
Solucionar problemas de conexión de Internet banda ancha.

4. **OBJETIVOS**

4.1. **Objetivo General**

Obtener conocimientos sobre la implementación de redes LAN to LAN, análisis y optimización en los procesos de operación.

4.2. **Objetivos Específicos**

Desarrollo e implementación de servidores, *Proxy, Web Server, DNS, DHCP*, utilizando sistema operativo Linux, con la distribución CentOs.

Identificar y conocer los parámetros, procedimientos técnicos y operativos en la adecuación de la red LAN to LAN, tanto físicamente en el par de cobre como en configuraciones del enlace de datos.

Adquirir conocimientos y claridad en los conceptos sobre la arquitectura de una red, plataformas, niveles, protocolos y dispositivos, que interactúan en su conformación.

Efectuar labores de operación y mantenimiento de la plataforma de la red multiservicios bajo la supervisión de personal de Telebucaramanga.

5. **PLAN DE TRABAJO**

5.1 **Actividades a Desarrollar**

5.1.1. **Revisión de logs de alarmas en los equipos del core (catalyst 4507 de cisco).**

Mediante comandos o de la interfaz grafica se revisan diariamente el log de alarmas de los siguientes equipos switch AMT-AXD-301, CISCO 7604, plataforma EDA; con el objetivo de realizar las operaciones de mantenimiento correctivo que sean necesarios.

5.1.2. **Pruebas y recepción de puertos ADSL.**

Junto con personal de telebucaramanga el estudiante en práctica realizara las pruebas y recepción de los puertos de la plataforma de adquisición de datos por Ethernet EDA entregados por el contratista; mediante pruebas de navegación con cada uno de los puertos, pruebas de redundancia a fuentes de poder y de conectividad con el core EDA.

5.1.3. **Apoyo operativo al personal de RMS en la implementación de nuevos proyectos (levantamiento de inventarios, documentación, entre otros).**

El estudiante en práctica realizara acompañamiento operativo al personal de operación y mantenimiento, participando asi en labores de mantenimiento que se realiza tanto con clientes externos como de la plataforma.

5.1.4. **Documentación de procedimientos técnicos y operativos específicos en cada uno de los equipos del core de la red.**

Estando bajo la supervisión de personal de telebucaramanga el estudiante realizara los procedimientos necesarios para realizar la configuración básica de los equipos como back-up, porcentaje de procesamiento entre otros.

5.1.5. **Actualización de inventarios de equipos del core de la red y su estado (dañado, en reserva, instalado, libre).**

Mediante la herramienta multired el estudiante en práctica realizara el inventario de los puertos EDA instalados, discriminando el estado, es decir en buen estado, dañado o en reserva.

5.2 Cronograma de Actividades

	SEMANAS																							
ACTIVIDADES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Inducción y reconocimiento del área de trabajo.																								
Instalación, mantenimiento y reparación de los enlaces de datos, redes LAN to LAN, Internet.																								
Estudio y conocimientos de implementación de Servidores con GNU/Linux, distribución Centos 5.1.																								
Acondicionamiento técnico y operativo de equipo PC para montaje de servidores.																								
Instalación de software Centos 5.1 y configuración para montaje del Proxy.																								
Verificación, Pruebas de funcionamiento del Proxy.																								
Evaluación y corrección de errores de los resultados obtenidos en la implementación del Proxy.																								
Configuración del servidor para implementación de Firewall.																								
Verificación, Pruebas de funcionamiento del Firewall.																								
Evaluación y corrección de errores de los resultados obtenidos en la implementación del Firewall.																								
Configuración del servidor para implementación de Web Server.																								
Verificación, Pruebas de funcionamiento del Web Server.																								
Evaluación y corrección de errores de los resultados obtenidos en la implementación del Web Server.																								
Preparación de Informes.																								

6. **MARCO TEORICO**

6.1. **¿Qué es Linux?**

GNU/Linux® es un sistema operativo con licencia libre y que implementa el estándar *POSIX* (acrónimo de Portable Operating System Interface, que se traduce como Interfaz de Sistema Operativo Portable). Fue creado en 1991 por Linus Torvalds, siendo entonces un estudiante de la Universidad de Helsinski, Finlandia.

GNU/Linux es *Programática Libre*. Esto significa que el usuario es libre de redistribuir y modificar de acuerdo a necesidades específicas, siempre que se incluya el código fuente, como lo indica la Licencia Pública General *GNU* (acrónimo de *GNU is Not Unix*), que es el modo que ha dispuesto la *Free Software Foundation* (Fundación de Programática Libre). Esto también incluye el derecho a poder instalar el núcleo de *GNU/Linux*® en cualquier número de ordenadores o equipos de cómputo que el usuario desee.

6.1.1. **¿Linux software de distribución libre?**

GNU/Linux® no es un sustento lógico gratuito (comúnmente denominada como *Freeware*); se trata de *Programática Libre*. Cuando nos referirnos a *Programática Libre*, lo hacemos en relación a la libertad y no al precio. La *GPL* (acrónimo de *General Public Licence*, que se traduce como Licencia Pública General), a la cual *Linus Torvalds* incorporó a *Linux*, está diseñada para asegurar que el usuario tenga siempre la libertad de distribuir copias del sustento lógico libre (y cobrar por el servicio si así lo desea). La *GPL* tiene como objetivo garantizar al usuario la libertad de compartir y cambiar *Programática Libre*; es decir, asegurarse de que el sustento lógico siempre permanezca siendo libre para todos los usuarios. La *GPL* es aplicable a la

mayoría del sustento lógico de la *Free Software Foundation* así como a cualquier otro programa cuyos autores se comprometan a usarlo.

6.1.2. **¿Por qué usar Linux?**

GNU/Linux® es también la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también requieren un sistema operativo estable, robusto y confiable. Es un sistema operativo idóneo para utilizar en Redes, como es el caso de servidores, estaciones de trabajo y también para computadoras personales. Las características de *GNU/Linux*® le permiten desempeñar múltiples tareas en forma simultánea de forma segura y confiable. Los distintos servicios se pueden detener, iniciar o reiniciar independientemente sin afectar al resto del sistema, permitiendo operar las 24 horas del día los 365 días del año. Tal ha sido el impacto alcanzado por *GNU/Linux*® en los últimos años, que muchas de las empresas de Software más importantes del mundo, entre las cuales están IBM, Oracle y Sun Microsystems, han encontrado en *GNU/Linux* una plataforma con un mercado amplio, y se han volcado al desarrollo de versiones para Linux de sus más importantes aplicaciones. Corporaciones, como COMPAQ, Dell, Hewlett Packard, IBM y muchos más, llevan varios años distribuyendo equipos con *GNU/Linux*® como sistema operativo. Gracias a sus características, la constante evolución de los ambientes gráficos para X Window®, que cada vez son de más fácil uso, como es el caso de *GNOME* y *KDE*, al trabajo de cientos de programadores y usuarios fieles alrededor del mundo, *Linux* ha dejado de ser un sistema operativo poco atractivo y complicado de utilizar, para convertirse en una alternativa real para quienes buscan un sistema operativo confiable y poderoso; ya sea para una servidor, estación de trabajo o la computadora personal de un usuario intrépido.

