

CONFIGURACIÓN DE SERVICIOS DE RED E INTERNET

Presentado por :

HECTOR GIL TRIANA
Ingeniero de Sistemas UIS
Especialista en sistemas operativos unix y redes
Gerente Sistemas Teleinformáticos y Servicios Ltda
E-mail : hector.gil@sts.com.co

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIA ELECTRICA Y
ELECTRONICA

JULIO DE 2016

INTRODUCCION.....	5
1. SISTEMA OPERATIVO LINUX.....	6
1.1 BREVE RESEÑA HISTORICA.....	6
1.1.1. RED HAT.....	7
1.1.2.SUSE LINUX.....	8
1.1.3. COMPATIBILIDAD DE LOS SISTEMAS OPERATIVOS Y LOS FABRICANTES.....	8
1.1.3.1. COMPATIBILIDAD ENTRE LAS MÁQUINAS IBM Y RED HAT ENTERPRISE.....	9
1.1.3.2. COMPATIBILIDAD ENTRE LAS MÁQUINAS IBM Y SUSE LINUX	9
1.1.3.3. COMPATIBILIDAD ENTRE LAS MÁQUINAS HP Y RED HAT ENTERPRISE Y SUSE.....	10
1.2. NIVELES DE SEGURIDAD.....	11
1.3.INSTALACIÓN Y ARRANQUE.....	12
1.3.1.INSTALACIÓN DE LINUX.....	12
1.3.2.CONFIGURACIÓN DE SERVICIOS DESEADOS EN EL ARRANQUE.....	14
1.3.3. BAJANDO EL SISTEMA.....	15
1.3.3.1. PARA COMPLEMENTAR.....	16
1.4. ALGUNAS TAREAS DE ADMINISTRACIÓN DEL SISTEMA.....	16
1.4.1.MANEJO DE USUARIOS Y GRUPOS.....	16
1.4.1.1. PARA COMPLEMENTAR.....	21
2. REDES CON LINUX.....	22
2.1.CONFIGURACIÓN DE TCP/IP POR COMANDOS Y ARCHIVOS INVOLUCRADOS.....	22
2.2.ALGUNOS COMANDOS TCP/IP.....	23
2.3. ASIGNACIÓN DE INTERFAZ LOGICAS.....	28
2.4. UTILITARIO DE ADMINISTRACIÓN WEBMIN.....	31
2.4.1. CREACIÓN DE USUARIOS WEBMIN.....	35
2.4.2. OPCIONES DEL MENU DE SISTEMA.....	36
2.4.3. OPCIONES DE PESTAÑA DE SERVIDORES.....	40
2.4.4. OPCIONES DE PESTAÑA DE RED.....	40
2.4.5. OPCIONES DE PESTAÑA DE HARDWARE.....	42
2.4.6. PARA COMPLEMENTAR.....	42
2.5. USO DE UN SNIFFER.....	43
2.5.1. NETXRAY EN WINDOWS.....	43
2.5.2. ETHEREAL EN LINUX.....	44
2.5.3. PARA COMPLEMENTAR.....	46
3.CONFIGURACION DE SERVICIOS DE INTERNET EN LINUX.....	47
3.1. QUE ES INTERNET.....	47
3.2. COMO FUNCIONAN LOS DIFERENTES SERVICIOS EN INTERNET.....	47
3.3. DOMAIN NAME SERVICE (SERVIDORES DNS).....	47
3.3.1.CONFIGURACIÓN DEL SERVIDOR DNS.....	51
3.3.2. CONFIGURANDO LA PARTE CLIENTE DEL DNS.....	59
3.3.3. PRUEBAS.....	59
3.3.4. ARCHIVOS INVOLUCRADOS.....	60

