

DISEÑO DE UN PROTOTIPO PARA LA ADMINISTRACION Y GESTION DE  
RECURSOS DE LA RED DEL PROGRAMA PRESIDENCIAL FAMILIAS EN  
ACCION DE BUCARAMANGA

ING. CESAR AUGUSTO LOPEZ CORTES

UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD FISICOMECHANICAS  
ESCUELA INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES  
BUCARAMANGA

2009

DISEÑO DE UN PROTOTIPO PARA LA ADMINISTRACION Y GESTION DE  
RECURSOS DE LA RED DEL PROGRAMA PRESIDENCIAL FAMILIAS EN  
ACCION DE BUCARAMANGA

CESAR AUGUSTO LOPEZ CORTES

Trabajo de Grado presentado como requisito  
para optar al título de Especialista en Telecomunicaciones  
Director: ING. PAOLA GUZMAN CASTILLO

UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD FISICOMECHANICAS  
ESCUELA INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES  
BUCARAMANGA

2009

## **AGRADECIMIENTOS**

A mi directora de tesis Ingeniera Paola Guzmán, por su constante apoyo y dedicación en la realización de este proyecto.

A mi familia por el apoyo económico y humano realizado; en fin a todas aquellas personas que nos ayudaron en todos los aspectos para que este proyecto sea exitoso. Gracias.

## **DEDICATORIA**

A mi madre Ruby de López Cortes, a mi padre Gustavo López Cardona y a mi hermana Tatiana López Cortés, por su gran apoyo en la realización de este proyecto.

Finalmente a nuestros amigos que nos han acompañado, quienes sin ningún interés nos apoyaron durante 2 años, con los cuales he crecido como persona.

## TABLA DE CONTENIDO

	pág.
INTRODUCCION	1
PLANTEAMIENTO DEL PROBLEMA	3
JUSTIFICACIÓN DEL PROBLEMA	4
OBJETIVO GENERAL	5
OBJETIVOS ESPECIFICOS	5
1 MARCO TEORICO	6
1.1 SISTEMA OPERATIVO LINUX	6
1.2 WEBMIN	9
1.3 SQUID DEFINICION	10
1.4 ACL (LISTAS DE CONTROL DE ACCESO)	11
1.4.1 DEFINICIÓN.	11
1.4.2 TIPOS DE ACL.	12
1.4.3 COLOCACIÓN DE LAS ACL.	12
1.5 ACL EN SQUID DEFINICION	13
1.5.1 DEFINICIÓN.	13
1.5.2 TIPOS DE ACL.	13
1.6 HTTP_ACCESS	18
1.6.1 CARACTERÍSTICAS DE HTTP_ACCESS.	19
1.6.2 EJEMPLOS DE ACL Y HTTP_ACCESS.	20
1.7 MODELOS DE GESTIÓN DE REDES	21
1.8 MODELO GESTOR-AGENTE Y COMPONENTES BÁSICOS	23
1.8.1 COMMON MANAGEMENT INFORMATION PROTOCOL.	23
1.8.2 SIMPLE NETWORK MANAGEMENT PROTOCOL.	25
1.8.3 COMPARACIÓN CON CMIP.	25
2 INSTALACION LINUX	26

2.1	INSTALACION DE FEDORA 10	26
2.2	CONFIGURACION DE USUARIO ROOT	37
2.3	CONFIGURACION DE RED	40
3	INSTALACION SERVIDOR	43
3.1	UTILITARIO WEBMIN	43
3.2	COMPROBACIÓN DE INSTALACIÓN WEBMIN	43
3.2.1	DESCOMPRESION PAQUETE.	44
3.2.2	INSTALACIÓN WEBMIN.	44
3.2.3	INICIANDO WEBMIN.	46
3.3	INSTALACION SQUID	48
3.3.1	INSTALACIÓN SERVIDOR PROXY SQUID.	48
3.3.2	INICIALIZACIÓN DE SQUID.	50
4	INSTALACION Y CONFIGURACION SQUID FAMILIAS EN ACCION	52
4.1	EDICION SQUID.CONF SERVIDOR FAMILIAS EN ACCION	52
4.2	CONFIGURACION DE LOS ERRORES DE SQUID	58
5	GESTION DE LA RED DE DATOS FAMILIAS EN ACCION	60
5.1	SELECCIÓN HERRAMIENTAS DE GESTION	61
5.2	MAPA DE LA RED FAMILIAS EN ACCION	63
5.3	LISTA DE DIRECCIONES MAC	64
5.4	ESCANEEO DE PUERTOS	65
6	PRUEBAS Y RESULTADOS	66
	CONCLUSIONES	68
	BIBLIOGRAFIA	70

## LISTA DE FIGURAS

	pág.
Figura No.1: Arquitectura OSI	23
Figura No.2: Arquitectura SNMP	24
Figura No.3: Opción de instalación	26
Figura No.4: Test de unidad	27
Figura No.5: Instalación en modo gráfico	27
Figura No.6: Selección de idioma de instalación	28
Figura No.7: Selección de idioma del teclado	28
Figura No.8: Selección del nombre del equipo	29
Figura No.9: Selección de huso horario	29
Figura No.10: Selección de contraseña de root	30
Figura No.11: Partición de discos duros	31
Figura No.12: Partición con encriptación	32
Figura No.13: Selección de aplicaciones	32
Figura No.14: Selección de herramientas de instalación	33
Figura No.15: Copia de archivos de instalación	33
Figura No.16: Proceso de configuración de usuario	34
Figura No.17: Información de licencia	34
Figura No.18: crear usuario	35
Figura No.19: Configuración de Fecha y hora	35
Figura No.20: Perfiles de hardware	36
Figura No.21: Inicio de sesión usuario sin privilegios	37
Figura No.22: Terminal	37

Figura No.23: Editar gdm	38
Figura No.24: Archivo gdm	38
Figura No.25: Inicio sesión root	39
Figura No.26: Sesión root	39
Figura No.27: Utilidad de Red	40
Figura No.28: Configuración de Red	40
Figura No.29: Configurar dispositivo ethernet	41
Figura No.30: Configurar eth0	41
Figura No.31: Archivo network-scripts	42
Figura No.32: Comando whereis	43
Figura No.33: Descomprimir archivo .tar	44
Figura No.34: Preba Webmin	46
Figura No.35: Configuración de tema Webmin	47
Figura No.36: Webmin con tema amigable	47
Figura No.37: Descarga del Servidor Squid	48
Figura No.38: Instalación de Squid	49
Figura No.39: Inicializar Squid	50
Figura No.40: Comando gedit	51
Figura No.41: Editar Squid.conf	51
Figura No.42: Editar ACL	52
Figura No.43: Editar Mis ACL	54
Figura No.44: ACL IVAN	54
Figura No.45: ACL NEGADOS	55
Figura No.46: ACL INOCENTES	56
Figura No.47: ACL MAC	57
Figura No.48: Editar ERR_ACCESS_DENIED	58
Figura No.49: Prueba pagina bloqueada	59
Figura No.50: Cuadro comparativo software de gestión	61

Figura No.51: Mapa de la red familias en Acción	63
Figura No.52: MAC Address Discovery	64
Figura No.53. Port Scanner	65

## RESUMEN

**TITULO:** DISEÑO DE UN PROTOTIPO PARA LA ADMINISTRACION Y GESTION DE RECURSOS DE LA RED DEL PROGRAMA PRESIDENCIAL FAMILIAS EN ACCION DE BUCARAMANGA\*

**AUTOR:** CESAR AUGUSTO LOPEZ CORTÉS\*\*

**PALABRAS CLAVES:** WEBMIN, SQUID, PROXY, GESTION DE REDES, ACL, HTTP-ACCESS.

### CONTENIDO:

La adecuada configuración y administración de recursos de la red es una tarea fundamental en pro de lograr un mejor desempeño, sin importar el tamaño o tipo de red, estas acciones tienen como fin la reducción de costos, el mejor aprovechamiento del ancho de banda y los recursos de la organización.

Entendiendo esto, la necesidad de una correcta administración de la red del programa Presidencial Familias en Acción de la ciudad de Bucaramanga se ha convertido en el objeto de estudio de este trabajo.

Los Objetivos del proyecto de grado son:

- ✚ Documentar la topología de la red, especificación de dispositivos de red, equipos de cómputo y servidor.
- ✚ Analizar las principales aplicaciones herramientas de software y sitios web a los que acceden los funcionarios.
- ✚ Realizar la instalación y configuración del servidor Linux.
- ✚ Implementar soluciones de software para la administración y gestión de la red.

Los temas principales son:

- ✚ WEBMIN: La gran mayoría de servicios y utilitarios de Linux se pueden administrar y configurar tanto de manera gráfica como por consola, y una de esas maneras es mediante la interfaz web Webmin.
- ✚ SQUID: Una forma de acelerar la navegación Web es mediante la instalación de una caché. Squid es un software que cachea datos de Internet. Lo realiza guardando las peticiones que los usuarios realizan.
- ✚ ACL: Las ACL permiten un control del tráfico de la red a nivel de los enrutadores. Una ACL es una lista de una o más instrucciones
- ✚ HTTP\_ACCESS: Este es el parámetro que permite o deniega accesos a una o más ACL.
- ✚ GESTION: El modelo de gestión OSI basado en el protocolo CMIP es más utilizado en la administración de equipos y redes de telecomunicación y el modelo de gestión de Internet basado en el protocolo SNMP para gestión de equipos y servicios sobre redes de datos.

\* Proyecto de Grado

\*\* Facultad Fisicomecánicas. Escuela Ingeniería Eléctrica, Electrónica y de Telecomunicaciones.  
Directora Ing. Paola Guzmán Castillo.

## ABSTRACT

**TITLE:** DESIGN OF A PROTOTYPE TO MANAGE AND ADMINISTRATE THE RESOURCES OF THE NETWORK OF THE PRESIDENTIAL PROGRAM “FAMILIAS EN ACCION” FROM BUCARAMANGA\*

**AUTHOR:** CESAR AUGUSTO LOPEZ CORTÉS\*\*

**KEY WORDS:** WEBMIN, SQUID, PROXY, NETWORK MANAGEMENT, ACL, HTTP-ACCESS.

### CONTENT:

The appropriate setup and management of the resources of the network is a fundamental task in order to achieve a better performance, without taking into account the size or type of network. The purpose of these actions is to reduce the cost, improve the use of the bandwidth and the resources of the organization. Having this in mind, the need of a right administration of the network of the presidential program Familias en Acción from the city of Bucaramanga has become in the aim of study of this project.

The objectives of this project are:

- ✚ To illustrate the features of the network, characteristics of the network devices, computers and server.
- ✚ To analyze the main tool applications of the software and the websites the staff members get Access to.
- ✚ To carry out the installation and setup of the Linux server. .
- ✚ To complement the software solutions for the administration and network management.

The principal topics are:

- ✚ WEBMIN: Most of the services and utilities of Linux can be managed and setup by console as well as graphically, one of these ways is through the webmin interface.
  - ✚ SQUID: One way to accelerate the Web navigation is through the installation of a cache. Squid is a software which cachés internet data. It makes this by saving the users requirements.
  - ✚ ACL: the ACL allows a network traffic control to the router level. An ACL is a list of one or more instructions.
  - ✚ HTTP\_ACCESS: It is the parameter that allows or denies the access to one or more ACLs.
- MANAGEMENT: it is the management model OSI based in the CMIP protocol, it is the most used in the device management and telecommunication networks and the internet management model based in the SNMP protocol for the management of devices and services of data network.

\*Proyecto de Grado

\*\*Facultad Fisicomecánicas. Escuela Ingeniería Eléctrica, Electrónica y de Telecomunicaciones.  
Directora Ing. Paola Guzmán Castillo.

## INTRODUCCION

La adecuada configuración y administración de recursos de la red es una tarea fundamental en pro de lograr un mejor desempeño, sin importar el tamaño o tipo de red, estas acciones tienen como fin la reducción de costos, el mejor aprovechamiento del ancho de banda y los recursos de la organización.

Entendiendo esto, la necesidad de una correcta administración de la red del programa Presidencial Familias en Acción de la ciudad de Bucaramanga se ha convertido en el objeto de estudio de este trabajo.

El presente trabajo se centra en la Administración y Gestión de redes de datos, que se puede definir como la utilización y disposición de los recursos para la planificación, organización, mantenimiento, supervisión, evaluación y control de los dispositivos y elementos de las redes de comunicaciones con el fin de adaptarse a la calidad de servicio requerida, a un costo específico<sup>1</sup>.

La característica principal de la gestión de redes es el rendimiento de la red la cual va directamente relacionada con la velocidad de la misma, por ejemplo la velocidad con la que es vista una aplicación por los usuarios finales.

---

<sup>1</sup> GESTION EN REDES DE COMPUTADORES. Cohorte IX, Ciclo IV. Especialización en Telecomunicaciones UIS, 2009. p 3.

El desarrollo de este trabajo obedece al interés de realizar una administración de recursos en la sede del Programa Presidencial de Familias en Acción dada por unas políticas de seguridad y de gestión ya establecidas por la Alcaldía de Bucaramanga.

La gestión de la red se realizó con herramientas de libre distribución encontradas en internet e instaladas sobre el sistema operativo Linux Fedora 10, y la metodología utilizada fue basada en la configuración de servicios de red mediante la interfaz web Webmin y el Proxy Squid.

## **PLANTEAMIENTO DEL PROBLEMA**

Las redes y los sistemas informáticos que complementan su entorno, deben proporcionar una respuesta flexible a las cargas de trabajo que generan las distintas aplicaciones de un sistema. La carga de trabajo es la adición de todos los procesos de una aplicación o grupo de aplicaciones. Para que una red sea flexible y estable debe contar con una administración y gestión de recursos apropiada que combina la restricción de acceso a recursos específicos, el manejo de preferencias de los usuarios, la regulación de los recursos que consume cada aplicación, la definición de prioridades por aplicación con base en eventos externos y equilibrar las garantías de recursos para un conjunto de aplicaciones con el fin de maximizar el uso del sistema.

La Alcaldía de Bucaramanga tiene unas políticas de seguridad estrictas en todas sus dependencias en cuanto al control y seguridad en sus equipos de cómputo, para que los funcionarios desempeñen un trabajo de mejor calidad y bajo los parámetros requeridos los cuales incluyen bloqueo de programas de mensajería, control de usuarios, acceso a páginas no permitidas, generación y restricción de privilegios.

El programa Presidencial Familias en Acción de la Ciudad de Bucaramanga cuenta con los equipos y dispositivos necesarios para la implementación de un sistema de administración que permita el manejo de restricciones, pero este aún no ha sido implementado.

La formulación del problema a resolver en este proyecto es la siguiente:

¿Cómo contribuir a la administración y gestión de recursos de la red del programa Familias en Acción de la Ciudad de Bucaramanga?