6.1.3. **Distribuciones Linux**

Al ser Linux un sistema de libre distribución en donde podemos encontrar todos los ficheros y programas necesarios para su funcionamiento en multitud de servidores. La tarea de reunir todos los ficheros y programas necesarios, así como instalarlos en tu sistema y configurarlo, puede ser una tarea bastante complicada y no apta para muchos. Por esto mismo, nacieron las llamadas *Distribuciones de Linux*, empresas y organizaciones que se dedican a hacer este trabajo para nuestro beneficio y comodidad.

Una *Distribución de Linux* no es otra cosa, que una recopilación de programas y ficheros, organizados y preparados para su instalación. Estas distribuciones se pueden obtener a través de Internet, o comprando los CDs de las mismas, los cuales contendrán todo lo necesario para instalar un sistema *Linux* bastante completo y en la mayoría de los casos un programa de instalación que nos ayudara en la tarea de una primera instalación.

Existen muchas y variadas distribuciones creadas por diferentes empresas y organizaciones, estas son algunas de las distribuciones más importantes: REDHAT**,** FEDORA, DEBIAN, GENTOO, UBUNTU, MANDRIVA.

6.2. **Introduccion a CentOs**

CentOS (Community ENTerprise Operating System), es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.
Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública

general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de los fuentes de Red Hat.

6.2.1. **CentOS 5.1**

CentOS 5.0 está basado en la versión 5 de Red Hat Enterprise Linux. Fue liberado el 12 de abril de 2007 para las arquitecturas i386 y x86_64. El 2 de diciembre de 2007 fue liberado CentOS 5.1 para las arquitecturas i386 y x86_64, Esta es la primera actualización para la serie de distribuciones CentOS 5. Contiene una gran cantidad de correcciones de errores, actualizaciones y nuevas funcionalidades.

6.3. **Fundamentos sobre redes**

Una red consiste en dos o más equipos interconectados entre sí por medio de un cable de red a través de una interfaz de red o tarjeta de red en cada uno los equipos. Las principal razón para la creación de una red es la de compartir, desde datos de información hasta Hardware y software, con la capacidad de administrar y dar apoyo a cada uno de los equipos que la componen, de esta manera se aumenta la eficiencia y rapidez en la comunicación debido a que la información esta disponibles para equipo de la red, sin la necesidad de usar medios de almacenamiento extraíbles, para el transporte de información de un equipo a otro.

Existen dos tipos o clases de redes, las cuales se clasifican según su tamaño o área geográfica. La red *LAN (Local Area Network o red área local)* es aquella conformada por dos o más equipos interconectados dentro de un espacio geográfico limitado como el de una empresa. La red *WAN* (*Wide*

Area Network o red de área amplia) la cual consta de dos o más redes *LAN* interconectadas en cualquier parte del planeta, no tiene limitaciones de espacio geográfico.

Los elementos básicos que componen una red son: *El Servidor* que es el equipo que ofrece los servicios y recursos a los usuarios de la red, los *Clientes* que son los equipos que acceden a los recursos compartidos que ofrece el servidor, el *Medio* que consta de la conexiones físicas de la red, como cables, fibra óptica, switchs, etc. (Ver figura 1)

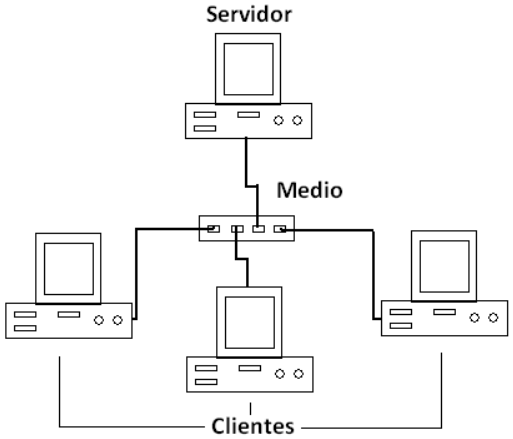

Figura 1. Red LAN

6.3.1. **Introduccion a TCP/IP**

La familia de protocolos de Internet es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina *conjunto de protocolos TCP/IP*, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de

100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

TCP/IP es la plataforma que sostiene Internet y que permite la comunicación entre diferentes sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN).

6.3.2. **Parámetros de red**

Los parámetros de red, son aquellos que se configuran dentro de cada equipo o dispositivo de la red, estos nos permiten identificar cada equipo mediante una dirección IP, con una máscara de red para la identificación de la red y una puerta de enlace para la comunicación con otras redes.

IPv4 es la versión 4 del Protocolo de Internet *IP* o Internet Protocol y constituye la primera versión de *IP* que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. El propósito principal de IP es proveer una dirección única a cada sistema para asegurar y facilitar que una computadora dentro de la red pueda identificar a otra.

6.3.2.1. **Dirección IP**

Una dirección IP se implementa con un número de 32 bits que suele ser mostrado en cuatro grupos de números decimales de 8 bits (IPv4). Cada uno de esos números se mueve en un rango de 0 a 255 expresado en decimal, o de 0 a FF en hexadecimal, o de 0 a 11111111 en binario. Las *direcciones IP*

se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto puede ser entre 0 y 255, el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total.

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iníciales, si los hubiera, se pueden obviar. Ejemplo de representación de dirección IPv4: *164.12.123.65.*
Hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C. En la actualidad, ICANN reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de red permite una cantidad fija de equipos (hosts).

En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]), es decir, 16777214 hosts.

En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} - 2, o 65 534 hosts.

En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^8 - 2, ó 254 hosts.

6.3.2.2. **Mascara de red**

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host. Las máscaras, se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo, de esta manera permite realizar una verificación de la dirección de la Red y con un OR y la máscara negada se obtiene la dirección del broadcasting.

Por ejemplo, si el router tiene la IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras IPs, para fuera como a internet u otra red local mayor.

6.3.2.3. **Puerta de enlace o Gateway**

Una puerta de enlace predeterminada en un dispositivo, un *router* o una computadora, sirve como enlace entre dos redes informáticas, es decir, es el dispositivo que conecta y dirige el tráfico de datos entre dos redes. Generalmente en las casas, ese dispositivo es el *router* y Cable-Modem o DSL-Modem que conecta la red local de la casa (LAN) con Internet (WAN). En las empresas, muchas veces es una computadora la que dirige el tráfico de datos entre la red local y la red exterior, y, generalmente, también actúa como servidor proxy y firewall. En el caso de un servidor o un modem en la

red, este posee su propia dirección IP, esto quiere decir que los demás equipos dentro de la red tendrán como puerta de enlace la dirección IP del servidor o del modem si fuera el caso.

6.3.2.4. **Dirección MAC**

En redes de computadoras la dirección MAC *(Media Access Control address* o dirección de control de acceso al medio) es un identificador de 48 bits, 6 bytes, que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI (Organizationally Unique Identifier). No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos. Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas *Las Direcciones Quemadas" (BIA, por las siglas de* Burned-in Address*).* La dirección MAC es un número único de 48 bits asignado a cada tarjeta de red. Se conoce también como la dirección física en cuanto identificar dispositivos de red.