3.3.5 TALLER DE CONFIGURACIÓN DE SERVIDOR Y CLIENTES DNS ...	62
3.3.6. PARA COMPLEMENTAR	62
3.4. CONFIGURACIÓN DEL SERVICIO WEB (WWW).....	62
3.4.1. CONCEPTOS BÁSICOS DEL WEB	62
3.4.2. CONFIGURACIÓN DEL SERVIDOR WEB APACHE	63
3.4.2.1. POR HERRAMIENTAS PROPIAS DEL SISTEMA.....	63
3.4.2.2. POR MANIPULACIÓN DE LOS ARCHIVOS	66
3.4.3. TALLER DE PUBLICACIÓN DE PAGINAS EN EL SERVIDOR WEB.	67
3.4.4. CONSIDERACIONES DE SEGURIDAD EN EL SERVIDOR APACHE	67
3.4.4.1. PROTEGER CON CONTRASEÑA	67
3.4.4.2. RESTRINGIR EL ACCESO DESDE UNA MÁQUINA	68
3.4.4.3. CONEXIONES SEGURAS (ENCRIPADAS).....	68
3.4.5. TALLER DE SERVIDOR WEB Y ALGUNOS ASPECTOS DE SEGURIDAD	70
3.4.5.1. PARA COMPLEMENTAR	70
3.5. CONFIGURACIÓN DE SERVICIO DE CORREO ELECTRONICO.....	71
3.5.1. CONFIGURACIÓN DE CORREO ELECTRÓNICO BASICO EN LINUX	73
3.5.2. ACTIVAR EL SERVICIO POP3 E IMAP	82
3.5.3. CONTROLES O FILTROS.	84
3.5.4. CREACION DE CUENTAS DE CORREO.	86
3.5.5. MANEJO DE CORREO ENCRIPADO	87
3.5.6. TALLER SERVICIO DE CORREO BASICO	89
3.5.7. CONTROL DE VIRUS Y SPAM	89
3.5.7.1. INSTALACIÓN Y CONFIGURACIÓN DE ANTIVIRUS	93
3.5.7.2. INSTALACIÓN, CONFIGURACIÓN MAILSCANNER E INTEGRACIÓN.....	97
3.5.7.3. PARA COMPLEMENTAR	108
3.5.8. TALLER SERVICIO DE CORREO CON FILTRADO DE VIRUS Y SPAM	108
3.5.9. CONFIGURACION DE INTERFAZ WEB PARA CORREO.....	108
3.5.9.1. CONFIGURACIÓN DE PLUGGIN PARA EL CORREO WEB.....	111
3.5.10. MANEJO DE QUOTAS DE DISCO	121
3.5.10.1. ASIGNACION DE QUOTAS A LOS USUARIOS	122
3.5.10.2. PRUEBAS DEL CONTROL POR QUOTAS	124
3.5.11. PARA COMPLEMENTAR	125
3.6. SERVICIO NFS (NETWORK FILE SYSTEM).....	126
3.6.1. CONFIGURANDO EL SERVIDOR NFS	126
3.6.2. CONFIGURANDO EL CLIENTE.....	129
3.6.3. TALLER DE SERVICIO NFS.....	130
3.7. SERVIDOR PROXY.....	130
3.7.2. MANTENIMIENTO DE LOS LOG DE EVENTOS.....	136
3.7.3. TALLER DE PROXY	136
3.7.3.1. PARA COMPLEMENTAR	137
3.7.4. PROXY TRANSPARENTE.....	137
3.8. SERVICIO DHCP	138
3.8.1. CONFIGURACIÓN DEL SERVIDOR DHCP.....	138
3.8.2. CONFIGURANDO EL CLIENTE.....	140
3.8.3. TALLER DE DHCP	141
3.9. SERVICIO SSH (SHELL SEGURO)	141

3.9.1. TALLER SSH	145
3.10. SERVICIO FTP	145
3.10.1. CONFIGURACIÓN DE FTP SERVER (ACCESO ANONYMOUS)	146
3.10.1. TALLER FTP	147
3.11. MANEJO DE SISTEMAS DE ARCHIVOS ENTRE LINUX Y WINDOWS	147
3.11.1. MONTAJE DE CARPETAS WINDOWS EN LINUX	147
3.11.2. USO DE SAMBA (SERVIDOR DE ARCHIVOS E IMPRESORAS)	148
3.11.3. TALLER CONECTIVIDAD CON WINDOWS	151
3.11.3.1. PARA COMPLEMENTAR	152
4. PROTECCIÓN DE LOS SERVICIOS DE INTERNET Y EL SERVIDOR	153
4.1. USO DE TCPWRAPPER (TCP/IP CONFIABLE)	153
Otro ejemplo:	156
4.2. TALLER CON TCPWRAPPERS	156
4.3. FILTRADO CON IPTABLES	157
4.4. EJERCICIO TEORICO CON IPTABLES	157
5. VIRTUALIZACION	159
5.1. VIRTUALIZACION CON VMWARE	159
5.1.1. INSTALACION DE UNA MAQUINA VIRTUAL Y UN SISTEMA OPERATIVO CON UNA CONFIGURACION POR DEFECTO	167
5.1.2. INSTALACION DE UNA MAQUINA VIRTUAL CON UN SISTEMA OPERATIVO PERSONALIZADO	172
5.1.3. CARGUE DE UN SISTEMA OPERATIVO A PARTIR DE UNA IMAGEN	201
5.2 VIRTUALIZACION CON VIRTUAL BOX	206
5.2.1. COMUNICACION ENTRE WINDOWS Y LINUX	219
5.2.2. CONFIGURACION DE VIRTUALBOX PARA QUE LAS MAQUINAS VIRTUALES SE COMUNIQUEN CON LOS DEMAS EQUIPOS DE LA RED LAN	220

INTRODUCCION

Muchas preguntas surgen cuando se desarrolla un sistema informático, al trabajar conectados hay que tener en cuenta que no todos los usuarios tienen los mismos derechos, hay personas dedicadas al mantenimiento del sistema y otras que sólo intentan obtener algún provecho de él ocasionalmente. Esto deriva sin dudas en la palabra seguridad. En contrapartida, se debe tener en cuenta la flexibilidad, la comodidad que brinda el sistema.

Los sistemas UNIX se caracterizan por combinar de forma armónica estos detalles. Son utilizados actualmente en la mayoría de las organizaciones públicas y privadas que necesiten comunicarse de la mejor manera. UNIX, es probablemente el sistema operativo más versátil y popular que se puede encontrar actualmente. Dentro de esta familia tenemos a LINUX, como el sistema operativo que inicio con el uso libre y que actualmente tiene gran variedad de versiones comerciales, pero que nos permite combinar el potencial de UNIX con productos gratuitos para la implementación de diversos tipos de soluciones. Aunque hay versiones comerciales del sistema operativo, aún existen numerosos productos gratuitos que se pueden configurar sobre este sistema.