## **JUSTIFICACIÓN DEL PROBLEMA**

Este trabajo de grado es una oportunidad para el estudiante de aplicar y profundizar los conocimientos y habilidades adquiridos en la especialización de Telecomunicaciones de la Universidad Industrial de Santander, específicamente en el campo de la administración y gestión de recursos de redes por medio de Proxy.

Con este proyecto se pretende dar solución en el campo de las Telecomunicaciones a un problema que se presenta constantemente en las empresas, y se trata de la seguridad informática, la cual tiene una gran importancia al tratarse de la protección de la información, el control y acceso de los usuarios a los equipos de cómputo.

Con el desarrollo de este proyecto se busca contribuir al control de la red del programa presidencial Familias en Acción.

## **OBJETIVO GENERAL**

- ✚ Diseñar un prototipo para la administración y gestión de la red del programa presidencial Familias en Acción.

## **OBJETIVOS ESPECIFICOS**

- ✚ Documentar la topología de la red, especificación de dispositivos de red, equipos de cómputo y servidor.
- ✚ Analizar las principales aplicaciones herramientas de software y sitios web a los que acceden los funcionarios.
- ✚ Realizar la instalación y configuración del servidor Linux.
- ✚ Implementar soluciones de software en la administración y gestión de la red, para el aprovechamiento ideal de todos sus recursos según sus requerimientos.
- ✚ Redactar el informe final del proyecto, con el cumplimiento de las normas de trabajos escritos y demás requisitos de calidad académica.

# 1 MARCO TEORICO<sup>2</sup>

## 1.1 SISTEMA OPERATIVO LINUX

El sistema operativo Linux nació en abril de 1991 como el pasatiempo de un estudiante finlandés de 21 años, llamado Linus Torvalds, quien cursaba segundo año de Ciencias de los Computadores en la universidad de Helsinki en Finlandia. Este joven empezó a crear un programa con la intención inicial de producir una versión más sencilla del sistema operativo Unix, que pudiera utilizarse en computadores personales y que brindara más estabilidad y confiabilidad que los actuales sistemas DOS y Windows. (Unix es un sistema operativo para servidores y máquinas de alto rendimiento).

En enero de 1992 Linux tenía cerca de 100 usuarios y varios de ellos ya participaban en su desarrollo con mejoras y correcciones que enviaban a través de Internet ya que su código fuente ha permanecido abierto a sus seguidores desde

---

<sup>2</sup> FUNDACIÓN EDUCATIVA CALASANZ    Informática    Linux [en línea].  
< <http://www.calasanz-pereira.edu.co/index.php/Informatica/linux.html> > [citado en 25 de junio de 2009]

un comienzo. Fue entonces cuando lanzó su primera versión, la 0.12 la cual incluía partes desarrolladas por otros programadores.

En 1994 se hizo pública la primera versión completa del sistema operativo: la 1.0. Esta versión ofreció soporte para redes y varias utilidades.

En 1998, los principales fabricantes de software como Corel, IBM, Netscape, Oracle, HP y Dell, anunciaron versiones para Linux de sus productos. Este respaldo fue clave para la consolidación de este sistema operativo que dominaba cerca del 17% del mercado con 7.5 millones de usuarios ;de ellos unos 10.000 participaban en su desarrollo y optimización.

En la actualidad, programadores de todo el mundo participan en su desarrollo. Está siendo utilizado ampliamente en servidores de Internet, lo utilizan Universidades alrededor del todo el mundo para sus redes y sus clases, en la industria como software de apoyo a su maquinaria, en cadenas de supermercados, estaciones de servicio y muchas instituciones del gobierno y militares en varios países. Obviamente, también es utilizado por miles de usuarios en sus computadores personales. El apoyo más grande, sin duda, ha sido Internet ya que a través de ella se ha podido demostrar que se puede crear un sistema operativo para todos los usuarios sin la necesidad de fines lucrativos.

Un ejemplo de la popularidad que ha alcanzado el sistema y la confianza que se puede depositar en él, es que incluso la NASA ha creído en su seguridad y eficacia utilizándolo en misiones espaciales y control de experimentos.

Torvalds distribuyó Linux bajo un tipo de licencia llamada GPL (Licencia Pública General), que permite a cualquier persona bajar, usar y modificar el software sin ningún costo; la única condición que ha impuesto su creador, es que los cambios o

mejoras que una persona o compañía realicen también deben ser públicos, es decir que debe quedar su código fuente disponible, de la misma forma que está disponible el código de Linux y que además no tienen permiso de realizar restricciones con respecto a la utilización de este programa modificado.

Este tipo de licencia llamada también de código abierto (Open Source), fue creada para mantener la libertad del software y evitar que alguien quiera apropiarse de la autoría intelectual de un determinado programa. La licencia advierte que el software debe ser gratuito y que el paquete final, ya modificado, también debe ser gratuito.

## 1.2 WEBMIN

La gran mayoría de servicios y utilitarios de Linux se pueden administrar y configurar tanto de manera gráfica como por consola, y una de esas maneras es mediante la interfaz web Webmin, la cual incorpora todos los servicios presentes en el sistema operativo. Se puede configurar por ejemplo un servidor web, un servidor de correo, servidor de DNS y muchas otras utilidades importantes como usuarios, cuotas de espacio, servicios, archivos de configuración y apagado del equipo.

La interfaz web Webmin se instaló con el fin de poder configurar de una manera más amigable tanto las funciones de red como la caché Squid que más adelante será necesario para la gestión de la red del programa presidencial Familias en Acción de la ciudad de Bucaramanga.

Los paquetes de instalación que se descargan de Internet como es el caso del utilitario Webmin, pueden ser descargados con diferentes tipos de extensiones las cuales son “.tar” el cual es un formato de archivo diseñado para almacenar archivos de forma conveniente en cintas magnéticas y por ello su nombre que proviene de “Tape Archiver” y “.rpm” originalmente llamado Red Hat Package Manager, el cual es capaz de instalar, desinstalar, verificar, solicitar y actualizar paquetes de programas.<sup>3</sup>

---

<sup>3</sup> RPM Start Page [en línea].  
< <http://www.rpm.org> > [citado en 15 de julio de 2009]

### 1.3 SQUID DEFINICION<sup>4</sup>

Una forma de acelerar la navegación Web es mediante la instalación de una caché. Squid se ha destacado por ser una de las mejores caches que existen, y es utilizada por miles de empresas y proveedores de servicios de Internet (ISP) en todo el mundo. Se trata de un software gratuito, diseñado para UNIX. De sobra es conocido que el ancho de banda de las conexiones es un bien preciado. La instalación de una caché eficientemente configurada puede dar resultados sorprendentes. Además, no es necesario hacer una fuerte inversión en un servidor SUN o similar, ya que Squid funciona bajo Windows NT y soporta lógicamente plataformas Intel.

Squid es un software que cachea datos de Internet. Lo realiza guardando las peticiones que los usuarios realizan. En otras palabras, si una persona quiere descargar una página Web, pide a squid que obtenga dicha página. Squid se conecta al servidor remoto y solicita la página. Después reenvía la petición al usuario ,pero al mismo tiempo mantiene una copia. La próxima vez que alguien desee dicha página, squid simplemente la lee del disco y la transfiere al usuario de forma instantánea. Squid soporta actualmente los protocolos HTTP, FTP, GOPHER, SSL y WHOIS. No soporta otros protocolos como RealAudio, Streams y similares.

---

<sup>4</sup> UNIVERSIDAD DISTRITAL Arincon Proxy [en línea].  
< <http://www.udistrital.edu.co/comunidad/estudiantes/arincon/proxy.php> > [citado en 27 de junio de 2009]

## 1.4 ACL (LISTAS DE CONTROL DE ACCESO)<sup>5</sup>

### 1.4.1 Definición.

Las ACL permiten un control del tráfico de la red a nivel de los enrutadores. Pueden ser parte de una solución de seguridad junto con otros componentes, como antivirus, anti-espías, firewall, proxy, etc.

Pasos que realiza una ACL

- + Una ACL es una lista de una o más instrucciones
- + Se asigna una lista a una o más interfaces
- + Cada instrucción permite o rechaza tráfico usando uno o más de los siguientes criterios: el origen del tráfico; el destino del tráfico; el protocolo usado.
- + El servidor proxy analiza cada paquete, comparándolo con la ACL correspondiente
- + El servidor proxy compara la ACL línea por línea. Si encuentra una coincidencia, toma la acción correspondiente (aceptar o rechazar), y ya no revisa los restantes renglones.
- + Si no encuentra una coincidencia en ninguno de los renglones, rechaza automáticamente el tráfico. Consideren que hay un "deny any" implícito, al final de cada ACL

---

<sup>5</sup> GEOCITIES Cisco ACL [en línea].  
< <http://www.geocities.com/hilmarz/cisco/acl.htm> > [citado en 27 de junio de 2009]

### 1.4.2 Tipos de ACL.

✚ Las ACL estándar (1-99) sólo permiten controlar en base a la dirección de origen.

✚ Las ACL extendidas (100-199) permiten controlar el tráfico en base a la dirección de origen; la dirección de destino; y el protocolo utilizado.

Es posible usar ACL nombradas en vez de usar un rango de números. El darles un nombre facilita entender la configuración y por lo tanto, también facilita hacer correcciones. Si se considera sólo el tráfico de tipo TCP/IP, para cada interface puede haber sólo una ACL para tráfico entrante, y una ACL para tráfico saliente.

### 1.4.3 Colocación de las ACL.

✚ Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones: no se puede distinguir el destino.

✚ Las ACL extendidas se colocan cerca del origen del tráfico, por eficiencia, es decir, para evitar tráfico innecesario en el resto de la red.

## 1.5 ACL EN SQUID DEFINICION<sup>6</sup>

### 1.5.1 Definición.

En Squid se especifica mediante el parámetro acl según la siguiente sintaxis:

```
acl nombre_acl tipo_acl descripción ...
```

```
acl nombre_acl tipo_acl "fichero_de_descripciones" ...
```

Cuando se usa un "fichero\_de\_descripciones", cada descripción se corresponde con una línea del fichero.

### 1.5.2 Tipos de ACL.

#### a) src

Especifica una dirección origen de una conexión en formato IP/máscara.

Ejemplo: se utilizará una ACL de tipo src para especificar la red local:

```
acl red_local src 192.168.1.0/24
```

---

<sup>6</sup> BDAT Documentos squid [en línea].  
< <http://dns.bdat.net/documentos/squid/x30.html> > [citado en 29 de junio de 2009]

También se pueden especificar rangos de direcciones mediante una ACL de tipo src:

```
acl jefes src 192.168.1.10-192.168.1.25/32
```

### **b) dst**

Especifica una dirección destino de una conexión en formato IP/máscara.

```
acl google_es dst 216.239.0.0/24
```

También se pueden especificar hosts específicos mediante una ACL de tipo dst:

```
acl google_es2 dst 216.239.59.104/32 216.239.39.104/32
```

Las definiciones son idénticas a las ACL de tipo src salvo que se aplican al destino de las conexiones no al origen.

### **c) srcdomain y dstdomain**

Estos tipos de ACL especifican un nombre de dominio.

En el caso de srcdomain es el dominio origen y se determina por resolución DNS inversa de la IP de la máquina, es decir, se debe tener bien configurado el DNS de la red local.

Si se quiere al PC del gerente llamada 'gerencia' identificarlo como 'gerencia.miempresa.com' como nombre DNS.

```
acl gerente srcdomain gerencia.miempresa.com
```

En el caso de `dstdomain` el nombre del dominio se comprueba con el dominio que se haya especificado en la petición de página web.

```
acl google_com dstdomain google.com
```

#### d) `srcdom_regex` y `dstdom_regex`

Especifican una expresión regular que verifica los dominios origen o destino. La expresión regular hace distinción entre mayúsculas y minúsculas salvo que se incluya la opción "-i" que evita dicha distinción.

```
acl google_todos dstdom_regex -i google\.*
```

Se observa como al incluir "-i" se está indicando que no haga distinción entre mayúsculas y minúsculas.

#### e) `time`

Este tipo de ACL permite especificar una franja horaria concreta dentro de una semana. La sintaxis es la siguiente:

```
acl nombre_acl_horaria time [dias-abrev] [h1:m1-h2:m2]
```

Donde la abreviatura del día es:

S - Sunday (domingo)

M - Monday (lunes)

T - Tuesday (martes)

W - Wednesday (miércoles)

H - Thursday (jueves)

F - Friday (viernes)

A - Saturday (sábado)

Además la primera hora especificada debe ser menor que la segunda, es decir h1:m1 tiene que ser menor que h2:m2

```
acl horario_laboral time M T W H F 8:00-15:00
```

Especificando un horario de 8 a 15 y de lunes a viernes.

#### f) url\_regex

Permite especificar expresiones regulares para comprobar una URL completa, desde el http:// inicial.

Ejemplo, establecer una ACL que se verifique con todos los servidores cuyo nombre sea adserver:

```
acl url_regex serv_publicidad ^http://adserver.*
```

Si se requiere una ACL que verifique las peticiones de ficheros mp3:

```
acl url_regex ficheros_mp3 -i mp3$
```

#### g) refer\_regex

Define una ACL que se comprueba con el enlace que se ha pulsado para acceder a una determinada página. Cada petición de una página web incluye la dirección donde se ha pulsado para acceder. Si se escribe la dirección en el navegador entonces se está haciendo una petición directa.

Ejemplo, establecer una ACL para todas las páginas a las que se acceda pulsando en una ventana de búsqueda de google:

```
acl pincha_google referer_regex http://www.google.*
```

## h) req\_mime

Las ACL de tipo req\_mime se utilizan para comprobar el tipo de petición mime que realiza un cliente, y se puede utilizar para detectar ciertas descargas de ficheros o ciertas peticiones en túneles HTTP.

Esta ACL sólo comprueba las peticiones que realiza el cliente, no comprueba la respuesta del servidor. Esto es importante para tener claro qué se está controlando

### Ejemplos

```
+ acl subida req_mime_type -i ^multipart/form-data$
+ acl javascript req_mime_type -i ^application/x-javascript$
+ acl estilos req_mime_type -i ^text/css$
+ acl audiompeg req_mime_type -i ^audio/mpeg$
```

## i) rep\_mime\_type

Este tipo de ACL se utiliza para verificar el tipo de respuesta recibida por el proxy. Este tipo de ACL, analiza una respuesta del servidor por lo que sólo le afectan las reglas de respuesta como **http\_reply\_access** y no las reglas **http\_access** que se aplican a las peticiones.