6.4. **Servidores**

Un servidor es un equipo o una computadora que forma o hace parte de una red, el cual ofrece y provee los servicios y recursos para la comunicación entre todos los equipos la red. Básicamente se trata de un software que corre en un ordenador administrando cada uno de los procesos y sirviendo a otros procesos para el intercambio de información.

6.4.1. **Servidor Proxy**

Un Servidor Intermediario o Proxy se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente: Cliente se conecta hacia un Servidor Intermediario o Proxy. Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto. El servidor Intermediario o Proxy proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché. En algunos casos el Servidor Intermediario Proxy puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los Servidores Intermediarios generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el Nivel de Red, actuando como filtro de paquetes, herramientas de cortafuegos, que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log, mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.

Una aplicación común de los Servidores Intermediarios es funcionar como caché de contenido de Red, principalmente HTTP, proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator), el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario

responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes.

Los Servidores Intermediarios para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

6.4.2. **Servidor DHCP**

DHCP, Dynamic Host Configuration Protocol que se traduce Protocolo de configuración dinámica de servidores, es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red, *dirección IP; máscara de sub-red, puerta de enlace, etc*. a partir de un servidor *DHCP*. Su propósito principal es hacer más fáciles de administrar las redes grandes.

Sin la ayuda de un servidor DHCP, tendrían que configurarse de forma manual cada dirección IP de cada cliente que pertenezca a una *red de área local*. Si un cliente se traslada hacia otra ubicación donde existe otra red de área local, se tendrá que configurar otra dirección IP diferente para poder unirse a esta nueva red de área local. Un servidor DHCP entonces supervisa y distribuye las direcciones IP de una red de área local asignando una dirección IP a cada cliente que se una a la red de área local. Cuando, por mencionar un ejemplo, una computadora portátil se configura para utilizar DHCP, a ésta le será asignada una dirección IP y otros *parámetros de red necesarios* para unirse a cada red de área local donde se localice.

Existen tres métodos de asignación en el protocolo DHCP:

Asignación manual: La asignación utiliza una tabla con direcciones MAC, Sólo los anfitriones con una dirección MAC definida en dicha tabla recibirá la IP asignada en la misma tabla.

Asignación automática: Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al cliente que la requiera.

Asignación dinámica: Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, utilizando un intervalo de tiempo controlable, de modo que las direcciones IP no son permanentes y se reutilizan de forma dinámica.

6.4.3. **Servidor DNS**

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

Clientes DNS: Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

Servidores DNS: Son servicios que contestan las consultas realizadas por los Clientes DNS.

6.4.4. **Servidor Web**

Un servidor web es un programa que implementa el protocolo *HTTP*, Hypertext Transfer Protocol, o Protocolo de Trasferencia de Hipertext. Este protocolo pertenece a la capa de aplicación del modelo OSI y 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 música.

Es un programa que se ejecuta continuamente en un ordenador, manteniéndose a la espera de peticiones por parte de un cliente, un navegador web, y que responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error.

Un servidor web se mantiene a la espera de peticiones *HTTP* por parte de un cliente *HTTP* que solemos conocer como navegador. El cliente realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear www.google.com en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo exhibe en pantalla. Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Las aplicaciones de servidor suelen ser la mejor opción para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad añadida, como sí ocurre en el caso de querer ejecutar aplicaciones java script o java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

7. **DESARROLLO DEL PLAN DE TRABAJO**

7.1. **Adecuaciones Técnicas para el Software**

En el equipo servidor para la instalación de *CentOs* se debe contar con la suficiente cantidad de memoria y un microprocesador en buen estado. Con casi cualquier distribución comercial de Linux, el ambiente gráfico necesitará al menos 192 MB RAM, y 650-800 MB de espacio en disco duro para la instalación mínima.

El servidor de vídeo puede funcionar con sólo 64 MB RAM; pero su desempeño será mas lento. Algunas aplicaciones para modo gráfico pueden necesitar escalar 64 MB, 128 MB o 256 MB de RAM adicional. El mínimo recomendado para utilizar GNOME 2.x es de 192 MB RAM; se recomiendan 256 MB. El óptimo es de 512 MB RAM.

7.2. **Adecuaciones Técnicas en Hardware.**

Siguiendo con las especificaciones mínimas, el equipo servidor cuenta con capacidad en disco duro de 40GB, capacidad de memoria RAM 512MB, procesador Pentium III a 200MHZ, más que suficiente para obtener la instalación en modo grafico y contar con mayor rendimiento en las aplicaciones prácticas.

Como requisito final, se instala una interfaz de red o tarjeta de red adicional para la administración de la red, esto quiere decir que el equipo cuenta con dos tarjetas de red, *eth0* y *eth1*, con la finalidad de configurar *eth0* como interfaz de red conectada a un modem con conexión a internet que suministra la empresa proveedora de servicios de internet, para comunicar la red *LAN* con la red *WAN* o internet, configurar eth1 como interfaz de red para conectar toda la red *LAN* con el equipo servidor. (Ver figura 2)

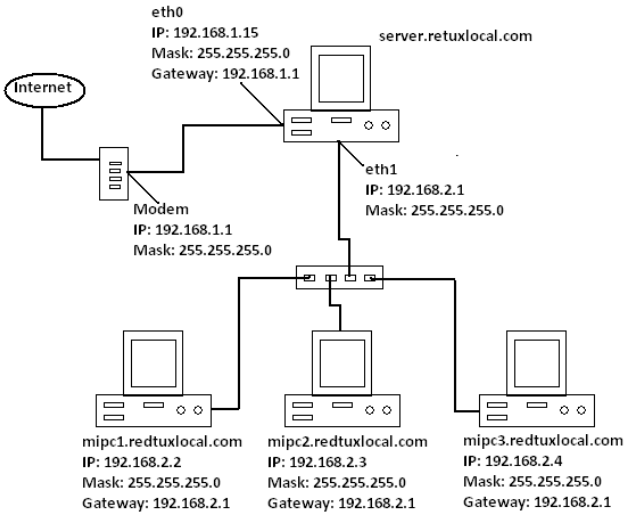

Figura 2. Diagrama de la red

7.3. **Configuración del Servidor**

CentOs cuenta con numerosas y poderosas herramientas para la configuración del servidor, tales como *Iptables, Squid, Dhcp, Bind y Apache*, cada una estas herramientas se configuran para ofrecer la mejor calidad en la administración de la red. La instalación de cada herramienta es muy práctica y sencilla, con tan solo ejecutar un comando en la terminal o ventana de ejecución de comandos. (Ver figura 3).