Este modulo, ha tenido en cuenta esto , por consiguiente, lo ideal es construir los sistemas informáticos bajo cimientos pensados para la gente y la situación actual de las empresas.

Por las facilidades que ofrece Linux, y de la gran cantidad de herramientas disponibles para este sistema como software libre, nos centraremos en él y la mayor parte de las actividades y talleres las realizaremos sobre esta plataforma. También incluiremos una sección para tratar Windows XP.

Se pretende esclarecer conceptos, y dar una bases sólidas para trabajar con el ambiente LINUX, y utilizar este sistema para la implementación de sistemas informáticos que aprovechen las ventajas de comunicación de Internet. Se implementarán los talleres necesarios para entender la instalación, configuración de servicios de internet en estas plataformas, reforzando los conocimientos básicos en este sistema operativo.

Algunas partes del material entregado en el seminario, son extraídos de internet y se realizarán las citas pertinentes en los pie de página y en la bibliografía al final del mismo. Otra parte, junto con los talleres propuestos son autoría del conferencista.

Para facilitar la comprensión de Linux, se recomienda revisar un material previo, llamado modulo-linux.doc que hace una inducción.

1. SISTEMA OPERATIVO LINUX¹

1.1 BREVE RESEÑA HISTORICA

Linux es una implementación del sistema operativo UNIX (uno más de entre los numerosos clónicos del histórico Unix), pero con la originalidad de ser gratuito y a la vez muy potente, que sale muy bien parado (no pocas veces victorioso) al compararlo con las versiones comerciales para sistemas de mayor envergadura y por tanto teóricamente superiores.

Comenzó como proyecto personal del entonces estudiante Linux Torvalds, quien tomó como punto de partida otro viejo conocido, el Minix de Andy. S. Tanenbaum (profesor de sistemas operativos que creó su propio sistema operativo Unix en PCs XT para usarlo en su docencia). Actualmente Linux lo sigue desarrollando, pero a estas alturas el principal autor es la red Internet, desde donde una gigantesca familia de programadores y usuarios aportan diariamente su tiempo aumentando sus prestaciones y dando información y soporte técnico mútuo. La versión original y aun predominante comenzó para PCs compatibles (Intel 386 y superiores), existiendo también en desarrollo versiones para prácticamente todo tipo de plataformas: PowerPC, Sparc, Alpha, Mips, etc.

¿Cómo conseguirlo?

Hace unos años, la primera fuente para conseguir el sistema Linux era Internet, pues las versiones eran free (libres). Actualmente allí es donde están siempre las últimas versiones y las aplicaciones más actualizadas pero existen varias versiones comerciales y se pueden obtener los medios magnéticos con los fabricantes. El corazón del sistema es el mismo, aunque pueden tener externamente presentaciones y formas distintas de instalación.

Una ventaja (para muchos usuarios termina siendo un inconveniente) es la gran rapidez con la que se desarrolla Linux. Constantemente llegan a los principales servidores Linux en la red actualizaciones del núcleo del sistema, de aplicaciones, utilidades, manuales y documentación, etc. Es bueno estar al día, seguir con atención su evolución y aprovechar las mejoras que se incorporen, pero en la mayoría de los casos no vale la pena estar reinstalando software por el simple hecho de ser una nueva versión, sino que hay que ser un poco selectivos, al menos con el software. En el caso de los manuales, HowTo's, grupos de noticias y/o listas de correo sí que vale la pena estar "a la última", sobre todo porque es allí donde nos sacarán de apuros cuando agotemos nuestros propios recursos...

¿Dónde están los manuales?

Como ocurre en todas las versiones de Unix, el primer sitio donde mirar cuando tenga una duda concreta sobre tal comando, fichero de configuración, etc. es la orden 'man', que incluye la ayuda de referencia de Unix. Pero sólo es útil en ese ámbito, cuando ya se sabe más o menos lo que busca, y sólo se necesita aclarar dudas concretas. Para todo lo demás la mejor fuente de información es, cómo no, la propia red. En ella están disponibles tanto libros completos (de los que algunas editoriales especializadas han publicado versiones en papel) como la colección "Linux HOWTO", de la que este documento forma parte. Hay una HOWTO para prácticamente cualquier tema. Su objetivo es cubrir, mediante manuales breves, concisos y específicos, cualquier duda que pueda surgir. Se actualizan permanentemente, y se distribuyen a través del denominado "Linux Documentation Project" (LDP) en Internet. La misma información se publica en muy diferentes formatos, orientados tanto a la búsqueda y consulta en línea como a su lectura convencional. Todas las versiones de Linux incluyen estos manuales (al menos la última edición disponible en el momento de recopilar el CDROM correspondiente).