### Ejemplos

```
+ acl javascript rep_mime_type -i ^application/x-javascript$
+ acl ejecutables rep_mime_type -i ^application/octet-stream$
+ acl audiompeg rep_mime_type -i ^audio/mpeg$
```

## 1.9 HTTP\_ACCESS

Este es el parámetro que permite o deniega accesos a una o más ACL.

La sintaxis de uso es:

```
⚡ http_access allow|deny [!]acl ...
```

Se observa como cada ACL puede ir precedida por un signo "!" que indicaría que la ACL no se verifica.

Por ejemplo, para permitir acceso fuera del horario laboral, según una ACL que definida anteriormente:

```
⚡ http_access allow! horario_laboral
```

Para denegar el acceso en horario laboral

```
⚡ http_access deny horario_laboral
```

Para dar acceso completo a la red local

```
⚡ http_access allow red_local
```

## 1.10 Características de `http_access`.

Si no hay ninguna línea de acceso la acción predeterminada es denegar la petición.

Si una petición no ha verificado ninguna línea de acceso, la acción que se realiza es la opuesta a la última línea de la lista. Si la última línea deniega entonces el valor predeterminado es permitir. Por este motivo es conveniente incluir una línea "deny all" o "allow all" al final de las listas de accesos para tener las cosas claras.

Es importante la forma en la cual se agregan los distintos parámetros **`http_access`** para determinar la forma en la que se comprueba. En primer lugar, todas las ACL incluidas en una cláusula `http_access` se comprueban y todas ellas tendrán que verificarse conjuntamente, es decir, como si estuvieran unidas por un operador AND. Después, los sucesivos parámetros **`http_access`** se evalúan individualmente, es decir, como si estuvieran unidos mediante un operador OR.

Ejemplo

```
+ acl red1 src 192.168.0.0/24
+ acl red2 src 192.168.1.0/24
+ http_access allow red1 red2
```

Permitiría el acceso a todas aquellas conexiones que procedieran a la vez de `red1` y de `red2`, que probablemente no es lo que se pretende. Para permitir acceso a las dos redes se podría emplear:

```
+ acl red1 src 192.168.0.0/24
+ acl red2 src 192.168.1.0/24
+ http_access allow red1
+ http_access allow red2
```

O también, de forma más sencilla:

```
+ acl redes src 192.168.0.0/24 192.168.1.0/24
+ http_access allow redes
```

### 1.11 Ejemplos de acl y http\_access.

Denegar las peticiones de ficheros de tipo exe, pif, bat y cmd

```
+ acl tipoexe url_regex -i exe$ pif$ bat$ cmd$
+ http_access deny tipoexe
```

Denegar el acceso a todos los servidores cuyo nombre comience por "popup", "banner" o "ads"

```
+ acl incordios url_regex http://popup.* http://ads.* http://ads.*
+ http_access deny incordios
```

Denegar todos los ficheros de tipo exe que provengan de virus\_fijo.com

```
+ acl anti_exe url_regex -i exe$
+ acl vfijo dstdomain virus_fijo.com
+ http_access deny anti_exe vfijo
```

Denegar las conexiones a las URL completas o incompletas que hay en el fichero "/etc/squid/lista\_negra\_1.txt"

```
+ acl ln1 url_regex "/etc/squid/lista_negra_1.txt"
+ http_access deny ln1
```

## 1.12 MODELOS DE GESTIÓN DE REDES

En los años 90 se dio la aparición de los primeros protocolos de gestión de redes como SNMP(Simple Network Management Protocol) y OSI SM(Open Systems interconnection) conocido también como CMIP propuesto por la organización internacional de estándares el cual permitió el acceso de manera uniforme a los recursos gestionados de una red de comunicaciones.

Hoy en día las soluciones que han permitido una gestión integrada de recursos, también han supuesto la paradoja de que no puede existir realmente una gestión integrada en su totalidad: El modelo de gestión OSI basado en el protocolo CMIP es más utilizado en la administración de equipos y redes de telecomunicación y el modelo de gestión de Internet basado en el protocolo SNMP para gestión de equipos y servicios sobre redes de datos, las cuales trabajan con diferente protocolo, su propia estructura de la información y sus propias definiciones de información, lo cual reside en la falta de interoperabilidad entre ellas.

Un modelo actual de gestión de redes es el modelo WBEM (gestión basada en web) y su modelo de información asociado CIM utilizado en la gestión de sistemas y aplicaciones.

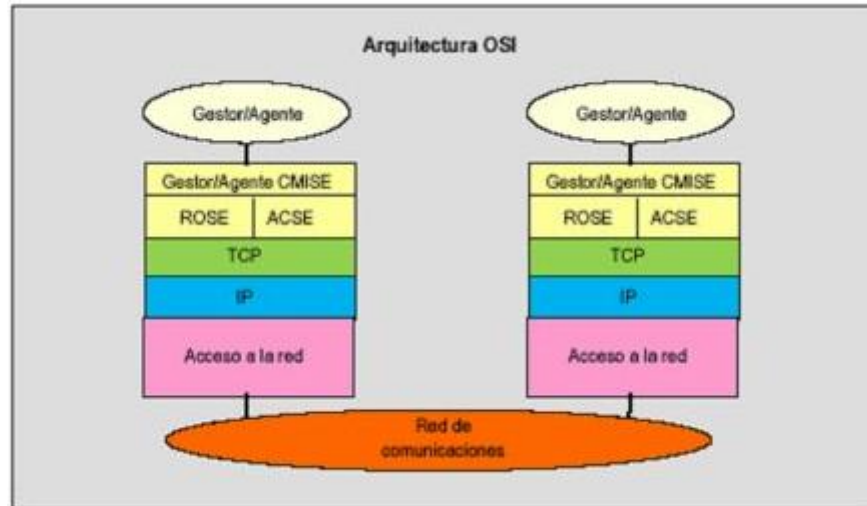
En cuanto a lo que se refiere con la estructura de la información, en Internet se ha definido SMI (Structure of management Information), mientras que OSI definió GDMO (Guidelines for the definition of Managed Objects); y en cuanto a gestión de equipos ha sido llevada por un modelo independiente DMI (Desktop Management Interface) con su propio protocolo MIF(Managed Information Format).

La utilización de CORBA (*Common Object Request Broker Architecture*), como aplicación de una tecnología de procesamiento distribuido a la gestión de red han permitido flexibilizar el acceso a los recursos, pero a la vez ha añadido más complejidad a la gestión integrada, sumando un nuevo protocolo de acceso (IIOP, Internet Inter-ORB Protocol) y estructura de definición de la información de gestión (IDL, Interface Definition Language) a los ya existentes.

En la actualidad se han realizado propuestas de soluciones para la integración estándar como son IIMC, DMI-SNMP y JIDM.

## 1.13 MODELO GESTOR-AGENTE Y COMPONENTES BÁSICOS<sup>7</sup>

Figura No.1: Arquitectura OSI



Fuente: Referencia 7

### 1.8.1 Common Management Information Protocol.

Desarrollado por ISO. Es de propósito general, no restringido a TCP/IP. Es sofisticado, incluye comandos potentes pero complejos. Es más versátil pero no está tan difundido. Es orientado a conexión.

CMIP comunica los gestores de cada capa (Layer Management Entities) con las aplicaciones de gestión (System Management Application Entities). Cada LME opera en un nivel OSI y no da una visión global de la operación. A su vez hay un

---

<sup>7</sup> CITEL COMISION INTEROAMERICANA DE TELECOMUNICACIONES TCP-IP [en línea].  
< [http://www.citel.oas.org/newsletter/2007/abril/tcp-ip\\_e.asp](http://www.citel.oas.org/newsletter/2007/abril/tcp-ip_e.asp) [citado en 30 de junio de 2009]

SMAE para cada LME. Los SMAE de diferentes dispositivos se comunican con CMIP para permitir al administrador la recolección y el análisis de los datos de la red como un todo, servicio llamado a veces Common Management Information Service.

Se definen las siguientes operaciones:

**ACTION** – Solicita se ejecute una acción de acuerdo con lo previsto en la estación gestionada.

**GET** – Solicita el valor de una instancia de un objeto gestionado.

**SET** – Establece el valor de una instancia de un objeto gestionado.

**CANCEL\_GET** – Cancela una solicitud GET.

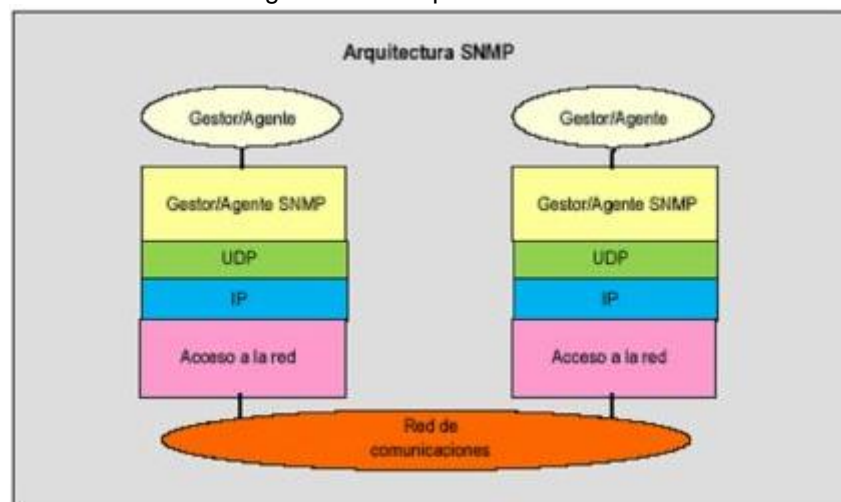
**CREATE** – Crea una instancia de un objeto gestionado.

**DELETE** – Elimina una instancia de un objeto gestionado.

**CMIP over TCP/IP (CMOT)**

Se definió por parte del Internet Architecture Board (IAB) como la solución de largo plazo que reemplazaría a SNMP.

Figura No.2: Arquitectura SNMP



Fuente: Referencia 7

### **1.8.2 Simple Network Management Protocol.**

Desarrollado por IETF se emplea ampliamente en ambientes TCP/IP. Es no orientado a conexión, emplea UDP y se sitúa en el nivel aplicación.

El agente reside en los dispositivos y emplea mínimos recursos para no perjudicar la performance. Colecciona datos y los almacena en la base que reside en el dispositivo.

La gestión con SNMP es de tipo distribuido, ya que cada entidad puede desempeñarse como gestor o como agente, o como ambos. A su vez, un agente puede responder a múltiples gestores.

Emplea UDP para las comunicaciones.

### **1.8.3 Comparación con CMIP.**

Las variables CMIP permiten ejecutar tareas y no sólo enviar información como en SNMP.

CMIP es más seguro que SNMP porque soporta autorización, control de accesos, y registros de seguridad (logs). CMIP logra mayor eficiencia que SNMP con una sola solicitud.

CMIP reporta mejor las condiciones inusuales de la red.

El protocolo SNMP es el de uso más difundido.

## 2 INSTALACION LINUX

### 2.1 INSTALACION DE FEDORA 10

Antes de instalar el sistema operativo hay que asegurar que el booteo se encuentre con la unidad DVD. Se inserta el DVD de instalación y se espera a que en la pantalla aparezca la imagen (Figura No. 1).

Figura No.3: Opción de instalación



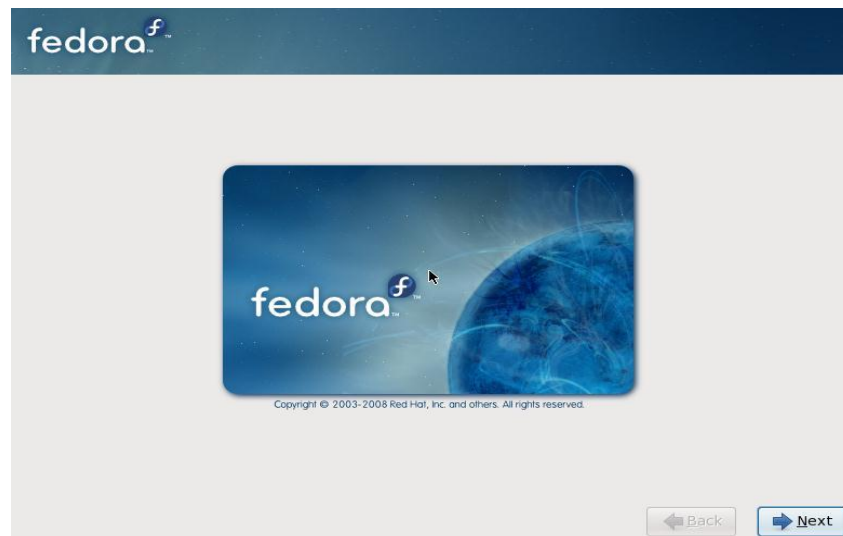
Se selecciona la primera opción de la figura No. 1 para una instalación nueva, a continuación se muestra la pantalla siguiente figura No. 2 la cual es un test para comprobar la unidad.

Figura No.4: Test de unidad



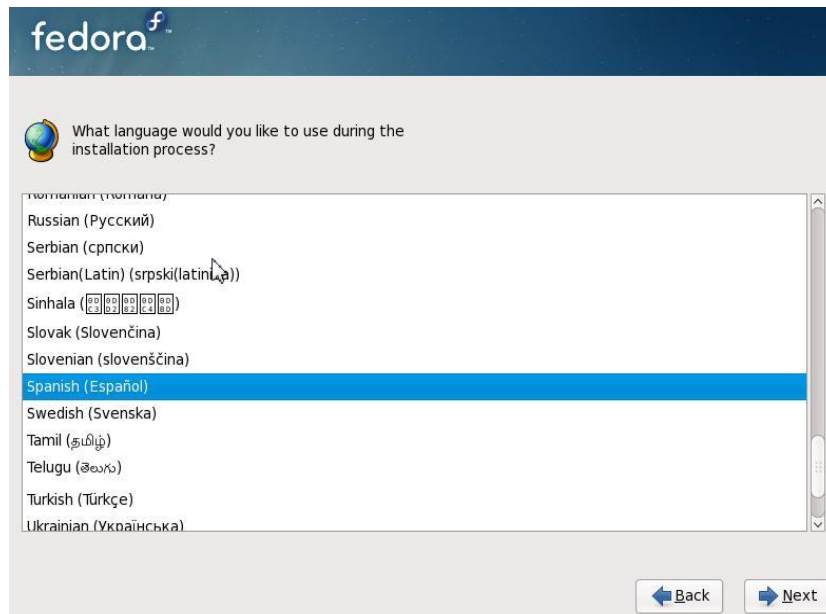
La figura No. 3 es el inicio de la instalación en modo gráfico. Al dar un click con el botón del mouse en el botón "NEXT" aparecerá la figura No. 4 para la selección del idioma de instalación.

Figura No.5: Instalación en modo gráfico



En la figura No. 4 se escoge el idioma con el que se desea realizar el proceso de instalación, en este caso se escogió el idioma español.