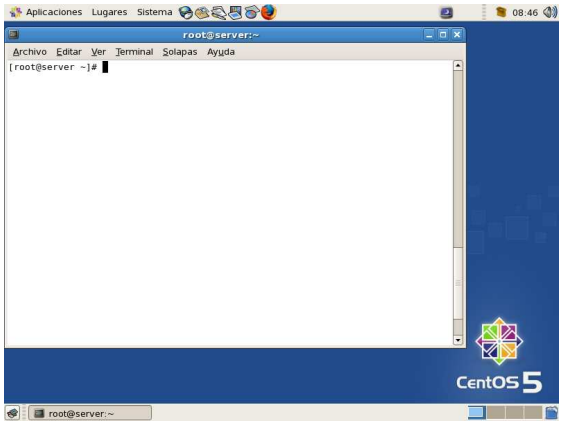

Figura 3. Terminal o Ventana de ejecución de comandos.

Para la instalación de cualquier herramienta, tan solo se requiere de tener una conexión a internet y por medio de la herramienta *Yum* que viene con el paquete de instalación de centos, se ejecuta el comando *yum –y install* seguida de la herramienta que se desee instalar. *Yum* descargara todos los paquetes necesarios y luego realizara la instalación, creando todas las carpetas y ficheros necesarios en sus respectivos directorios para que la herramienta pueda ser configurada.

7.3.1. **Crear la conexión a Internet**

Para tener acceso internet se configura la interfaz de red *eth0* con los parámetros de red adecuados para que pueda comunicarse con el modem. Siguiendo la configuración del diagrama de la red en la figura 2, el modem tiene como IP la dirección 192.168.1.1 y mascara de red 255.255.255.0, por tal motivo el servidor deberá apuntar hacia esta dirección como su puerta de enlace o Gateway y tener dirección IP en el rango 192.168.1.

Para configurar la tarjeta de red *eth0* se siguen los siguientes pasos, ir al menú *Sistema*, escoger la opción *Administración de red*, se abre la ventana de configuración de la interfaz de red, en la pestaña de *Dispositivos de red*, escoger la interfaz *eth0* con doble clic y editar cada uno de los parámetros de red así, dirección IP 192.168.1.15, mascara de red 255.255.255.0 y puerta de enlace 192.168.1.1, aceptar. Seguidamente en la pestaña de *DNS* escribir la dirección IP de los servidores DNS del proveedor de internet, por último salir guardando los cambios. Después de haber configurado todos los parámetros de red deseados, sólo deberá ser reiniciado el servicio de red, ejecutando el siguiente comando: *service network restart. (*Ver figura 4*)*.

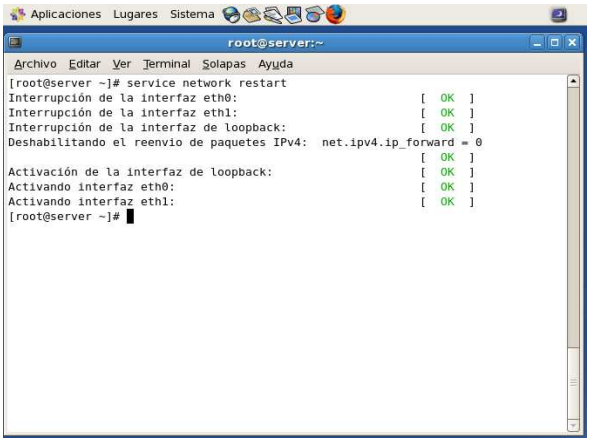

Figura 4. Ejecución del comando de reinicio del servicio de red.

Para verificar la configuración de cada interfaz de red, se ejecuta el comando *ifconfig*, donde se mostraran los parámetros de red de cada una de las tarjetas.

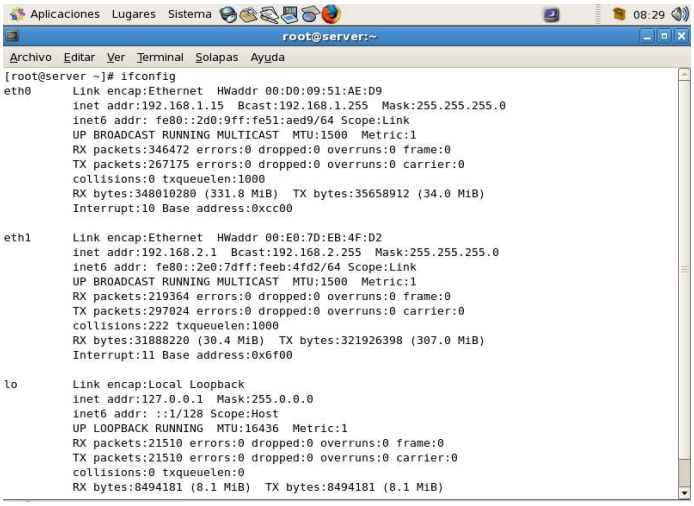

Figura 5. Verificar configuración de la interfaz de red con *ifconfig.*

En estos momentos el servidor deberá contar la conexión a internet, permitiendo navegar por internet como si se tratara de cualquier computador personal o estación de trabajo.

7.3.2. **Configurar la interfaz de red local**

Para configurar la segunda interfaz de red o tarjeta de red *eth1*, se hace de manera igual como se explico anteriormente para la interfaz de red *eth0*. Siguiendo el diagrama de la red en la figura 2, la red local o red LAN tiene como dirección la 192.168.2.0, de este modo *eth1* se configura en este rango de direcciones con dirección IP 192.168.2.1 y mascara de red 255.255.255.0, por este motivo todos los equipos de la red deberán apuntar hacia esta dirección como su puerta de enlace o Gateway y direcciones IPs en el rango 192.168.2. Para verificar su configuración, de manera igual con el comando *ifconfig* como se muestra en la figura 5.
Luego de tener correctamente configurado los parámetros de red para cada interfaz de red, se procede a realizar una pequeña prueba en donde se demuestra que las conexiones y la configuración están de forma correcta. Desde un terminal o ventana de comandos ejecutamos el comando *Ping* y la dirección IP de cualquier equipo de la red así: *ping 192.168.2.2*. Este comando envía una señal hacia el quipo cliente con dirección 192.168.2.2 y este devuelve su respuesta, de manera que si el servidor obtiene respuesta del equipo cliente existe la conexión entre el servidor y el equipo cliente de la red.

Como se puede observar en el diagrama de la red de la figura 2, la interfaz de red eth1 no tiene puerta de enlace o Gateway, por tal motivo no existe comunicación entre la interfaz de red eth0 y eth1, entre la red 192.168.1.0 y la red 192.168.2.0. Para que exista comunicación entre ellas se deberá crear un camino virtual por software entre estas, de manera que la red local pueda tener conexión a internet, es aquí cuando entra en acción el servidor con la herramienta *Iptables* como muro cortafuegos *y Squid* como Proxy.

7.4. **Servidor Proxy con *Squid* e *Iptables*.**

7.4.1. **Configuracion de *Ipatables***

Por medio de la herramienta *Iptables* se crea un camino virtual o muro cortafuegos para que exista comunicación entre la interfaz de red *eth1* y *eth0*, ejecutando ciertas reglas para definir cuál es la interfaz de red de trafico saliente *eth0* y trafico entrante *eth1*, hacer el reenvió de trafico entre ellas, definir cuál es la dirección de red que tendrá acceso por el muro cortafuegos, dirigir todo el trafico que entra por *eth1* hacia un puerto determinado.