Distribuciones

El único elemento común a todas las versiones Linux es su kernel el núcleo del sistema operativo, que se desarrolla de forma coordinada y con actualizaciones sistemáticas. Sin

¹ Tomado de Artículo Spanish Linux Howto

embargo todo sistema operativo necesita, junto al núcleo del sistema, todo un conjunto de utilidades y herramientas de instalación, configuración y uso. Ahí juegan su papel las diferentes distribuciones: algunos particulares, entidades y empresas se dedican a hacer determinadas recopilaciones de software que ellos mismos preparan para que sean fácilmente instalables y configurables. Todas ellas facilitan el software junto a su código fuente, pero la flexible licencia GNU a la que se acojen permite tanto ofrecerlas gratuitamente como distribuir las por canales comerciales (lo que se paga es el trabajo de recopilación, el software de cosecha propia que pueda aportar, una presentación más elaborada, gastos de distribución y soporte técnico al usuario).

Por ejemplo, para las versiones de Linux como RedHat 9, Suse 8, RedHat enterprise, y otras el kernel era 2.4.X.

Para versiones actuales de los sistemas linux, el kernel es 2.6.X.

Algunas de las distribuciones más conocidas son:

1.1.1. RED HAT

Creada por Red Hat Software, en Connecticut, EE.UU. Una de sus ventajas es el atractivo sistema de instalación (en modo gráfico) y el cómodo mantenimiento de componentes de software, lo que facilita enormemente las tan frecuentes actualizaciones. Se puede obtener tanto gratuitamente en la red (por ejemplo la distribución de Fedora, que aún es libre) como adquiriendo las versiones comerciales (tal es el caso de Enterprise 4, 5, Advanced Server, etc).

Estas versiones son soportadas por la mayoría de los fabricantes de hardware de servidores en el mundo (HP, IBM, Dell, etc..)

Todos los productos de linux redhat se basan en un único núcleo, bibliotecas, herramientas de desarrollo y utilidades. Esto proporciona un ambiente homogéneo ideal para multisistema simplificado y de escritorio a configuraciones de centros de bases de datos. La ventaja inmediata es el despliegue simplificado de aplicaciones distribuidas y un sólido ambiente para los usuarios y los administradores del sistema.

El sistema operativo linux proporciona la infraestructura de sistema operativo y básicas de red mediante una amplia gama de servicios:

- Correo electrónico
- Archivos (SMB/NFS)
- Impresión
- Firewall
- Interpretores de comandos de acceso remoto
- DHCP
- DNS
- Autenticación de red (Kerberos)
- Noticias
- Respaldo
- Servicio de Directorio (LDAP)
- SSL

Soporta múltiples arquitecturas como

- Intel X86
- Intel Itanium
- AMD AMD64
- IBM zSeries
- IBM iSeries
- IBM pSeries
- IBM S/390

Después de la versión 9.00 , se ofrecen versiones comerciales (enterprise versión 2, 3, 4 o Advance Server), sobre todo para servidores, y tienen un costo asociado (ver <http://www.redhat.com/software/rhel/purchase/index.html>) , ofreciendo como valor agregado servicio de soporte por correo, web o teléfonos gratuitos internacionales, copia de los medios y actualizaciones por el año. Como se mencionó, estas versiones son recomendadas para servidores, por su completa integración con los fabricantes.

En algunas situaciones, en máquinas de un procesador, aún se puede trabajar con versiones free, como Fedora, que se descargan de la web, pero se deben obtener los driver que no llegase a incluir. Para máquinas de dos procesadores se debe descargar la versión que soporta SMP.

Las versiones comerciales de RedHat Enterprise son vendidas por suscripción anual y corren en múltiples arquitecturas, certificadas por varios fabricantes. Si no re renueva las suscripción, se pierde el derecho a las actualizaciones.

Para ver más información, se puede consultar: <http://www.redhat.com/software/rhel/>

En estas versiones hay dos familias que son la ES y AS, las cuales mencionaremos brevemente:

Red hat Enterprise Linux ES: Provee el core de sistema operativo para servidores e infraestructura de red de la mayoría de aplicaciones. Es compatible totalmente con toda la familia RedHat Enterprise, y soporta las necesidades para aplicaciones críticas. Se recomienda para sistemas de hasta 2 Cpus y 8 GB de RAM.

Tiene dos versiones la Básica y Estándar que difieren principalmente en el tipo de soporte técnico ofrecido.

Para más información ver: <http://www.redhat.com/software/rhel/es/>.

Red hat Enterprise Linux AS: Provee el core para sistemas de mayor envergadura, y soporta múltiples arquitecturas, de hasta 16 Cpus y 64 GB de RAM .

También tiene dos versiones : Estándar y Premium.

Para ver más información ver: <http://www.redhat.com/software/rhel/as/>.

1.1.2.SUSE LINUX

De forma semejante a la distribución de RedHat, Suse tiene varias familias de productos.

La versión más reciente de SUSE linux es la versión Enterprise 9.