Figura No.6: Selección de idioma de instalación



En la figura No. 5 se escoge la configuración de idioma del teclado el cual también se encuentra en español.

Figura No.7: Selección de idioma del teclado

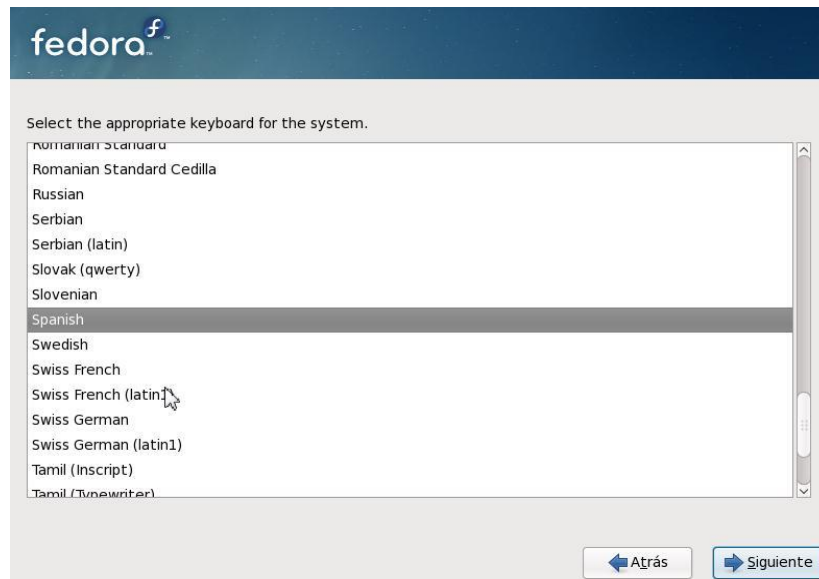
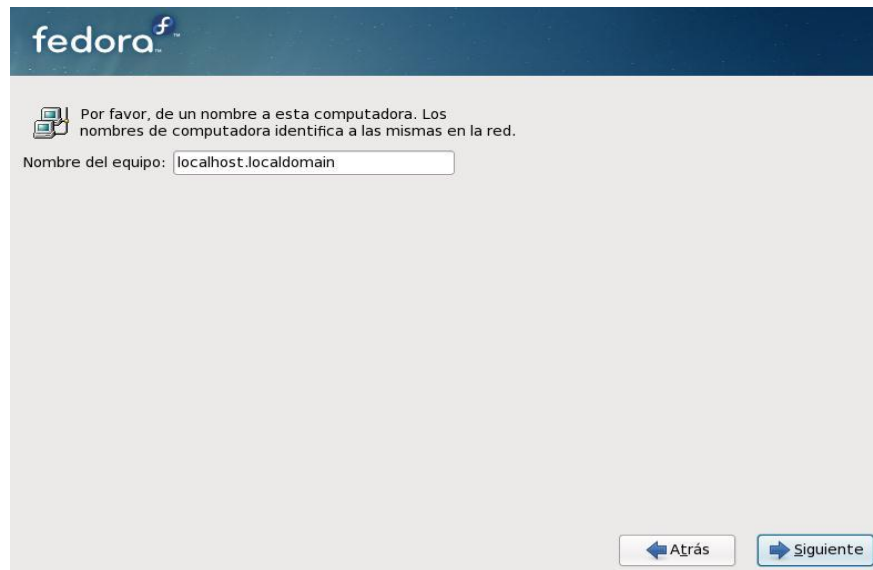


Figura No.8: Selección del nombre del equipo



El nombre del equipo puede ser seleccionado a gusto como se muestra en la figura No. 6, en este caso se le asignó el nombre de “servidor” al tratarse del servidor de Familias en Acción.

Figura No.9: Selección de huso horario



En la figura No. 7 se selecciona el huso horario de acuerdo a la ubicación actual, por ejemplo América/Bogotá, a continuación en la figura No. 8 se selecciona una contraseña para el root la cual debe ser de más de 12 caracteres por seguridad.

Figura No.10: Selección de contraseña de root



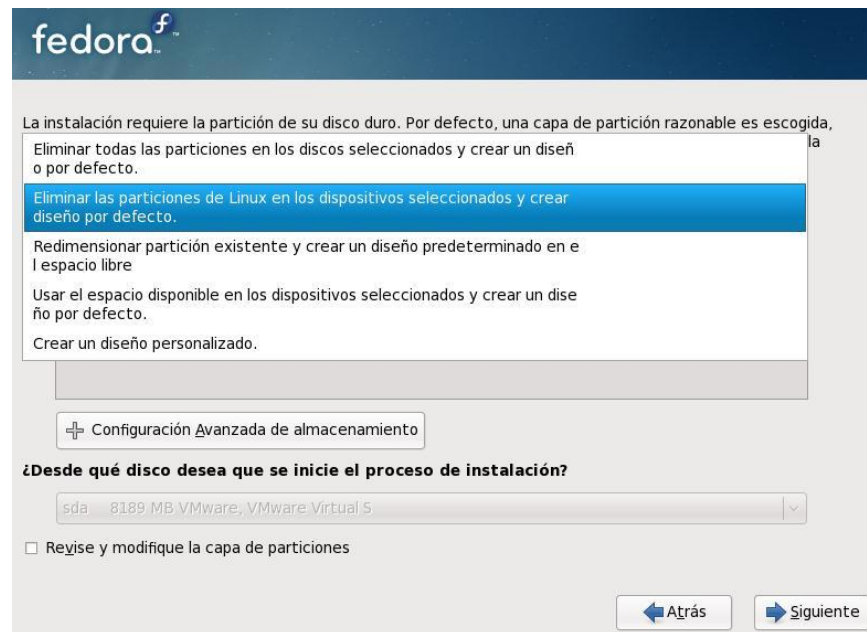
The screenshot shows the Fedora installer's root password setup screen. At the top, the Fedora logo is displayed. Below it, a yellow shield icon is followed by the text: "La cuenta root se utiliza para la administración del sistema. Introduzca una contraseña para el usuario root." There are two input fields: "Contraseña de root:" and "Confirmar:". Both fields contain masked characters (dots). A mouse cursor is positioned over the "Confirmar:" field. At the bottom right, there are two buttons: "Atrás" (Back) and "Siguiente" (Next).

Se debe tener cuidado en el proceso de partición de los discos duros y en las diferentes opciones de configuración. En la figura No. 9 se encuentran las opciones disponibles.

- ✚ Eliminar todas las particiones del disco duro y realizar una instalación por defecto en todo el espacio.
- ✚ Eliminar todas las particiones con el sistema de ficheros de cualquier distribución de GNU/Linux e instalar Fedora 10 sobre ese espacio.
- ✚ Redimensionar cualquier partición del disco y usar el espacio liberado para realizar la nueva instalación.

- ✚ Usar el espacio libre de los discos que se seleccionen para completar la instalación.
- ✚ Crear un diseño personalizado de la tabla de particiones.

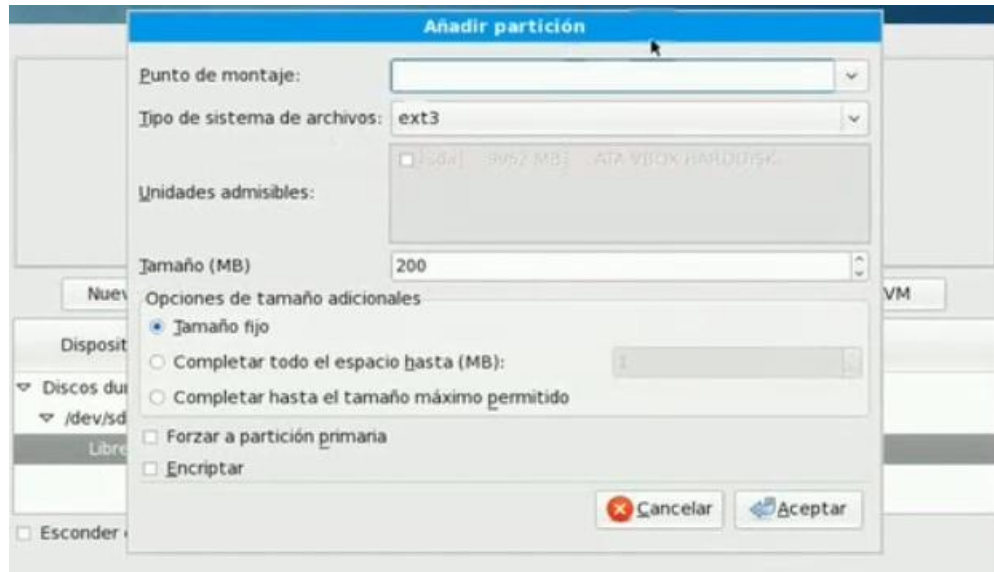
Figura No.11: Partición de discos duros



En la última opción de configuración de particiones se encuentra la creación de diseño personalizado. El programa mostrará la figura No. 10 con todo el sistema de particionado, en el cual se puede ir creando cada espacio, punto de montaje, sistema de ficheros, cifrado y todas las demás opciones necesarias.

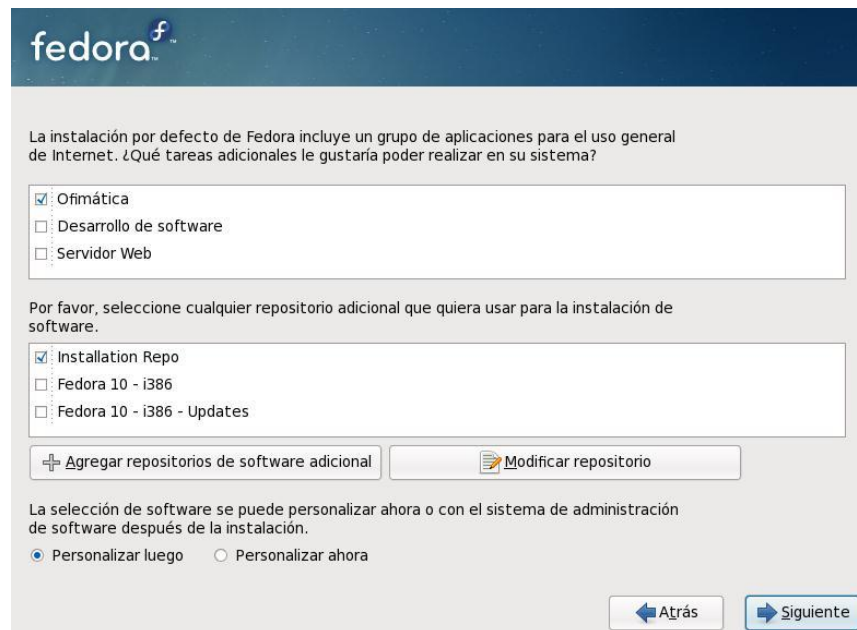
La instalación brinda la posibilidad de crear las particiones con un sistema de ficheros **cifrado**, pensando en el usuario que requiera una especial privacidad y seguridad sobre sus datos.

Figura No.12: Partición con encriptación



En la figura No. 11 se realiza la selección de aplicaciones dependiendo de las necesidades del servidor o su finalidad.

Figura No.13: Selección de aplicaciones



En las opciones de selección de herramientas de instalación, como son las opciones de servidores se deben seleccionar solo los servicios indispensables dentro del servidor por cuestiones de seguridad se evita abrir puertos innecesarios como muestra la figura No. 12.

Figura No.14: Selección de herramientas de instalación

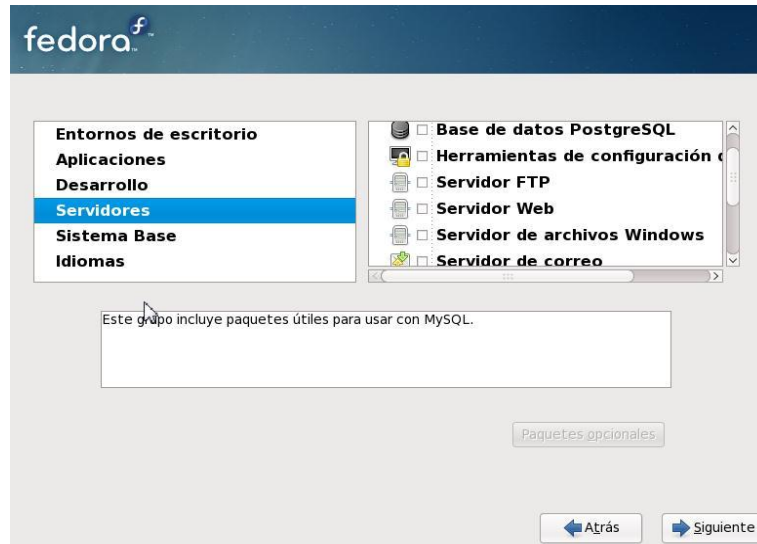


Figura No.15: Copia de archivos de instalación

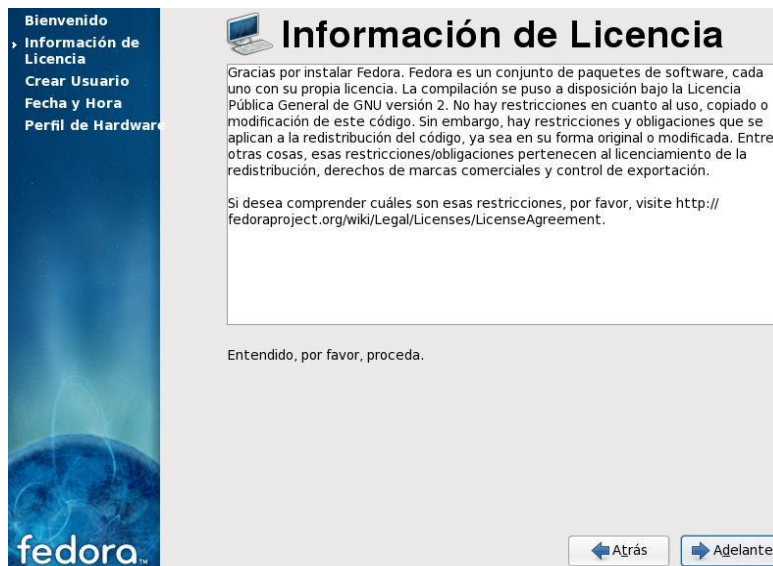


Después de seleccionar las herramientas de instalación se procede a iniciar la copia de archivos como se muestra en la figura No. 13. A continuación se inicia un proceso de configuración de usuario referenciado en la figura No. 14 y un acuerdo de información de licencia referenciado en la figura No. 15.

Figura No.16: Proceso de configuración de usuario



Figura No.17: Información de licencia



Se recomienda crear un usuario para uso normal sin preferencias administrativas referenciado en la figura No. 16.