Las cadenas pueden ser para tráfico entrante (INPUT), tráfico saliente (OUTPUT) o tráfico reenviado (FORWARD).
Las reglas de destino pueden ser aceptar conexiones (ACCEPT), descartar conexiones (DROP), rechazar conexiones (REJECT), encaminamiento posterior (POSTROUTING), encaminamiento previo (PREROUTING), SNAT, NAT, entre otras.

Las opciones más comunes son:

-A añade una cadena.
-i define una interfaz de tráfico entrante.
-o define una interfaz para trafico saliente.
-j establece una regla de destino del tráfico, que puede ser ACCEPT, DROP o REJECT.
-m define que se aplica la regla si hay una coincidencia específica.
--state define una lista separada por comas de distinto tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
--to-source define que IP reportar al tráfico externo.

-s define trafico de origen.
-d define tráfico de destino.
--source-port define el puerto desde el que se origina la conexión.
--destination-port define el puerto hacia el que se dirige la conexión.
-t tabla a utilizar, pueden ser nat, filter, mangle o raw.

Desde la ventana, consola o terminal de ejecución de comandos editar los siguientes comandos para la configuración de reglas de *Iptables*, cada comado termina con un enter.

Instalacion de *Iptables.*

yum –y install iptables

Luego de instalar la herramienta los siguientes comandos cargan la herramienta
Iptables para ser configurada.

modprobe ip_tables
modprobe iptable_nat

Para crear nuevas reglas, se deben borrar las existentes con los siguientes comandos.

iptables -F INPUT
iptables -F FORWARD
iptables -F OUTPUT
iptables -F -t nat

Definir el reenvio de paquetes entre la interfaz de trafico entrante y trafico saliente.

iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Definir todos los rangos de direcciones de origen y destino del trafico sean aceptadas.

iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT

Dirigir todo el trafico entrante por *eth1* hacia el puerto 8080.
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Habilitar el reenvio de paqutes.

echo 1 > proc/sys/net/ipv4/ip_forward

Salvar las reglas e iniciar el servicio *Iptables.*

service iptables save
service iptables start
chkconfig iptables on

7.4.2. **Configuracion de *Squid***

El control de acceso a Internet se hace por medio de la herramienta *Squid*, que brinda la posibilidad de administrar el contenido de tráfico proveniente de la red local. El control de acceso se hace ya sea por pagina Web, URL, Usuario, IP o intervalo de tiempo de conexión, *squid* permitirá o denegara el acceso por ejemplo si es o no un usuario valido de la red, el equipo tiene o no una IP valida, el sitio Web a visitar es permitido para ser visto por los usuarios de la red, la dirección del sitio Web contiene URL con contenido que el administrador considera no que no debe ser visto, el horario es o no el establecido para entrar en la Web. En el caso de hacerse la restricción de acceso se arrojara un mensaje por medio del navegador impidiendo la visita al sitio web o la conexión del usuario. *Squid* hace el filtrado escuchando peticiones por un puerto determinado, que por defecto de instalación es el puerto 8030, con *Iptables* se dirige todo el trafico hacia el puerto 8080 para que *Squid* haga el filtrado por este puerto.
Desde la ventana, consola o terminal de ejecución de comandos editar los siguientes comandos:

Instalación de *Squid.*

yum -y install squid

Entrar al directorio de *Squid.*

cd /etc/squid

Crear el directorio *listas* dentro del directorio *squid*.

sudo mkdir listas/

Dentro de *listas* crear los ficheros para las listas de restricciones y accesos permitidos.

sudo touch listas/{libres,redlocal,porno,extensiones,claves,inocentes}

Listar las propiedades del fichero que será utilizado para almacenar las claves de acceso, cambiar atributos de lectura y escritura solo para el usuario propietario:

ls -l listas/claves
sudo chmod 600 listas/claves

Cambiar el propietario del fichero de claves de acceso hacia el usuario *squid*, listar de nuevo las propiedades del fichero que será utilizado para almacenar las claves de
sudo chown squid.squid listas/claves
ls -l listas/claves

Crear los usuarios y sus contraseñas.

for usuario in mipc1 mipc2 mipc3
do
sudo htpasswd listas/claves $usuario
done

Editar los ficheros del directorio *listas,* cada uno con su contenido de restricción o de acceso correspondiente, con el comando editor de texto *sudo vim.* Luego de ejecutar el comando con el fichero a editar, oprimir la tecla *insert* y escribir el contenido correspondiente, para salir y guardar con el comando, *:wq* seguido de un enter.

Dentro de *libres* colocar la ip del servidor

sudo vim listas/libres

192.168.2.1

Dentro de *redlocal* colocar las ips de los equipos de la red.

sudo vim listas/redlocal

192.168.2.2

192.168.2.3

192.168.2.4

Dentro de *porno* colocar todos los contenidos, URL, sitios web, que no puedan ser vistos por los usuarios de la red.

sudo vim listas/porno

sex

www.porno.com

etc…..

Dentro de *extensiones* colocar todas las extensiones de archivos ejecutables o que puedan ser maliciosos.

sudo vim listas/extensiones

\.*bat$*

\.*pif$*

\.*sys$*

\.*lnk$*

\.*scr$*

\.*exe$*

Dentro de *inocentes* colocar todos los sitios web que no tiene restricciones de acceso.

sudo vim listas/inocentes

.alcancelibre.org

.google.com

Editar el fichero de configuración de *squid, squid.conf*, cambiando algunos parámetros que deja por defecto la instalación y agregando los necesarios para hacer el control y filtro de contenido.

Desde *vim*, ejecutar las siguientes búsquedas con /:

/# http_port 3128 , Reemplazar por*, http_port 192.168.2.1:8080.*
/#cache_dir ufs /var/spool/squid 100 16 256, remplazar por*, cache_dir ufs /var/spool/squid 512 16 256.*

/#auth_param basic program <uncomment and complete this line>, remplazar por*,*
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/listas/claves.
/#acl password proxy_auth REQUIRED, quitar el símbolo *#.*

/acl to_localhost dst 127.0.0.0, Debajo de ésta línea, agregar*:*

acl redlocal src "/etc/squid/listas/redlocal"
acl libres src "/etc/squid/listas/libres"
acl porno url_regex "/etc/squid/listas/porno"
acl extensiones urlpath_regex "/etc/squid/listas/extensiones"
acl inocentes dstdomain "/etc/squid/listas/inocentes"
acl matutino time MTWHF 08:00-19:00

/http_access deny all, Arriba de dicha línea, agregar*:*

http_access allow matutino redlocal password !porno !extensiones
http_access allow inocentes redlocal password
http_access allow libres

/# httpd_accel_port 80, Debajo de dicha línea, agregar*:*

httpd_accel_host virtual
httpd_accel_port 0
httpd_accel_with_proxy on

/# error_directory /usr/share/squid/errors/English, Remplazar por, *error_directory /usr/share/squid/errors/Spanish*

Iniciar la configuración de Squid a fin de verificar si hubo errores fatales:

service squid restart

Si hay errores, corregirlos. Si no devuelve depuración, examinar el fichero *squid.out*, en la dirección */var/log/squid/squid.out****.*** realizar correcciones.

sudo tail -f /var/log/squid/squid.out

Recargar la configuración de *Squid* a fin de verificar si hubo errores no fatales.

sudo service squid reload

7.4.3. **Pruebas del servidor proxy con *Squid* e *Iptables***

Luego de que la configuración de *squid* e *iptables* no tenga ningún error, se realizan las pruebas correspondientes para probar su funcionamiento, con un equipo perteneciente a la red o equipo de prueba, para el caso se toma un equipo con sistema operativo *Windows XP*.