SUSE® LINUX Enterprise Server 9 permite a las empresas aprovechar al máximo Linux* y el código abierto y constituye una base ampliable y de alto rendimiento para la informática empresarial segura. Diseñado para proporcionar fiabilidad, ofrece toda la funcionalidad y potencia que precisan las redes de hoy en día y responde a las demandas de los usuarios. SUSE LINUX Enterprise Server también es compatible con una amplia gama de plataformas hardware y las principales aplicaciones software.

http://www.novell.com/products/linuxenterpriseserver8/sles_datasheet.pdf

1.1.3. COMPATIBILIDAD DE LOS SISTEMAS OPERATIVOS Y LOS FABRICANTES.

Es importante tener en cuenta la compatibilidad que debe existir entre la plataforma de hardware del servidor y el sistema operativo Linux ofrecido. Vamos a presentar algunos

ejemplos de información que garantiza la compatibilidad de estos fabricantes con dos posibles versiones de Linux (redhat y suse):

1.1.3.1. COMPATIBILIDAD ENTRE LAS MÁQUINAS IBM Y RED HAT ENTERPRISE.

En la página <http://www.pc.ibm.com/us/compat/nos/redchat.html>

Red Hat Operating Systems																		
Model	x455-8855	x450-8680	x445-8870	x440-8687	x382-8834	x365-8861,8862	x360-8686	x346-8840	x345-8670	x336-8837	x335-8676,8830	x306-8836	x255-8685	x236-8841	x235-8671	x226-8640	x225-8647,8649	x206-8482
Red Hat Enterprise Linux 3 AS for Itanium	✓	✓			✓													
Red Hat Enterprise Linux 3 WS for x86									✓		✓	✓	✓		✓		✓	✓
Red Hat Enterprise Linux 3 AS for AMD64/EM64T								✓		✓				✓				
Red Hat Enterprise Linux 3 ES for x86								✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Red Hat Enterprise Linux 3 AS for x86			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Red Hat Enterprise Linux WS (v2.1 for x86)							✓	✓	✓		✓		✓		✓		✓	
Red Hat Enterprise Linux ES (v2.1 for x86)							✓	✓	✓		✓		✓		✓		✓	
Red Hat Linux 9.0							✓	✓			✓				✓			
Red Hat Enterprise Linux AS 2.1 for the Itanium Processor	✓	✓			✓													
Red Hat Enterprise Linux AS (v2.1 for x86)			✓	✓		✓	✓	✓	✓		✓	✓	✓		✓		✓	✓
Red Hat Linux 8.0							✓	✓			✓							
Red Hat Linux Professional 7.3								✓					✓					
Red Hat Linux Professional 7.2							✓	✓					✓		✓			
Red Hat Linux 7.1							✓											

1.1.3.2. COMPATIBILIDAD ENTRE LAS MÁQUINAS IBM Y SUSE LINUX

Ver: <http://www.pc.ibm.com/us/compat/nos/suselinux.html>

SUSE LINUX Operating Systems																		
Model	x455-8855	x450-8688	x445-8870	x440-8687	x382-8834	x365-8861,8862	x360-8686	x346-8840	x345-8670	x336-8837	x335-8676,8830	x306-8836	x255-8685	x236-8841	x235-8671	x226-8648	x225-8647,8649	x206-8482
SUSE LINUX Enterprise Server 8 for x86 (UL 1.0)			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SUSE LINUX Standard Server 8 (UL 1.0)			✓			✓	✓					✓	✓	✓		✓		✓
SUSE LINUX Enterprise Server 9 for AMD64/EM64T							✓			✓								
SUSE LINUX Enterprise Server 9 for x86						✓	✓	✓	✓	✓	✓		✓		✓		✓	
SUSE LINUX Professional 8.2								✓		✓		✓			✓			
SUSE LINUX Enterprise Server 8 for Itanium (UL 1.0)	✓	✓			✓													
SUSE LINUX Professional 8.1							✓	✓		✓					✓		✓	
SUSE LINUX Professional 8.0				✓			✓	✓		✓		✓			✓		✓	
SUSE LINUX Enterprise Server 7				✓			✓	✓		✓		✓						
SUSE 7.3													✓					
SUSE 7.2							✓											

1.1.3.3. COMPATIBILIDAD ENTRE LAS MÁQUINAS HP Y RED HAT ENTERPRISE Y SUSE.

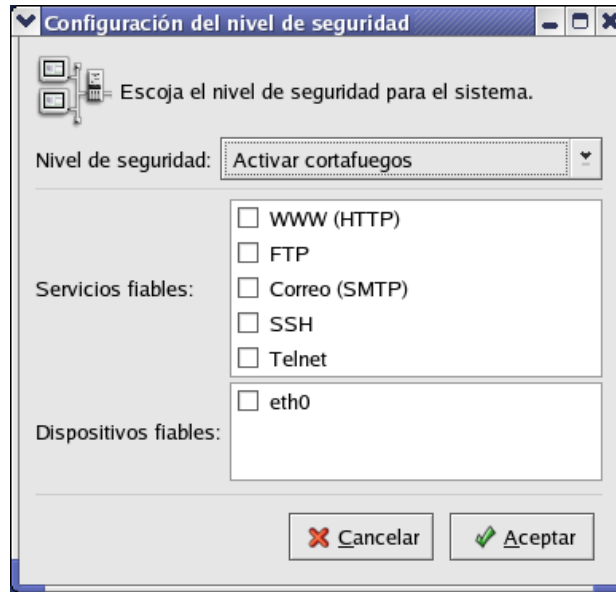
Ver: <http://h18004.www1.hp.com/products/servers/linux/hpLinuxcert.html>