Figura No.18: crear usuario

Bienvenido  
Información de Licencia  
▶ Crear Usuario  
Fecha y Hora  
Perfil de Hardware

## Crear Usuario

Se recomienda crear un 'nombre\_usuario' para uso normal (no administrativo) de su sistema. Para crear un sistema 'nombre\_usuario', por favor, provea la información que se pide más abajo.

Nombre de Usuario: Familias  
Nombre Completo: Familias en Acción  
Contraseña: \*\*\*\*\*  
Confirme la Contraseña: \*\*\*\*\*

Si necesita usar autenticación de red, tal como Kerberos o NIS, por favor haga clic en el botón Usar Ingreso por Red.

Usar Ingreso por Red...

← Atrás    Adelante →

Figura No.19: Configuración de Fecha y hora

Bienvenido  
Información de Licencia  
Crear Usuario  
▶ Fecha y Hora  
Perfil de Hardware

## Fecha y Hora

Por favor, ingrese la fecha y hora del sistema.

Fecha y hora    Protocolo de Tiempo de Red (NTP)

Fecha

< mayo >							< 2009 >						
lun	mar	mié	jue	vie	sáb	dom							
27	28	29	30	1	2	3							
4	5	6	7	8	9	10							
11	12	13	14	15	16	17							
18	19	20	21	22	23	24							
25	26	27	28	29	30	31							
1	2	3	4	5	6	7							

Hora

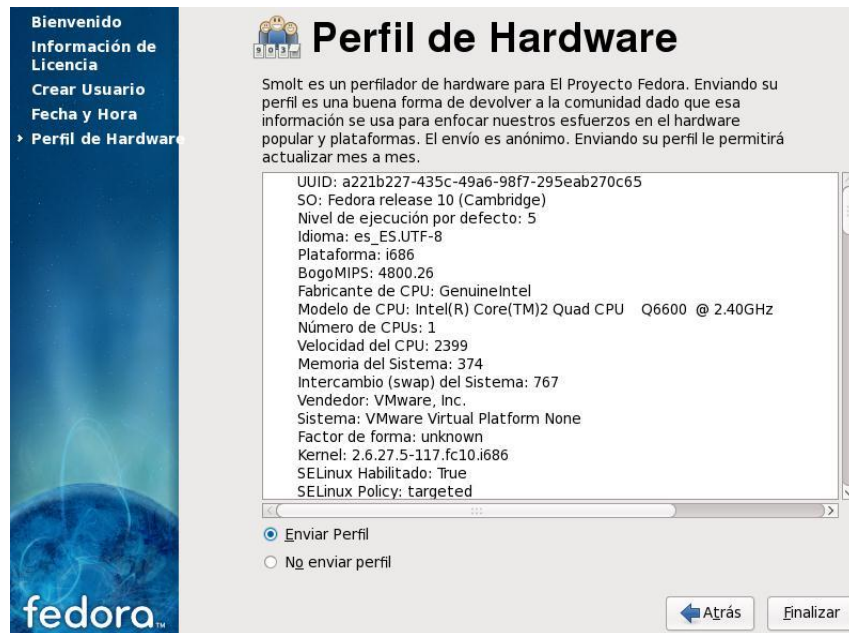
Hora actual : 10:24:44

Hora : 10  
Minuto : 9  
Segundo : 37

← Atrás    Adelante →

En la figura No. 17 se configura la fecha y hora actual de acuerdo a la ubicación, y por último en la figura No. 18 se decide sobre el envío del perfil de hardware a los desarrolladores de Fedora para su mejoramiento.

Figura No.20: Perfiles de hardware



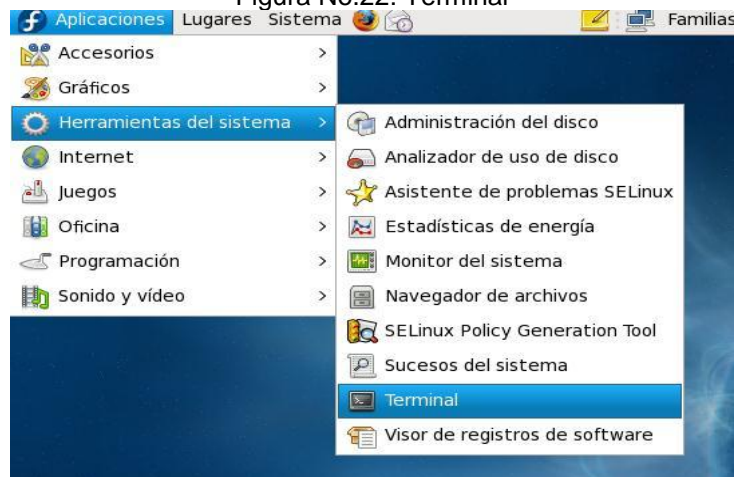
## 2.2 CONFIGURACION DE USUARIO ROOT

Se inicia sesión con el nombre de usuario (sin privilegios) creado y su respectiva contraseña figura No. 19, y a continuación se ingresa al Terminal para configurar el inicio con usuario root como en la figura No. 20.

Figura No.21: Inicio de sesión usuario sin privilegios



Figura No.22: Terminal



Se edita el archivo gdm dentro de la carpeta /etc/pam.d/, para editarlo se abre el terminal y se escribe lo indicado en la figura No. 21,

(su -) este comando permite entrar como root

(gedit /etc/pam.d/gdm) Edición del archivo gdm

Figura No.23: Editar gdm



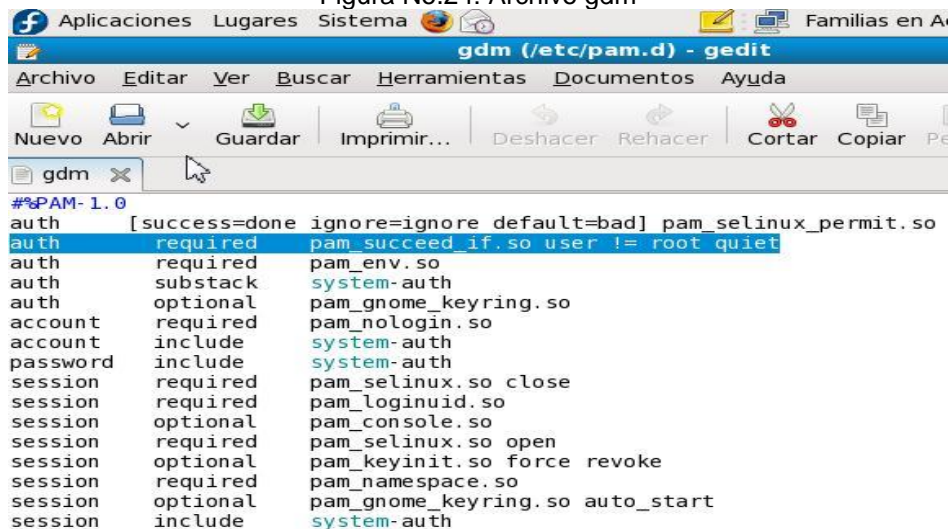
En el archivo se buscamos una línea que dice;

auth required pam\_succeed\_if.so user != root quiet (figura No. 22).

Se edita la línea para que quede de la siguiente manera.

auth required pam\_succeed\_if.so user quiet

Figura No.24: Archivo gdm



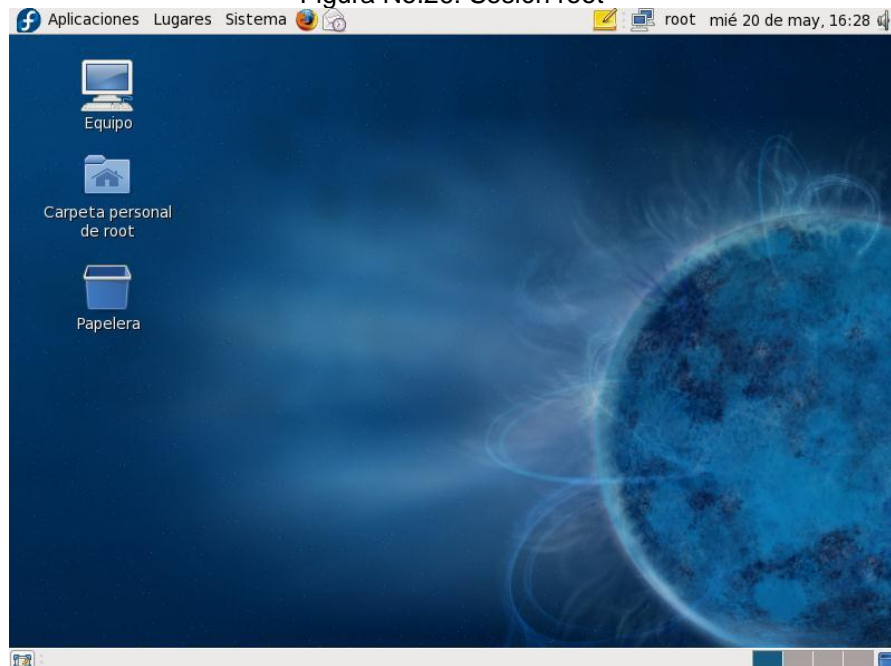
Ahora se puede cerrar sesión e iniciar como root para tener todos los privilegios habilitados como se muestra en la figura No. 23.

Figura No.25: Inicio sesión root



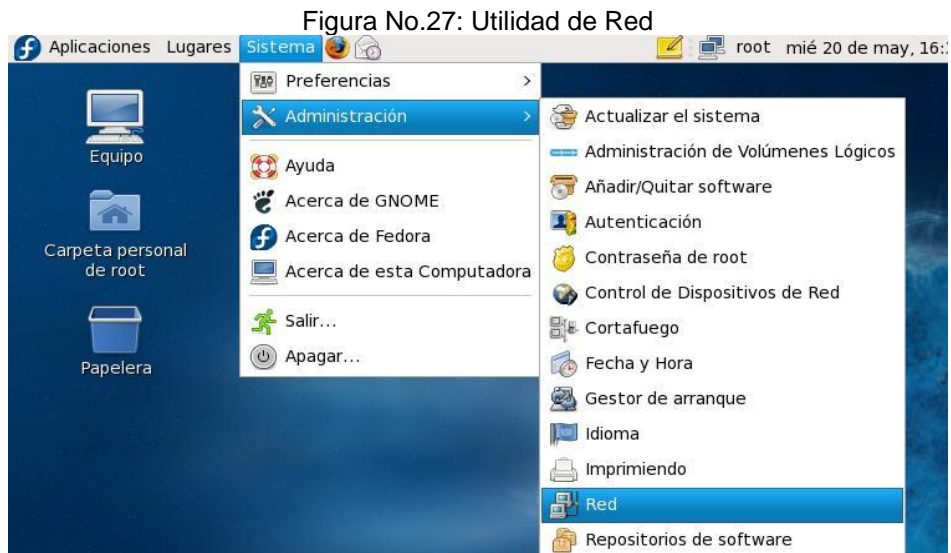
En la figura No. 24 se puede observar el escritorio de la sesión root.

Figura No.26: Sesión root



## 2.3 CONFIGURACION DE RED

En la pestaña Sistema y dentro de esta en la pestaña Administración se encuentra la utilidad para configurar la red, figura No. 25.



En la configuración de red se encuentran las 2 tarjetas de red del servidor como se muestra en la figura No. 26. Una de las tarjetas de red va a recibir la IP pública y la otra va a ir conectada al router o switch de la red privada.

Figura No.28: Configuración de Red



En la configuración del dispositivo ethernet se puede asignar dirección IP, máscara de subred y dirección de puerta de enlace dependiendo de las necesidades y configuración (figura No. 27). Si está misma configuración se desea hacer manualmente se edita el archivo respectivo (figura No. 28).

Figura No.29: Configurar dispositivo ethernet

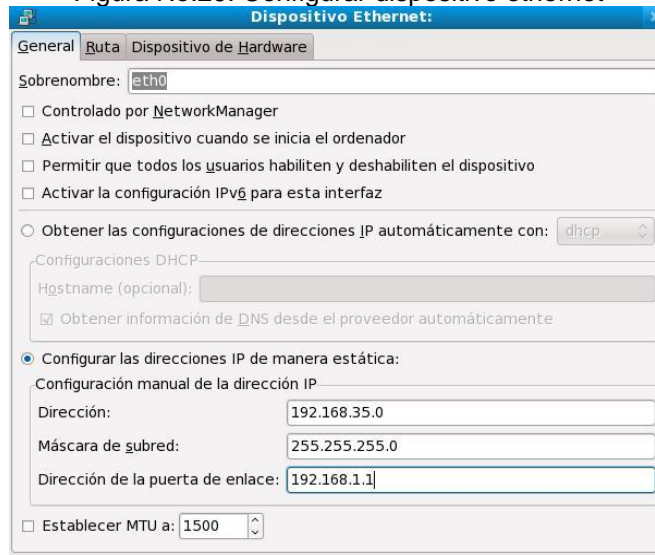
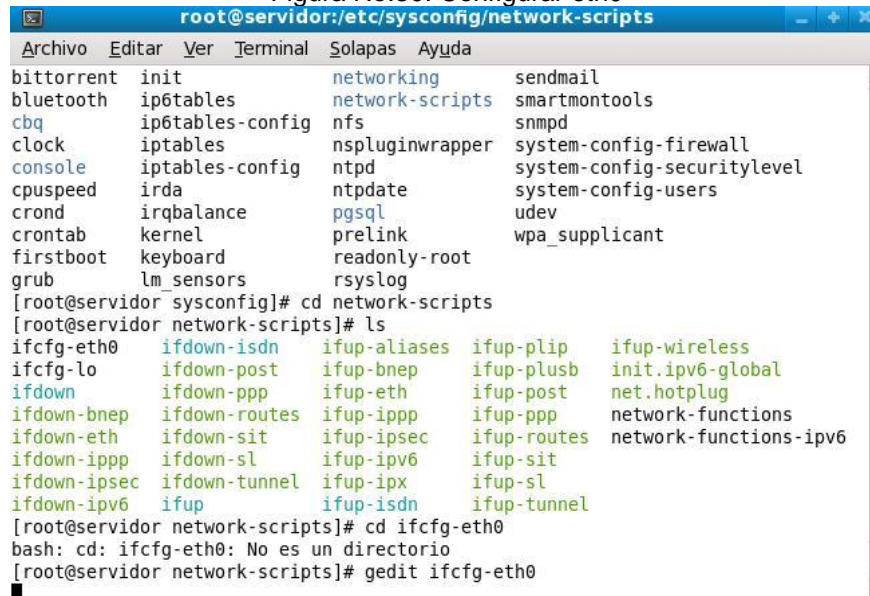



Figura No.30: Configurar eth0



En el archivo de configuración manual de ethernet se pueden configurar todas las opciones que se tienen por el modo gráfico, se modifican los datos necesarios y se guarda (figura No. 29).