Desde el equipo de la red, se configura su tarjeta red con los parámetros de red correspondientes para ser atendido por el servidor, siguiendo el diagrama de red de la figura 2, colocar al equipo la dirección IP 192.168.2.2, mascara 255.255.255.0 y puerta de enlace 192.168.2.1, además colocar las direcciones DNS de acuerdo a la empresa proveedora de internet.

Abrir el explorador de internet, y configurar la conexión en el menú *Herramientas*, pestaña de *Conexiones, Configuracion de LAN,* los parámetros para que se conecte al servidor proxy, como dirección IP del servidor y puerto. Luego de configurar la conexión, suministrar el usuario y contraseña, tal y como se creó en la configuración de *Squid.* (Ver figura 6).

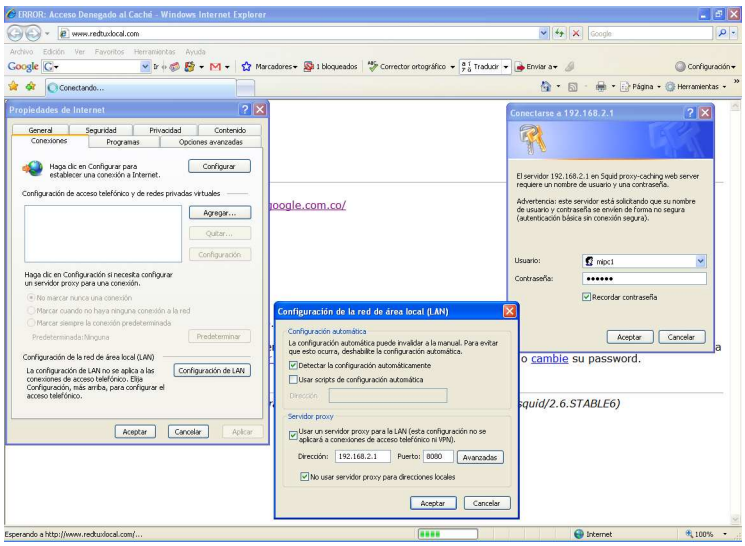

Figura 6. Configuración para usar Proxy.

En la barra de direcciones, colocar como sitio web *www.google.com*, realizar una búsqueda que contenga la palabra *sexo* o alguna definida en el fichero *porno* en la configuración de *Squid.* El servidor deberá impedir la entrada a todos los sitios web que contengan la URL sexo, o cualquiera definida en fichero *porno* con un mensaje como se muestra en la figura 7. Además no permitirá descargar archivos con las extensiones definidas en el fichero de *extensiones.* Solo permitirá hacer conexiones a los equipos que contengan una IP valida definidas en el fichero *redlocal*, y en el horario definido en el fichero de configuración de *squid squid.conf.*

Figura 7.

7.5. **Servidor DHCP con *Dhcp***

7.5.1. **Configuración de *Dhcp***

Dhcpd es una herramienta sencilla de instalar y configurar, tan solo después instalarse se edita el fichero de configuración *dhcpd.conf* en la ruta o directorio */etc/dhcpd.conf,* con los parámetros de red correspondientes a la

red local, que deberá entregar de forma automática a cada equipo que se conecte a la red.

Desde la ventana, consola o terminal de ejecución de comandos editar los siguientes comandos:

Instalar *Dhcp.*

yum -y install dhcp
Editar el fichero *dhcpd.conf* con el editor de *texto sudo vim*.

sudo vim /etc/dhcpd.conf

Escribir dentro del fichero el siguiente código.

```
ddns-update-style interim;
ignore client-updates;
shared-network eth1 {
        subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers 192.168.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.2.255;
        option domain-name "redtuxlocal.com";
        option domain-name-servers 201.221.151.31, 201.221.151.32,
192.168.2.1;
        range 192.168.2.2 192.168.2.253;
        default-lease-time 21600;
        max-lease-time 43200;
                        }
        host m2 {
```

option host-name "m2.redtuxlocal.com";
hardware ethernet 00:13:72:21:2D:09;
fixed-address 192.168.2.2;
}
}

En el fichero *dhcpd* ubicado en la ruta */etc/sysconfig/dhcpd*, colocar la interfaz de red perteneciente a la red local, editando DHCPDARGS=eth1.

sudo vim /etc/sysconfig/dhcpd

```
# Command line options here
DHCPDARGS=eth1
```

Iniciar el servicio

service dhcpd start

7.5.2. **Pruebas del servidor con *Dhcp***

Despues de configurar *Dhcp,* desde el equipo de pruebas de la red, configurar su tarjeta de red de manera que obtenga sus parámetros de red de manera automática o por dhcp. (Ver figura 8).

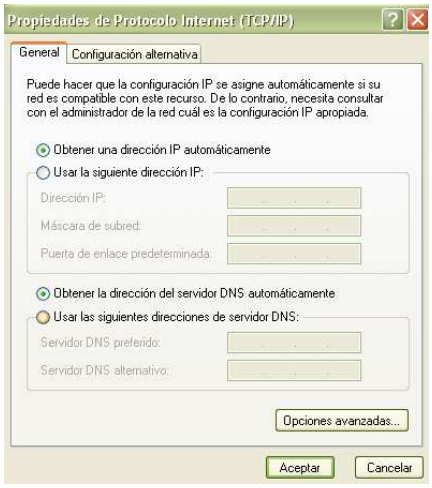

Figura 8. Configuración por dchp.

En el código que se edito en el fichero de configuración *dhcpd.conf*, se asigno la dirección 192.168.2.2 al equipo que contenga en su tarjeta de red la dirección *MAC,* 00:13:72:21:2D:09, de manera que al equipo de pruebas que contiene esta dirección *MAC* el servidor deberá entregar la dirección 192.168.2.2, además de la máscara 255.255.25.0, puerta de enlace 192.168.2.1 y Dns 201.221.151.31, 201.221.151.32, 192.168.2.1. A los demás equipos deberá entregar una dirección en el rango comprendido entre 192.168.2.2 a 192.168.2.253.

Para verificar en el equipo de pruebas que dirección le entrega el servidor, se ejecuta el comando *ipconfig /all* en la ventana de ejecución de comandos de Windows. (Ver figura 9).