DL385	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$
DL740	✓	\$			✓	\$	✓	\$					✓	\$				
DL760 G2	✓	\$			✓	\$	✓	\$					✓	\$				
ML series	RH EL 3*		RH EL 2.1		SLES 9		SLES 8											
	x86	AMD64/EM64T	x86	x86	AMD64/EM64T	x86	AMD64											
ML110 ²			✓	\$														
ML150 ³							✓	\$ ³										
ML150 G2 SCSI	✓	\$	✓	\$		✓	\$	✓	\$									
ML330 G3 ATA			✓	\$				✓	\$									
ML330 G3 SCSI	✓	\$	✓	\$	✓	\$		✓	\$									
ML350 G3	✓	\$	✓	\$	✓	\$		✓	\$									
ML350 G4	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$								
ML370 G3	✓	\$	✓	\$	✓	\$		✓	\$									
ML370 G4	✓	\$	✓	\$	✓	\$	✓	\$	✓	\$								
ML530 G2	✓	\$	✓	\$	✓	\$		✓	\$									
ML570 G2	✓	\$	✓	\$	✓	\$		✓	\$									

1.2. NIVELES DE SEGURIDAD

Es muy importante , como lo trataremos al final del módulo, la seguridad del sistema operativo y los servicios a implementar.

En la fase de instalación de linux, se pregunta por el nivel de seguridad deseado para configuración del firewall y se pregunta si se desea activar o no el firewall. Si se activa, se deben escoger los servicios que se van a permitir, pues el firewall por defecto cierra todos los servicios.



En la instalación de RedHat, se pregunta por el SELinux, que es un sistema adicional que nos permite notificar si alguna labor coloca en riesgo el sistema.

Si se activo el SELinux, para desactivarlo, se debe editar el archivo selinux de la carpeta:

```
[root@demos ~]# cd /etc/sysconfig/
[root@demos sysconfig]# ls -l selinux
lrwxrwxrwx 1 root root 19 nov 16 22:48 selinux -> /etc/selinux/config
[root@demos sysconfig]#
```

Estaba :

```
[root@demos sysconfig]# cat selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - SELinux is fully disabled.
SELINUX= permissive
# SELINUXTYPE= type of policy in use. Possible values are:
#   targeted - Only targeted network daemons are protected.
#   strict - Full SELinux protection.
SELINUXTYPE=targeted
```

Y se debe desactivar:

```
[root@demos sysconfig]# cat selinux
# This file controls the state of SELinux on the system.
```

```
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#   targeted - Only targeted network daemons are protected.
#   strict - Full SELinux protection.
```

1.3.INSTALACIÓN Y ARRANQUE

Para estos laboratorios, se trabajará con máquinas virtuales, como se detalla en el último capítulo. Se mencionarán dos herramientas que permiten esta labor, para efectos de las prácticas.

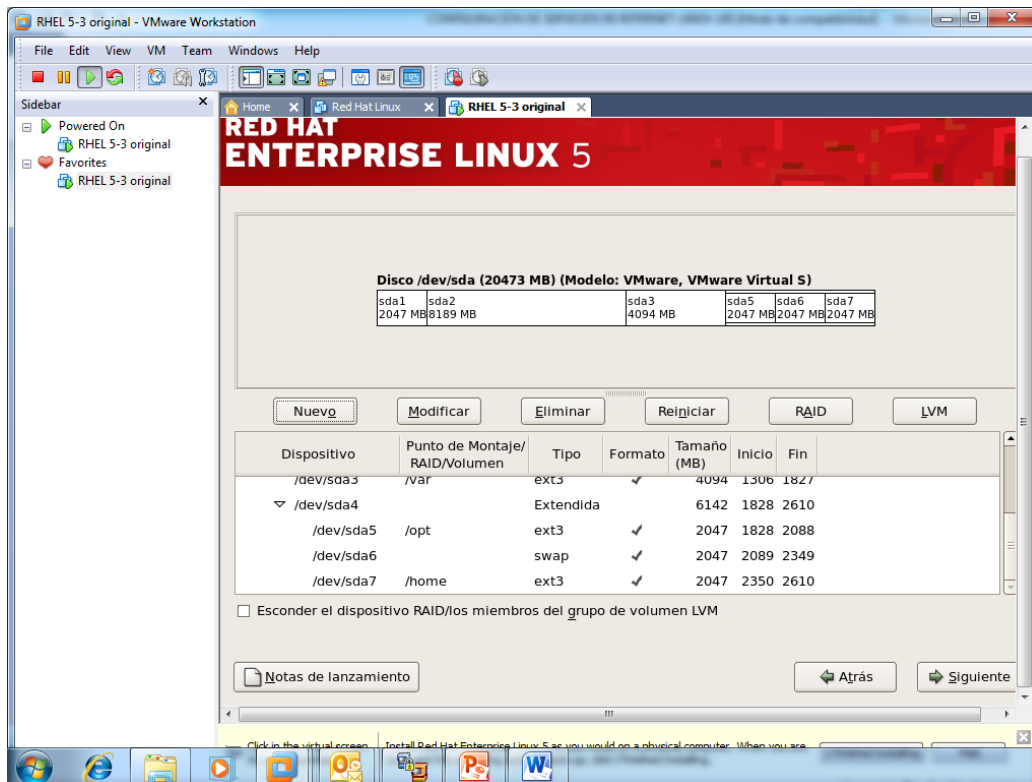
1.3.1.INSTALACIÓN DE LINUX.