Figura No.31: Archivo network-scripts



The image shows a screenshot of a gedit editor window titled '\*ifcfg-eth0 (/etc/sysconfig/network-scripts) - gedit'. The window contains the following configuration text:

```
# Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
DEVICE=eth0
HWADDR=00:0c:29:cc:1:09
ONBOOT=no
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.35.1
USERCTL=no
PEERDNS=yes
IPV6INIT=no
NM_CONTROLLED=no
GATEWAY=192.168.1.1
TYPE=Ethernet
```

### 3 INSTALACION SERVIDOR

#### 3.1 UTILITARIO WEBMIN

Webmin es un utilitario vía web con el cual se puede realizar la configuración de diferentes servicios como Apache, Samba, Configuración de red entre otros, de una forma más sencilla en cuanto a labores de administración y operación se trata. Webmin no viene incluido dentro de ningún instalador Linux por lo cual el paquete se debe instalar de forma individual. Primero se debe comprobar que webmin no ha sido instalado con anterioridad, y si es así se revisa la versión instalada para actualizarla.

#### 3.2 COMPROBACIÓN DE INSTALACIÓN WEBMIN

El comando “whereis” permite averiguar si una aplicación software se encuentra instalado. La figura 30 muestra la respuesta obtenida en caso de que webmin no se encuentre instalado, en este caso solo aparece el nombre del programa seguido de dos puntos y no aparece la dirección de instalación.

Figura No.32: Comando whereis



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# whereis webmin  
webmin:  
[root@localhost /]#
```

### 3.2.1 Descomprimir Paquete.

Se descarga el instalador de la página [www.webmin.com](http://www.webmin.com) y se descomprime como se muestra en el siguiente figura.

Figura No.33: Descomprimir archivo .tar



### 3.2.2 Instalación Webmin.

El proceso de instalación de webmin consta de algunas configuraciones como selección de usuario, contraseña, puerto entre otras las cuales se configuran de la siguiente manera:

```
[root@servidor webmin-1.470]# ./setup.sh
*****
* Welcome to the Webmin setup script, version 1.470
*****
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.
Installing Webmin in /opt/webmin-1.470...
*****
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.
Config file directory [/etc/webmin]:
Log file directory [/var/webmin]:
```

```

Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.
Full path to perl (default /usr/bin/perl):
Testing Perl ...
Perl seems to be installed ok
*****

Operating system name: Redhat Linux
Operating system version: Fedora 10
*****

Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
- What port to run the web server on. There must not be another
web server already using this port.
- The login name required to access the web server.
- The password required to access the web server.
- If the webserver should use SSL (if your system supports it).
- Whether to start webmin at boot time.
Web server port (default 10000):
Login name (default admin):
Login password:
Password again:
The Perl SSLLeay library is not installed. SSL not available.
Start Webmin at boot time (y/n): y
*****

Creating web server config files..
..done
Creating access control file..
..done
Inserting path to perl into scripts..
..done
Creating start and stop scripts..
..done
Copying config files..
..done
Configuring Webmin to start at boot time..
Created init script /etc/rc.d/init.d/webmin
..done
Creating uninstall script /etc/webmin/uninstall.sh ..
..done
Changing ownership and permissions ..

```

```
..done
Running postinstall scripts ..
..done

Attempting to start Webmin mini web server..
Starting Webmin server in /opt/webmin-1.470
..done
*****
Webmin has been installed and started successfully. Use your web
browser to go to
http://servidor:10000/
and login with the name and password you entered previously.
```

### 3.2.3 Iniciando Webmin.

Para probar que webmin se instaló correctamente se procede a abrir una página del explorador web y a continuación se digita la ruta del equipo y el puerto, lo cual mostrará un cuadro para ingresar el nombre de usuario y la contraseña seleccionados durante la instalación.

Figura No.34: Preba Webmin



## a) Configuración de tema Webmin

Lo primero que se puede modificar es el idioma y el tema, y de esta manera tener una configuración más amigable y sencilla.

Figura No.35: Configuración de tema Webmin

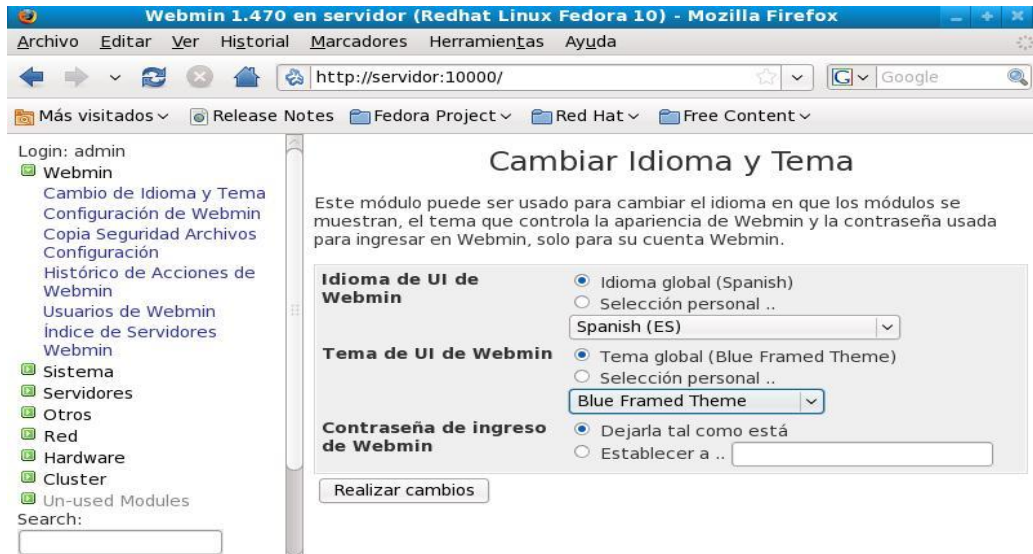


Figura No.36: Webmin con tema amigable



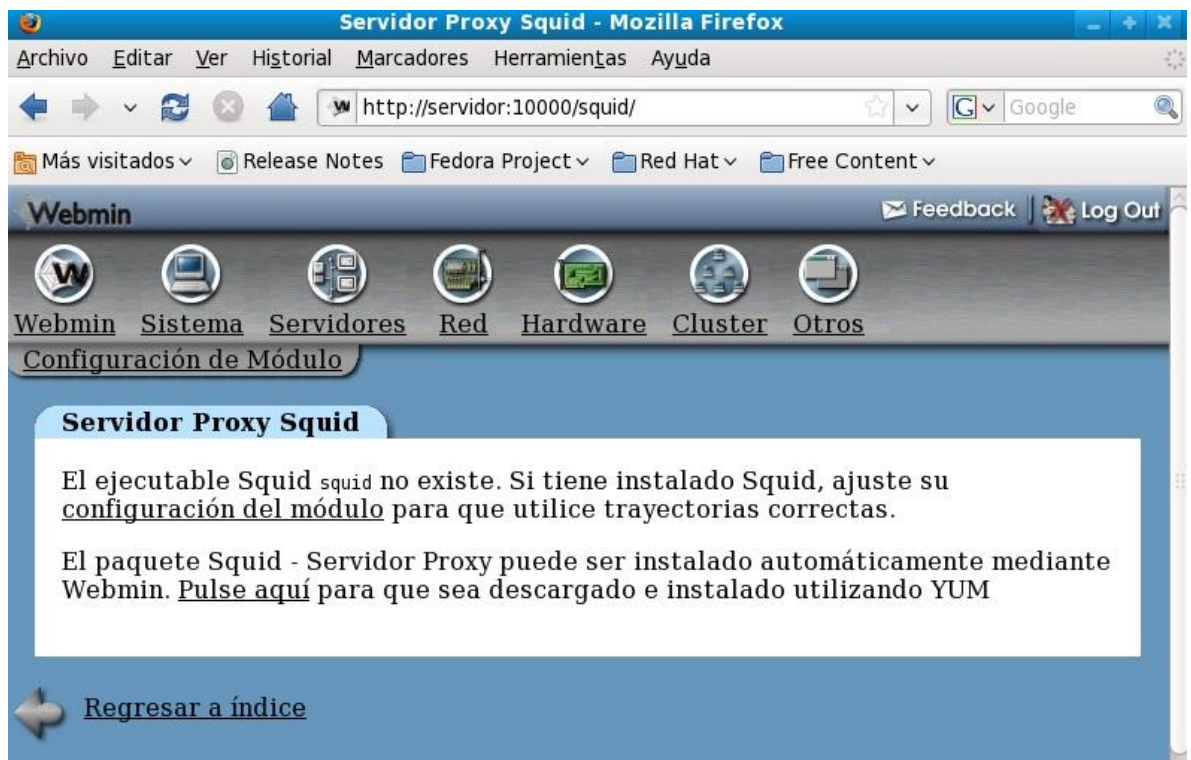
### 3.3 INSTALACION SQUID

#### 3.3.1 Instalación servidor proxy Squid.

La instalación del servidor proxy Squid, se puede realizar en un entorno gráfico y sencillo mediante Webmin.

Ingresando en la pestaña servidores y a continuación en el icono SQUID, el cual se muestra en la imagen de la figura No. 35 desde la cual se realiza la correspondiente instalación. Usando la opción 'Pulse aquí' se inicia la descarga del servidor proxy y posteriormente su instalación.

Figura No.37: Descarga del Servidor Squid



En la figura No. 36 se instala el Servidor Proxy Squid mediante Yum, el cual es un programa automático para instalar o desinstalar los RPM del sistema. Obtiene automáticamente dependencias y previene que ha de ocurrir para instalar correctamente los paquetes. Hace más fácil mantener grupos de máquinas sin tener que poner al día manualmente cada RPM que usan. Al final de la figura No. 36 se puede observar que fue instalado con éxito.

Figura No.38: Instalación de Squid

```

Instalar Paquete

Instalando paquete(s) con el comando yum -y install squid ..

Loaded plugins: refresh-packagekit
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package squid.i386 7:3.0.STABLE15-2.fc10 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package      Arch      Version                Repository      Size
=====
Installing:
squid        i386      7:3.0.STABLE15-2.fc10 updates         1.6 M

Transaction Summary
=====
Install     1 Package(s)
Update     0 Package(s)
Remove     0 Package(s)

Total download size: 1.6 M
Downloading Packages:
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 4ebfc273
Importing GPG key 0x4EBFC273 "Fedora (10) <fedora@fedoraproject.org>" from /etc/pki/rpm-gpg/RPM-GPG-KEY-f
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : squid                                     1/1

Installed:
  squid.i386 7:3.0.STABLE15-2.fc10

Complete!

.. instalación completa.

) Regresar a Servidor Proxy Squid

```

### 3.3.2 Inicialización de squid.

Al ir al menú del servidor Proxy Squid (figura No. 37) se observa que el servidor no se encuentra inicializado, se puede inicializar por modo gráfico oprimiendo en el botón ‘inicializar caché’ o por modo consola con los comandos.

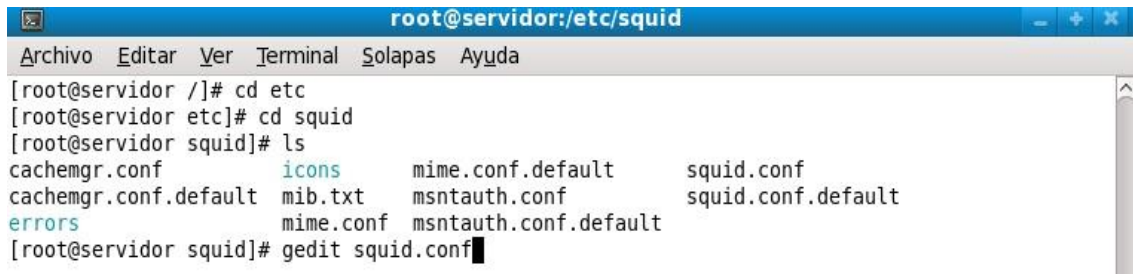
✚ Service squid start, Service squid stop y Service squid restart.

Figura No.39: Inicializar Squid



Se edita el archivo de configuración de Squid ‘squid.conf’ para editar las ACL y demás configuraciones necesarias para el servidor como se observa en la figura No. 38, esto se realiza usando el comando ‘gedit’ el cual es un completo editor de textos libre que se distribuye junto al gestor de escritorio GNOME para sistemas tipo Unix. Este editor se caracteriza principalmente por su facilidad de uso, conseguida en gran parte gracias a una interfaz gráfica clara y limpia, mostrando únicamente las funcionalidades principales que suelen requerir la mayoría de usuarios.

Figura No.40: Comando gedit

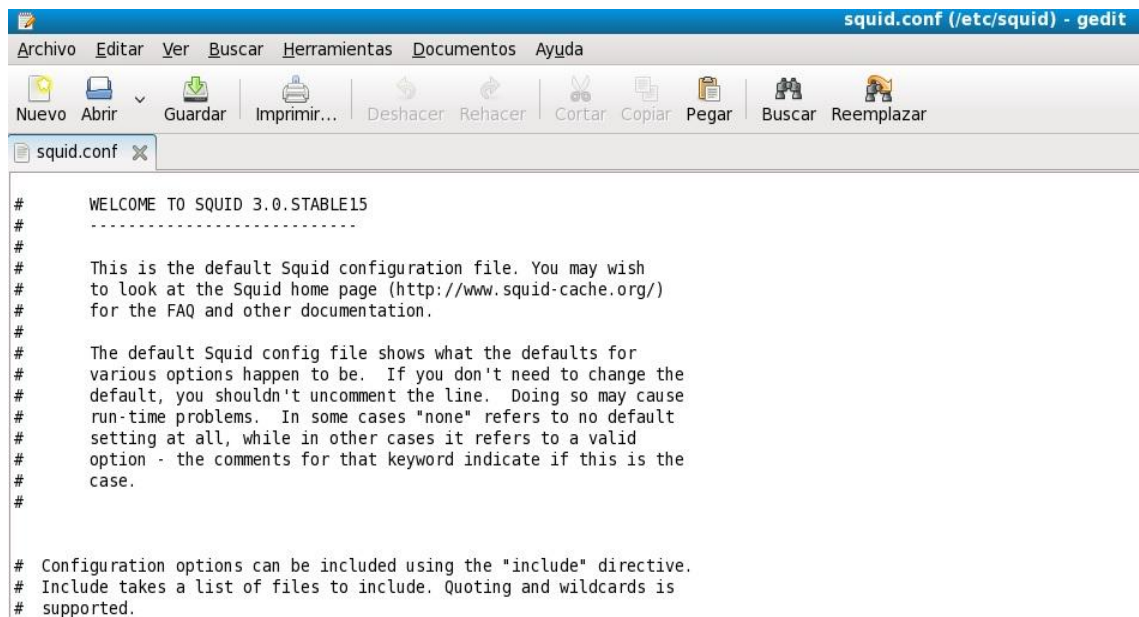