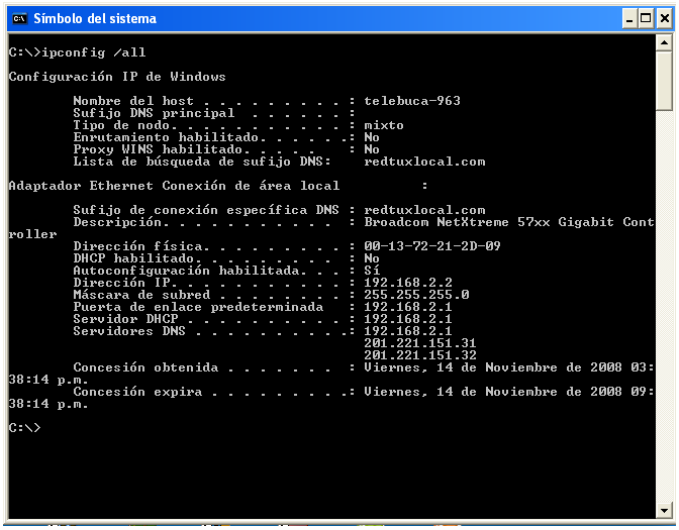

Figura 9. Ventana de comandos de Windows. Comando *ipconfig /all.*

7.6. **Servidor DNS con *Bind***

7.6.1. **Configuración de *Bind***

BIND, Berkeley Internet Name Domain, es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen: Un servidor de sistema de nombres de dominio *named*, Una biblioteca resolutoria de sistema de nombres de dominio, herramientas para verificar la operación adecuada del servidor *DNS bind-utils*.

Desde la ventana, consola o terminal de ejecución de comandos editar los siguientes comandos:

Instalar *bind,* sus librerías y herramientas necesarias para su configuración.

yum –y install bind bind-utils bind-libs bind-chroot caching-nameserver
yum –y install system-config-bind

Editar el fichero de configuración named.conf y definir los permisos de las IP que tienen acceso a consultar el servidor DNS, definir las zonas de reenvió y resolución inversa que serán consultadas por el servidor para la resolución de nombres y direcciones IP.

sudo vim /var/named/chroot/etc/named.conf

```
acl "redlocal" {
        127.0.0.1;
        192.168.2.0/24;
        192.168.3.0/24;
        };
options {
directory "/var/named/";
dump-file "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
allow-recursion { redlocal; };
                forwarders {
                200.33.146.209;
                200.33.146.217;
                };
        forward first;
        allow-query {
        redlocal;
        192.168.1.1;
        192.168.1.15;
        };
};
zone "localhost" {
type master;
```

file "localhost.zone";
allow-update { none; };
};
zone "localdoamin" {
type master;
file "localdomain.zone";
allow-update { none; };
};
zone "redlocal" {
type master;
file "redtuxlocal.zone";
allow-update { none; };
};
zone "2.168.192.in-addr.arpa" {
type master;
file "2.168.192.in-addr.arpa.zone";
allow-update { none; };
};

Crear el fichero de configuración .zone para la zona de reenvio y tendrá como contenido las IPs correspondientes a los nombres de cada equipo de la red.

sudo vim /var/named/chroot/var/named/redtuxlocal.com.co.zone

$TTL 86400
@ IN SOA server.redtuxlocal.com.co. root (
2008072542 ; número de serie
28800 ; tiempo de refresco
7200 ; tiempo entre reintentos de consulta

604800 ; tiempo tras el cual expira la zona
86400 ; tiempo total de vida
)

@	*IN*	*NS*	*server*	
@	*IN*	*MX*	*10*	*mail*
@	*IN*	*A*		*192.168.2.1*
intranet	*IN*	*A*		*192.168.2.1*
mipc1	*IN*	*A*		*192.168.2.2*
mipc2	*IN*	*A*		*192.168.2.3*
mipc3	*IN*	*A*		*192.168.2.4*
www	*IN*	*CNAME*		*intranet*
mail	*IN*	*A*		*192.168.2.1*
ftp	*IN*	*CNAME*		*intranet*
server	*IN*	*CNAME*		*intranet*

Crear el fichero de configuración .zone para la zona de resolucion inversa y tendrá como contenido el último numero de la dirección IP de la red correspondiente al nombre de dominio consultado.

sudo vim /var/named/chroot/var/named/2.168.192.in-addr.arpa.zone

$TTL 86400

@ IN SOA server.redtuxlocal.com.co. root (
2008072542 ; número de serie
28800 ; tiempo de refresco
7200 ; tiempo entre reintentos de consulta
604800 ; tiempo tras el cual expira la zona
86400 ; tiempo total de vida
)

@ IN NS server.redtuxlocal.com.co.
1 IN PTR intranet.redtuxlocal.com.co
2 IN PTR mipc1.redtuxlocal.com.co.
3 IN PTR mipc1.redtuxlocal.com.co.
4 IN PTR mipc1.redtuxlocal.com.co.

Reiniciar el servicio para guardar la configuración.

service named restart

En el fichero de consulta del servidor, colocar la dirección IP del servidor DNS, para indicarles al servidor que haga consultas con esa dirección.
sudo vim /etc/resolv.conf

search redtuxlocal.com.co
nameserver 127.0.0.1
nameserver 201.221.151.31
nameserver 201.221.151.32
nameserver 192.168.2.1

7.6.2. **Pruebas del servidor DNS con *Bind***

Luego de realizar la configuración de cada uno de los ficheros correspondientes, se prueba el funcionamiento con el equipo de pruebas de la red o desde el mismo servidor. El equipo de pruebas deberá tener como dirección de Dns la dirección IP del servidor 192.168.2.1.

Desde el terminal o ventana de comandos de Windows, ejecutar el comando *ping* seguido del nombre de dominio de la red o de cualquier equipo

perteneciente a la red, si se obtiene respuesta, el servidor estará resolviendo nombres de dominio de forma correcta. (Ver figura 10).

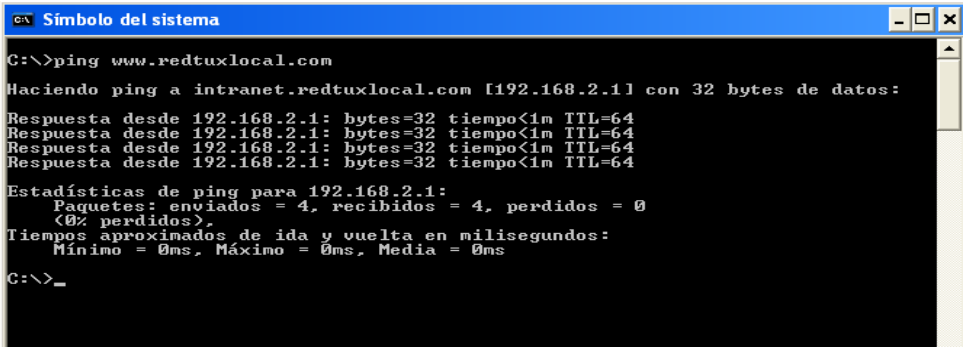

Figura 10.

7.7. **Servidor Web con *Apache***

7.7.1. **Configuración de *Apache***

Apache es un servidor *Http*, de código abierto y licenciamiento libre, que funciona en Linux, sistemas operativos derivados de Unix™, Windows, Novell Netware y otras plataformas. Ha desempeñado un papel muy importante en el crecimiento de la red mundial, y continua siendo el servidor *Http* más utilizado, siendo además el servidor de facto contra el cual se realizan las pruebas comparativas y de desempeño para otros productos competidores. Apache es desarrollado y mantenido por una comunidad de desarrolladores auspiciada por Apache Software Foundation.