Se resumen aquí, pero el detalle de la instalación se encuentra en el capítulo 5 , al final de este libro, cuando se hace la instalación por medio del VMWare.

Los pasos para la instalaciones de RedHat Linux se resumen en:

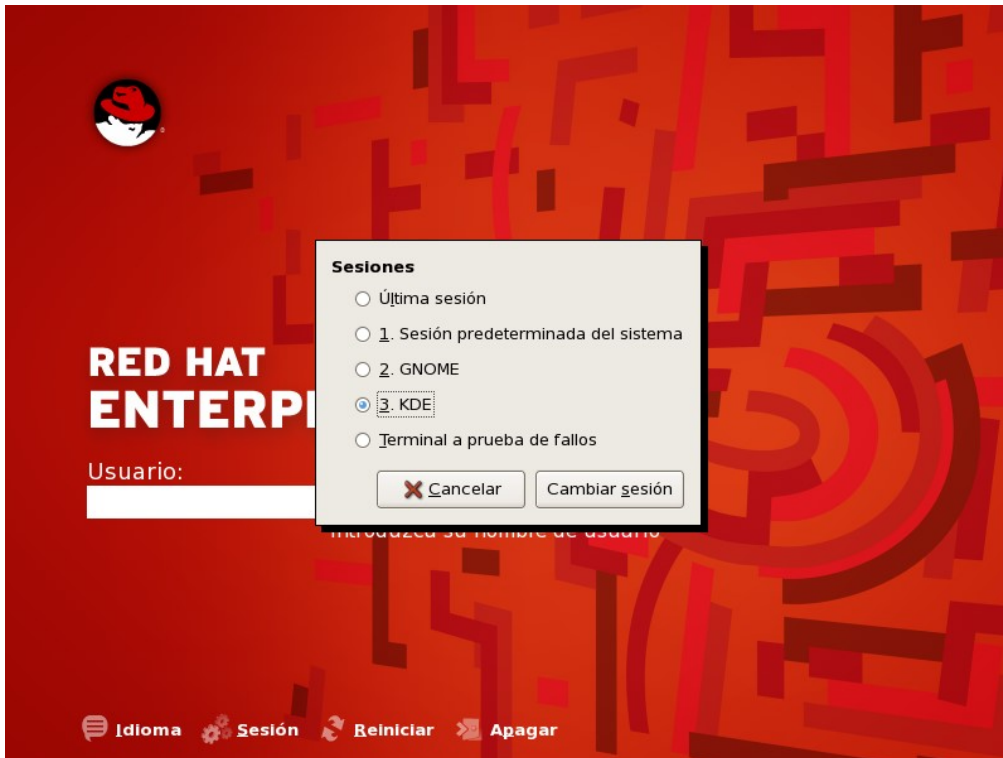
- Se debe de disponer de toda la información sobre el hardware de la máquina, por si se requiere algún controlador, o driver. Conocer que tipo de video, controladora, tarjeta de red, etc. Si se tienen periféricos, se debe de disponer de los drivers respectivos. Las versiones nuevas de sistemas operativos generalmente reconocen automáticamente los elementos de equipos antiguos.
- Planear el esquema de particionamiento de los discos, por ejemplo:

Numero partición	Nombre	Tamaño (Mb)
Sda6	Swap	2048
Sda1	/	2048
Sda2	/usr	8192
Sda7	/home	2048
Sda5	/opt	2048
Sda3	/var	4096



- Determinar la dirección IP que se asignará al equipo, dirección del DNS, puerta de enlace, nombre del mismo.
- Se bootea con el CD 1 del sistema o el DVD . Se puede obviar el chequeo de los CDs, y se escoge idioma de instalación español y el teclado en US Internacional (depende de cada caso).
- Se hace búsqueda de instalaciones anteriores y para nuestro caso se le indica que es una nueva instalación. Se escoge personalizada (para poder seleccionar los paquetes) y que el particionamiento se va a hacer con DiskDruid. Esta es una herramienta que permite definir y configurar las particiones del sistema. De acuerdo al disco que tengamos, el esquema de particionamiento puede cambiar, pero se recomienda dejar mínimo las particiones presentadas en el cuadro anterior. El nombre del dispositivo asociado a cada partición puede variar con el tipo de disco. En este momento se decide si las particiones serán formateadas o no.
- Luego se procede con la asignación de la dirección IP, el nombre del sistema, puerta de enlace y DNS .
- Se pregunta si se habilita el cortafuegos que trae el sistema, y además si se activa el SELinux o se deja en advertencia o apagado.
- Se escogie la zona horaria y luego la clave del root.
- Se inicia la búsqueda de paquetes y se pregunta por cuales se desea instalar. Para nuestro caso de pruebas se le indica que todos. Hace chequeo de dependencias e inicia la instalación.
- Al terminar, rebootea el sistema y muestra una serie de mensajes antes de cargar Linux .
- Carga RedHat Linux y entra a un diálogo de tareas postconfiguración. Pregunta si acepta los términos de la licencia, la fecha y hora, la hora y la configuración de pantalla.
- Pregunta un usuario adicional y no se le indica ninguno.
- Pregunta si se van a instalar Cds adicionales, termina y muestra la ventana de RedHat.
- Se ingresa con sesión KDE y se le indicó que fuese la predeterminada.