```
root@servidor:/etc/squid
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@servidor /]# cd etc
[root@servidor etc]# cd squid
[root@servidor squid]# ls
cachemgr.conf      icons      mime.conf.default  squid.conf
cachemgr.conf.default  mib.txt  msntauth.conf      squid.conf.default
errors            mime.conf  msntauth.conf.default
[root@servidor squid]# gedit squid.conf
```

Después de ejecutar el comando gedit aparece una ventana con toda la información correspondiente al archivo squid.conf (Figura No.39) ,donde se puede modificar ,agregar o eliminar cualquier parte de la configuración según sea necesario .

Además el gedit tiene opciones como mostrar el número de líneas, aumentar el tamaño de la letra, cambiar el esquema de color, realizar búsquedas rápidas en el archivo, imprimir y muchas opciones que nos facilitan la edición.

Figura No.41: Editar Squid.conf



```
squid.conf (/etc/squid) - gedit
Archivo  Editar  Ver  Buscar  Herramientas  Documentos  Ayuda
Nuevo  Abrir  Guardar  Imprimir...  Deshacer  Rehacer  Cortar  Copiar  Pegar  Buscar  Reemplazar
squid.conf x
#      WELCOME TO SQUID 3.0.STABLE15
#      -----
#
#      This is the default Squid configuration file. You may wish
#      to look at the Squid home page (http://www.squid-cache.org/)
#      for the FAQ and other documentation.
#
#      The default Squid config file shows what the defaults for
#      various options happen to be.  If you don't need to change the
#      default, you shouldn't uncomment the line.  Doing so may cause
#      run-time problems.  In some cases "none" refers to no default
#      setting at all, while in other cases it refers to a valid
#      option - the comments for that keyword indicate if this is the
#      case.
#
# Configuration options can be included using the "include" directive.
# Include takes a list of files to include. Quoting and wildcards is
# supported.
```


## 4 INSTALACION Y CONFIGURACION SQUID FAMILIAS EN ACCION

### 4.1 EDICION SQUID.CONF SERVIDOR FAMILIAS EN ACCION

Las ACL como se explicaba en el capítulo 1.4 son las listas de control de acceso con las cuales se permite un control de tráfico en la red a través de los enrutadores.


Figura No.42: Editar ACL

```
#      # use REQUIRED to accept any non-null user name.
#
#Examples:
#acl macaddress arp 09:00:2b:23:45:67
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Recommended minimum configuration:
acl all src
acl manager proto cache_object
acl localhost src 192.168.35.0/255.255.255.0
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#-----MIS ACL-----
```

 `acl manager proto cache_object8`

El campo "proto" de la primera línea se refiere que la ACL bloquea un protocolo específico, en este caso el protocolo "cache\_object". Puede utilizarse también otro protocolo como "HTTP" o "FTP". En concreto, se trata de un protocolo propio de squid. Este protocolo retorna información acerca de cómo está configurada la cache, o cómo se está ejecutando. Está dentro de la sección "http\_access" ya que se trata de una petición HTTP a squid, pero en lugar de conectar a un servidor remoto es squid quien gestiona la información.

El ejemplo anterior indica: si squid recibe una petición intentando utilizar el protocolo "cache\_object" (definido en el ACL manager), debe denegarla a no ser que provenga de localhost. De este modo, un programa que este ejecutándose en el servidor de caché puede obtener información del estado interno de squid pero no una máquina del exterior. Recuerde que el carácter "!" significa NO, por lo que se está diciendo "denegar manager NO localhost".

 `acl localhost src 192.168.35.0/255.255.255.0`

Se define el localhost el cual es el servidor propio para más adelante darle reglas que permitan únicamente el acceso a squid desde el servidor.

 `Acl to_localhost dst 127.0.0.0/8`

---

<sup>8</sup> UNIVERSIDAD DISTRITAL Arincon Proxy [en línea].  
< <http://www.udistrital.edu.co/comunidad/estudiantes/arincon/proxy.php> > [citado en 27 de junio de 2009]

Se crean las ACL de todos los puertos (Figura No.42), para más adelante asignarle reglas dependiendo de las necesidades de la red. Se crearon las ACL de los puertos SSL, http, https, gopher, wais, http-mgmt, gss-http, filemaker, multiling y los puertos comprendidos entre los valores 1025 al 65535.

Después de haber creado las ACL generales, se procede a crear las ACL específicas, correspondientes a listas de direcciones físicas, páginas web, Mac, puertos etc. y todas aquellas listas que sea necesario bloquear o desbloquear (Figura No.43).

Figura No.43: Editar Mis ACL

```
#-----MIS ACL-----  
acl ivan arp "/etc/squid/listas/ivan"  
#acl permitidos src "/etc/squid/listas/permitidos"  
acl negados url_regex -i "/etc/squid/listas/negados"  
acl inocentes url_regex -i "/etc/squid/listas/inocentes"  
#acl simee arp "/etc/squid/listas/simee"  
#acl dllmsn url_regex -i "/etc/squid/listas/dllmsn"  
#acl mee url_regex -i "/etc/squid/listas/mee"  
#acl msn-dirs url_regex "/etc/squid/listas/msn-dirs"  
#acl msn port 6891-6901  
#acl msn-app req_mime_type ^application/x-msn-messenger$  
#acl msn-gat url_regex gateway.dll?  
acl mac arp "/etc/squid/listas/mac"  
#-----
```

#### a) ACL ivan

Se crea esta lista con las direcciones MAC de los equipos del administrador de la red y el encargado de la coordinación del programa Familias en Acción, los cuales van a tener prioridades especiales (Figura No.42).

Figura No.44: ACL IVAN

```
00:21:97:8D:C1:E9#ivan  
00:21:97:8D:DA:4C#sergio
```

## b) ACL negados

En la ACL negados se encuentran todas las direcciones web o palabras que se desea estén deshabilitadas para los funcionarios que trabajan en el programa, en esta lista se pueden agregar todas las páginas o palabras que se considere necesario como facebook, hi5, ebuddy, rcn, caracol etc. (Figura No.43).

Figura No.45: ACL NEGADOS

```
www.iloveim.com
www.radiusim.com
www.20minutos.es/rss
www.fotos.org
www.ziza.es
media.rcn.com.co
AdiumX
www.micosta.com
www.gennio.com
adoosimg
trillian
dundoo
jsonrpc
wind.exe
www.knightfight.es/?ac=vid&vid=66130560
world6.monstersgame.es/?ac=vid&vid=166045640
ajaxim
latinowebs
adoosimg
eldesparche
www.michiquimula.com
www.micholita.com
hi5
metroflog
x-zip-com
ui.skype.com/ui/0/3.6.0.248/es/installed?
skype.4publishers.com:443
ADSAdClient31.dll
webim
messidog.live.com
shttp.msg.yahoo.com/notify
download.yimg.com/yca/msg/dl/msgr8/es/ymsgr810_421_es.exe
installerstats.yahoo.com/appusage.asp
```

### c) ACL inocentes

La ACL inocentes contiene todas las direcciones y palabras que pueden ser accesadas vía web. En nuestro caso son direcciones de entes gubernamentales, direcciones del programa Familias en Acción y palabras referentes al trabajo del programa.

Figura No.46: ACL INOCENTES

```
190.27.199.5:8083/tipificadoras
69.147.103.179
nxt.legis.com.co/NXT/gateway.dll?
vinculo
209.191.106.128
.fmx
.gov
131.110.1.1
131.110.1.1:8070
131.110.1.10
190.25.231.242
anon
articulo
bmanga
bucaramanga
bucaramanga.gov.co
bumanga
bumanga.gov.co
cgibin
circular
circulo
colombianos
colombianostrabajando
computa
computacion
computador
computadora
cromos
```

#### d) ACL MAC

En la ACL MAC se encuentran las direcciones MAC de los equipos de todos los funcionarios del programa Familias en Acción, es decir todas las estaciones de trabajo de la red.

Figura No.47: ACL MAC

```
00:21:97:8b:81:c7#alejandra
00:1D:92:F4:A6:D6#mantonia
00:1E:0B:3D:C9:EF#carolina
00:21:97:8D:DA:4C#drsergio
00:1E:0B:3D:CA:AE#pilar
00:1D:92:F4:C3:EF#yuri
00:21:97:8D:F5:AF#leidy
00:1f:29:34:02:8a#edna
00:21:97:8b:80:83#marcela
00:21:97:8D:DD:B9#lorena
00:1D:92:F4:C3:EA#marthaandra
00:1C:10:89:06:4C#routerdlink
00:1C:C0:81:41:EF#juntos1
00:1C:C0:81:41:33#juntos2
00:1E:0B:3D:C7:EB#coorjuntos
00:1D:92:F4:C7:62#nubia
00:21:97:8D:EA:B6#johana
00:21:97:8D:C1:EC#wiilliam
00:1C:25:0F:00:B4#lorena2
```

## 4.2 CONFIGURACION DE LOS ERRORES DE SQUID

En el proxy Squid, se puede configurar el mensaje de error que se despliega en el momento en el que el funcionario intenta acceder a una página que no está permitida por las políticas de la Alcaldía de Bucaramanga.

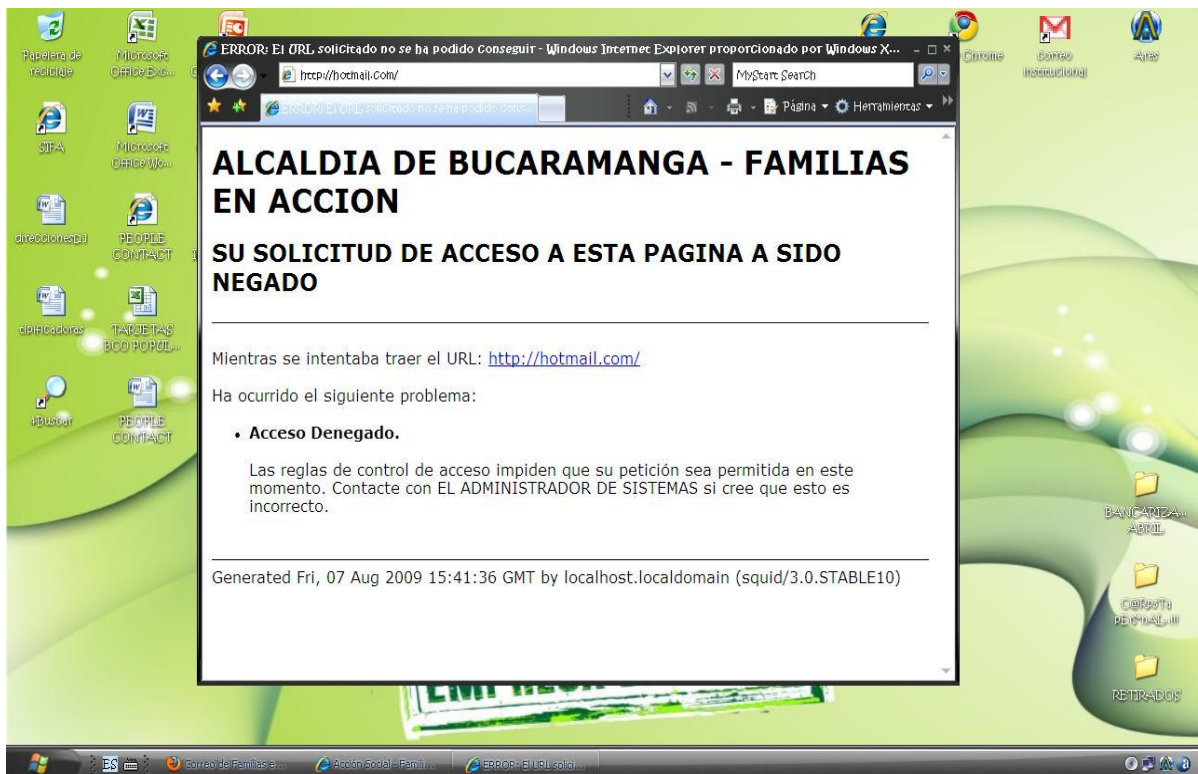
El archivo que se modifica es el ERR\_ACCESS\_DENIED el cual se edita con un editor de texto, en este caso se editó con gedit el cual es un editor de texto muy completo y de fácil manejo (figura No. 40).

Figura No.48: Editar ERR\_ACCESS\_DENIED

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html;
charset=iso-8859-1">
<TITLE>ERROR: El URL solicitado no se ha podido conseguir</TITLE>
<STYLE type="text/css"><!--BODY{background-color:#ffffff;font-
family:verdana,sans-serif}PRE{font-family:sans-serif}--></STYLE>
</HEAD><BODY>
<H1>ALCALDIA DE BUCARAMANGA - FAMILIAS EN ACCION</H1>
<H2>SU SOLICITUD DE ACCESO A ESTA PAGINA A SIDO NEGADO</H2>
<HR noshade size="1px">
<P>
Mientras se intentaba traer el URL:
<A HREF="%U"%>%U</A>
<P>
Ha ocurrido el siguiente problema:
<UL>
<LI>
<STRONG>
Acceso Denegado.
</STRONG>
<P>
Las reglas de control de acceso impiden que su petici&oacute;n
sea
permitida en este momento. Contacte con EL ADMINISTRADOR DE
SISTEMAS
si cree que esto es incorrecto.
</P>
</UL>
```

Después de realizar los respectivos cambios como nombre, fuentes y estilos dependiendo de las necesidades y guardar el archivo se procede a intentar entrar a una página bloqueada para sus respectivas pruebas.

Figura No.49: Prueba pagina bloqueada



## 5 GESTION DE LA RED DE DATOS FAMILIAS EN ACCION

La gestión de una red de datos es de gran importancia para cualquier red ya sea pequeña, mediana o grande, al tratarse del máximo aprovechamiento de la misma y de sus recursos. Se realizó la gestión de la red del programa Presidencial Familias en Acción con el fin de tener un control de todos los equipos, teniendo de esta manera un mapa completo con direcciones IP y MAC por medio del software SolarWinds<sup>9</sup> el cual es uno de los software más completos y confiables que existen hasta el momento a nivel de gestión de redes de datos. Con este paquete se puede monitorear la red en todo momento y a su vez crear diferentes alertas dependiendo de las necesidades, además se puede tener un completo manejo de los dispositivos Cisco y todos aquellos dispositivos que soporten el protocolo simple de administración de red (SNMP)

En el caso de la red de Familias en Acción no se cuenta con un switch que soporte SNMP por lo cual no es posible hacer el estudio de sus puertos para no tener la necesidad de ir hasta el rack, pero sí se puede obtener información relacionada con los equipos de cómputo.