Desde la ventana, consola o terminal de ejecución de comandos editar los siguientes comandos:

Instalar *Apache* mediante la herramienta *httpd.*

yum -y install httpd
yum -y install php php-mysql mod_perl mod_python mod_ssl

Luego de la descarga e instalación de las herramientas, *Apache* es un servicio que por fortuna solo es necesario instalar e iniciar. No requiere modificaciones adicionales para su funcionamiento básico.

chkconfig httpd on
service httpd start

7.7.2. **Prueba del servidor Web con *Apache***

Procedemos a probar el servicio entrando desde cualquier equipo de la red, en el navegador editamos en la barra de direcciones el nombre de dominio de la red www.redtuxlocal.com y deberá devolver la pagina HTML que trae por defecto *Apache*. (Ver figura 11).

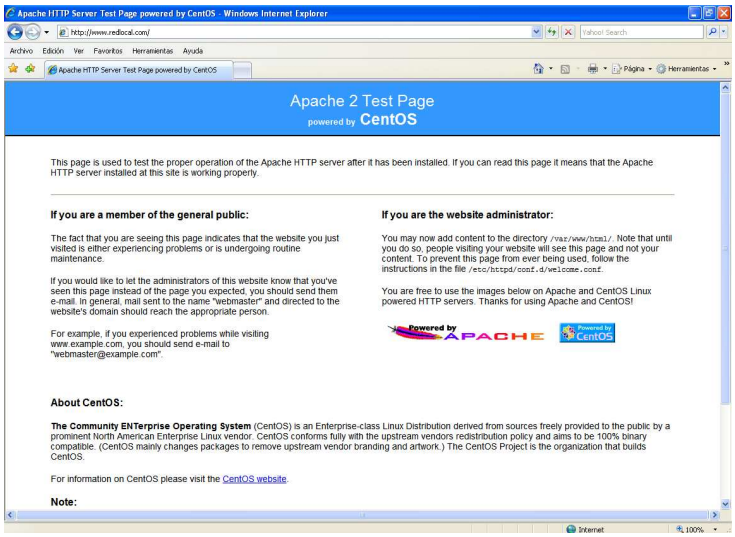

Figura 11. Pagina HTML por defecto en la configuración de *Apcahe*.

Si se desea crear y diseñar una página Web en formato HTML, se puede crear un archivo con extensión *.html* y guardar este archivo que contiene el diseño de la página web dentro del directorio /var/www/html/. (Ver figura 12).

/var/www/html/paginaprueba.html

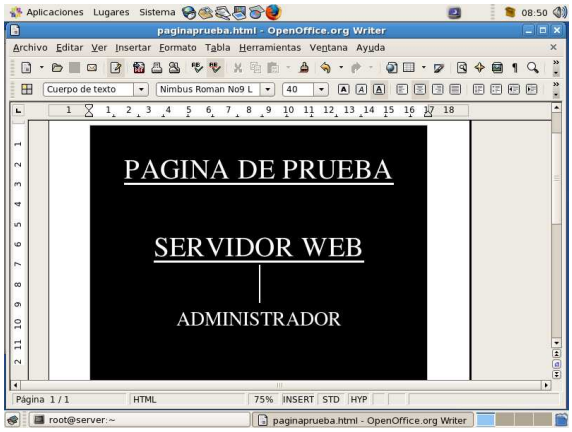

Figura 12. Creando página web en formato HTML con OpenOffice.org.

En el fichero *welcome.conf* ubicado en el directorio */etc/httpd/conf.d/welcome.conf*, deshabilitar todos los comandos dentro del fichero, colocándolos en comentario agregando el símbolo numeral # al inicio de cada línea de código para quitar la pagina por defecto.

Luego en el fichero *php.conf* ubicado en la dirección */etc/httpd/conf.d/php.conf*, cambiar la línea que dice, *DirectoryIndex index.php*, por, *DirectoryIndex paginaprueba.html.*

Reiniciamos el servicio *httpd*.

service httpd restart

Entrar de nuevo al navegador y escribir la dirección de la red www.redtuxlocal.com, debe aparecer la página web creada. (Ver figura 13).

Figura 13. Pagina web de la red.

8. **Conclusiones**

La implementación de un servidor en una red de área local es de gran utilidad en el intercambio de información, en la organización y administración de la red, permitiendo a los usuarios compartir información de manera rápida y segura en forma simultánea sin afectar los recursos de la red.

Al ser Linux un software de distribución libre, coloca a disposición el código fuente del software para todo aquel que requiera modificar y adaptar alguna característica en cualquier aplicación que esté desarrollando, mejorando la funcionalidad y utilidades del sistema de acuerdo a sus necesidades.

Contar con un servidor proxy ofrece a los administradores de la red controlar la información filtrando su contenido, protegiendo a la red de información no deseada y restringiendo el acceso a la red por medio del muro cortafuegos a los intrusos además de funcionar como cache disminuyendo el tiempo en la consulta de archivos.

Los servidores basados en Linux son programas que se ejecutan en una maquina que tan solo requiere de un procesador en buen estado, tan solo cierta capacidad de memoria RAM y memoria de almacenamiento, ofreciendo la capacidad de bajo costo en su implementación y desarrollo.

Los conocimientos adquiridos en la práctica profundizan y enriquecen la orientación teórica obtenida en cada semestre de la carrera, alimentados de la experiencia de cada uno de los compañeros de trabajo, complementando la formación profesional en el campo laboral.

Durante la práctica se tuvo contacto con equipos de alta tecnología y arquitectura, aprendiendo y observando su funcionamiento, configuraciones y utilidades, generando un gran aporte en el conocimiento tecnológico de herramientas y equipos que se encuentran en el mercado.

Las relaciones en el campo laboral con el supervisor de la practica y jefe inmediato fueron muy agradables y llevaderas, así como el ambiente laboral con los demás compañeros de trabajo, en el cual me brindaban su ayuda y conocimientos, contaban con mis opiniones y sugerencias, dejando así una huella en la calidad de mi trabajo.

9. **Bibliografía**

Manual de Referencia LINUX, Richard Petersen, Segunda edición, Osborne Mc Graw Hill.

Linux Para Todos Implementación de Servidores con GNU/Linux, Joel Barrios Dueñas, Edición febrero 2007.

http://www.alcancelibre.org/staticpages/index.php/manuales-indice, (23 de Junio de 2008).

http://www.alcancelibre.org/staticpages/index.php/introduccion-iptables, (25 de Junio de 2008).

http://www.alcancelibre.org/staticpages/index.php/como-dhcp-lan, (4 de Julio de 2008).

http://www.alcancelibre.org/staticpages/index.php/manuales-indice, (29 de Julio de 2008).

http://www.alcancelibre.org/staticpages/index.php/como-dns, (12 de Agosto de 2008).

http://www.alcancelibre.org/staticpages/index.php/como-apache, (14 de Octubre de 2008).