---

<sup>9</sup> SOLARWINDS                      toolsets                      engineer  
< <http://www.solarwinds.com/products/toolsets/engineer.aspx>>

[en línea].  
[citado en 03 de julio de 2009]

## 5.1 SELECCIÓN HERRAMIENTAS DE GESTION





La selección de herramientas de gestión a emplear inicia con una revisión de las herramientas disponibles en el mercado.

Figura No.50: Cuadro comparativo software de gestión

Característica	CISCOWORKS	HP OPENVIEW	SOLARWINDS
<b>NIVEL DE COMPLEJIDAD</b>	ALTO	MEDIO ALTO	MEDIO
<b>ELABORACIÓN DE MAPA DE RED DE FORMA GRÁFICA</b>	SI	SI	SI
<b>PLATAFORMAS SOPORTADAS</b>	Microsoft Windows Vista, XP sp2, Server 2008, Server 2003 sp1 and r2, y Server 2000 sp4	Windows Server 2008, Vista, Windows Server 2003, Windows XP, Windows 2000	Windows XP, Windows 2000 Professional, Windows Vista y Windows Server 2003 y 2008
<b>COMPATIBILIDAD CON OTROS DISPOSITIVOS</b>	NO	SI	SI
<b>ENTORNO AMIGABLE</b>	MEDIO	MEDIO	ALTO
<b>TAMAÑO DE RED IDEAL SOPORTADA</b>	MUY GRANDES	GRANDES	MEDIANAS
<b>REPORTE DE ALARMAS</b>	SI	SI	SI
<b>COSTO EN PESOS</b>	21.145.000	20.000.000	2.500.000

A partir de esta primera inspección y teniendo como criterios de selección, el contar con versiones libres o demo, una interfaz de usuario amigable y el volumen de dispositivos soportados se hizo una preselección de tres de las más populares: CiscoWorks, HP Openview y Solarwinds Tools for Engineers. Con base en esta preselección y teniendo en cuenta los requerimientos del proyecto se realizó una comparación (figura No. 50).

Se seleccionó la herramienta solarwinds por varias criterios importantes como son:

-  Precio
-  Tamaño de red ideal soportado
-  Nivel de complejidad
-  Entorno amigable

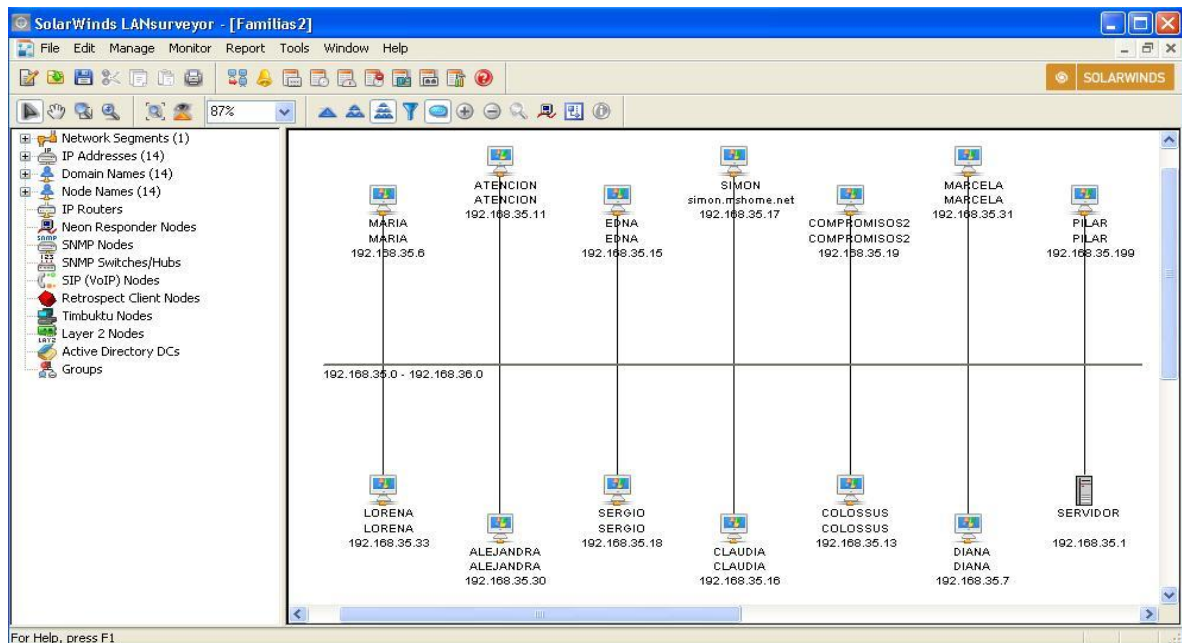
El software de gestión solarwinds cuenta con una versión demo, la cual ofrece las facilidades necesarias y un buen desempeño de la red.

Es ideal para gestionar redes pequeñas y medianas como es el caso de nuestra red de Familias en Acción, la cual es una red de trece computadores mas el servidor; además por su entorno amigable, nivel de complejidad y costos, se acomoda eficazmente a las necesidades requeridas.

## 5.2 MAPA DE LA RED FAMILIAS EN ACCION

Para obtener el diseño de la red, se utilizó el software SolarWinds LANsurveyor<sup>10</sup> el cual tiene utilidades para generar el mapa automático de toda la red incluyendo dispositivos del modelo OSI capa 2 y capa 3 como router y switch, además de mostrar el nombre del equipo con su respectiva dirección IP. La red cuenta con 13 equipos de cómputo y 1 servidor, así como un rack con un router Linksys-Cisco y un Switch D-LINK (Figura No. 42).

Figura No.51: Mapa de la red familias en Acción



<sup>10</sup> SOLARWINDS products lansurveyor  
< <http://www.solarwinds.com/products/lansurveyor/>>

[en línea].  
[citado en 03 de julio de 2009]

El software SolarWinds LANsurveyor cuenta además con opciones para generar alarmas en los días y las horas que se desee, inclusive se puede hacer que lleguen a al correo electrónico de quien sea necesario o que se active un sonido. Se puede apagar un equipo, reiniciarlo, iniciar una sesión de Telnet, enviar mensajes, iniciar un escritorio remoto para cuestiones de mantenimiento o solución a problemas sin tener la necesidad de ir hasta donde se encuentra el equipo.

### 5.3 LISTA DE DIRECCIONES MAC

Es importante tener a la mano la lista de direcciones MAC de todos los equipos para su correspondiente configuración en Squid y tener la opción de bloquear o habilitar recursos para cada uno. Para obtener estas direcciones se emplea una herramienta de descubrimiento remoto contenida en el paquete SolarWinds Engineer's toolset, denominada MAC Address Discovery el cual realiza la búsqueda de las direcciones MAC de todos los equipos dentro del segmento de red con su respectivo nombre y dirección IP (Figura No. 43).

Figura No.52: MAC Address Discovery

IP Address	MAC Address	DNS	Network Card Manufacturer
192.168.35.1	0019.21FA.6FD9		
192.168.35.6	001D.92F4.A6D6	MARIA	
192.168.35.7	001E.0B3D.C9EF	DIANA	
192.168.35.11	001D.92F4.C762	ATENCION	
192.168.35.13	0021.978D.F5AF	COLOSSUS	
192.168.35.15	001F.2934.028A	EDNA	
192.168.35.16	0021.978D.C1EC	CLAUDIA	
192.168.35.17	0021.978D.DA4C	simon.mshome.net	
192.168.35.19	001D.92F4.C3EA	COMPROMISOS2	
192.168.35.30	0021.978B.81C7	ALEJANDRA	
192.168.35.31	0021.978B.8083	MARCELA	
192.168.35.33	0021.978D.DDB9	LORENA	
192.168.35.60	001C.250F.00B4		
192.168.35.199	001E.0B3D.CAAE	PILAR	
192.168.35.250	001C.1089.064C		

## 5.4 ESCANEO DE PUERTOS

Cuando se realiza la configuración del Proxy Squid se seleccionan los puertos que se quiere habilitar y bloquear, para realizar la confirmación de que dicha configuración funciona de una manera adecuada se verifica que puertos están activos a través del software Port Scanner, el cual se encarga de revisar cuales puertos de cada equipo de cómputo se encuentran habilitados y cuáles no (Figura No. 44).

Figura No.53. Port Scanner

IP Address	DNS Lookup	9 discard	7 echo	23 telnet	80 www-http	21 ftp	25 smtp	100 newacct	443 https	993 imaps	8080 http-alt
192.168.35.17	simon.mshome.net						No Reply				
192.168.35.18							Open				
192.168.35.19	COMPROMISOS2										
192.168.35.20											
192.168.35.21											
192.168.35.22											
192.168.35.23											
192.168.35.24											
192.168.35.25							No Reply				
192.168.35.26											
192.168.35.27											
192.168.35.28											
192.168.35.29											
192.168.35.30	ALEJANDRA										
192.168.35.31	MARCELA	No Reply	No Reply	No Reply	No Reply	No Reply	Open	No Reply	No Reply	No Reply	No Reply
192.168.35.32							Open				
192.168.35.33	LORENA										

## 6 PRUEBAS Y RESULTADOS

El mejoramiento de las características del servidor fue una acción necesaria, ya que en un principio el equipo contaba con 1Gb RAM, lo cual fue insuficiente al momento de todos los equipos estar trabajando simultáneamente al proxy Squid manejar la caché de todos, por tal razón fue necesario subir la RAM a 4Gb.

Las primera prueba realizada corresponde a la configuración de las dos tarjetas de red del servidor, por lo cual se procedió a verificar la conexión desde el punto de vista físico, como son, prueba del cable UTP por medio de un probador y posteriormente la revisión del correcto encendido de los Leds de las tarjetas. Por último se procedió a hacer un ping a cada IP asignada a cada tarjeta, luego a la puerta de enlace, DNS y por último se abrió el explorador Mozilla Firefox y se revisó que se tuviera acceso a internet.

La segunda prueba realizada, corresponde a la comprobación de la configuración del router Linksys-Cisco, así como las opciones de seguridad de la red inalámbrica. Se conectó un portátil a la red inalámbrica para comprobar la detección de la red de Familias en Acción y su correspondiente correcta conexión a dicha red, así como la revisión del acceso al protocolo http mediante el explorador Internet Explorer.

La tercera prueba fue la comunicación del Servidor con el Router y el Switch, para ello se conectó a uno de los puertos del switch un computador

destinado a un funcionario para probar el acceso a los diferentes servicios habilitados en la configuración.

Se realizaron las pruebas de la configuración del Proxy Squid, y para ello se intentó ingresar desde un computador asignado a un funcionario, a una página de Internet no autorizada para confirmar su correcta ejecución, lo cual resultó acorde a las configuraciones hechas con anterioridad.

Las últimas pruebas que se realizaron fueron las relacionadas con la gestión de la red, por lo tanto se utilizó el paquete de gestión SolarWinds para probar puertos habilitados, vulnerabilidades y rendimiento general de la red. Los programas de SolarWinds utilizados fueron LANsurveyor para generar el mapa de la red, MAC Address discovery para descubrir la lista de las MAC de los equipos, Port Scanner para analizar los puertos habilitados y Ping Sweep para verificar los tiempos de respuesta. Al finalizar las pruebas se obtuvieron resultados apropiados a las configuraciones realizadas.

## **CONCLUSIONES**

La correcta selección de los equipos de cómputo con características acordes a las necesidades de la red es fundamental para el buen desempeño y el buen aprovechamiento de todos los recursos de la misma.

El reconocimiento del hardware y patrones de uso por parte de los usuarios de los recursos de la red, son un punto clave dentro de las actividades de administración de red, ya que de esto dependen las políticas que se adopten, orientadas a mejorar el rendimiento y aprovechamiento de los recursos.

La implementación de un sistema de gestión y administración de red como el desarrollado para el programa Presidencial Familias en Acción, se valora a partir de su flexibilidad para adaptarse a nuevas necesidades.

En el sistema de gestión se puede observar que al tener el programa familias en acción un Call Center con acceso a base de datos vía web y todos los demás equipos de los funcionarios acceso simultaneo al mismo, la conexión a Internet debe ser superior a 1Mbps y las especificaciones de los computadores igual o mayores a un procesador Pentium 4.

En el sistema proxy Squid, se comprobó la eficiencia y estabilidad del mismo y sus ventajas para la fácil administración de usuarios y dispositivos.

El desarrollo del sistema de gestión bajo ambiente Linux es una buena decisión ya que este además de ser compatible con la mayoría de computadores actuales, es un software libre lo cual reduce los costos de implementación.

La gestión de redes de datos es indispensable para el buen rendimiento y el máximo aprovechamiento de los recursos de una red, para esto se debe escoger el software específico e idóneo para su administración, así como el manejo debe estar a cargo de una persona profesional y capacitada para tales funciones.

SolarWinds es el software de gestión ideal para gestionar redes medianas y pequeñas, debido a su nivel de complejidad, entorno amigable, compatibilidad con otros dispositivos y costo.

## BIBLIOGRAFIA

GESTION EN REDES DE COMPUTADORES. Cohorte IX, Ciclo IV. Bucaramanga. Especialización en Telecomunicaciones UIS, 2009. p 3.

< <http://www.calasanz-pereira.edu.co/index.php/Informatica/linux.html>> [citado en 25 de junio de 2009]

✚ Página web de la FUNDACIÓN EDUCATIVA CALASANZ con información de Informática Linux.

< <http://www.rpm.org>> [citado en 15 de julio de 2009]

✚ Pagina web de RPM Package Manager (RPM).

< <http://www.udistrital.edu.co/comunidad/estudiantes/arincon/proxy.php>> [citado en 27 de junio de 2009]

✚ Pagina web de la UNIVERSIDAD DISTRITAL ARINCON con información acerca de Proxy.

< <http://www.geocities.com/hilmarz/cisco/acl.htm>> [citado en 27 de junio de 2009]

✚ Pagina web GEOCITIES con interesante información acerca de ACL.

< <http://dns.bdat.net/documentos/squid/x30.html>> [citado en 29 de junio de 2009]

✚ Pagina web con documentos acerca del Servidor Proxy Squid.

< [http://www.citel.oas.org/newsletter/2007/abril/tcp-ip\\_e.asp](http://www.citel.oas.org/newsletter/2007/abril/tcp-ip_e.asp)> [citado en 30 de junio de 2009]

✚ Pagina web de CITEL COMISION INTEROAMERICANA DE TELECOMUNICACIONES con información acerca de TCP-IP.

< <http://www.solarwinds.com/products/toolsets/engineer.aspx>> [citado en 03 de julio de 2009]

✚ Pagina web del software de gestión y administración de redes SOLARWINDS.