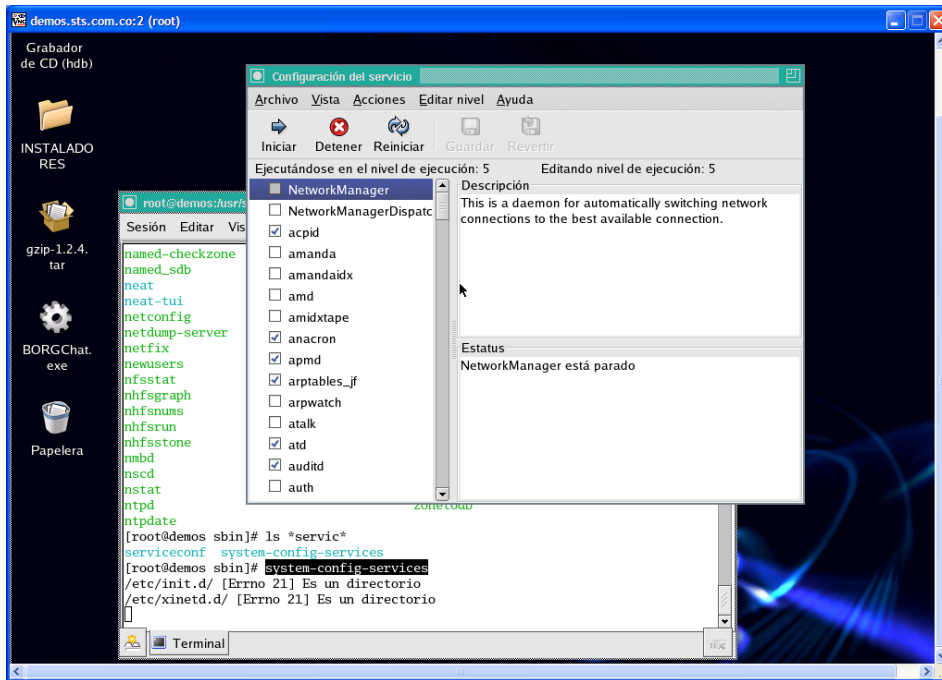
Ya en el ambiente Linux, se puede empezar a trabajar:



1.3.2. CONFIGURACIÓN DE SERVICIOS DESEADOS EN EL ARRANQUE.

Aunque en el momento de la instalación, nosotros seleccionemos una serie de servicios disponibles en el sistema, estos pueden no arrancar en el momento de subir Linux, y deben ser arrancados manualmente. En los respectivos directorios para cada nivel (ejm: `/etc/rc/rc5.d`) están los script que empiezan por la letra S, indicando que ese servicio debe ser arrancado en el momento de pasar a ese nivel.

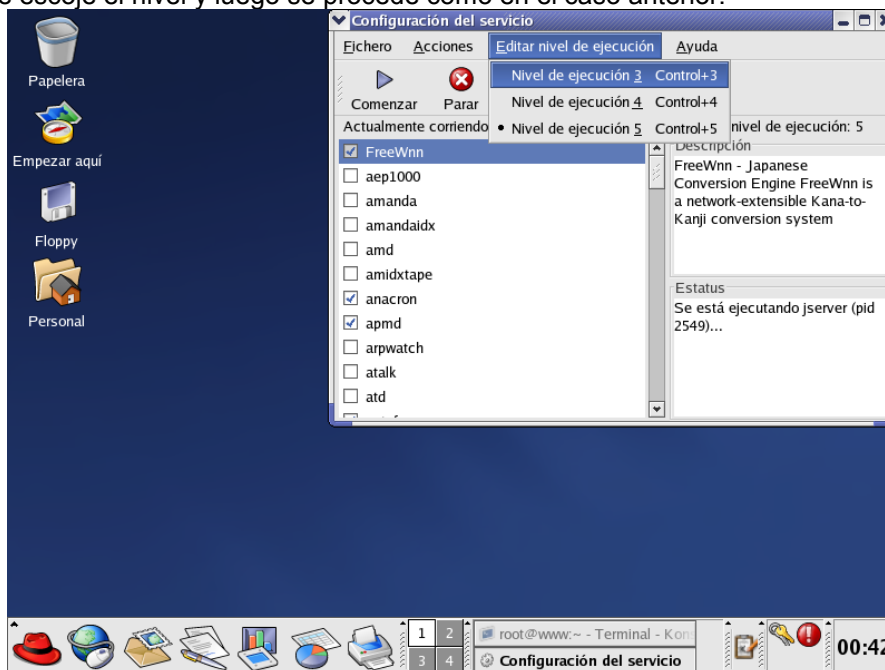
Sin embargo, podemos indicarle, después de la instalación que procesos deseamos que suba el sistema automáticamente, desde el interfaz gráfico una ventana de comandos se digita el comando `system-config-services`, o se ingresa por el sombrero de inicio, configuración del sistema, configuración de servidores y por ultimo servicios y aparece:



Dependiendo del nivel en que arranque la máquina linux, se pueden configurar los servicios para cada uno de ellos. En la pantalla anterior se configuran para el nivel 5 por defecto (multiusuario con interfaz gráfica) .

Se escoge marcando el servicio y si se desea que inicie inmediatamente en la parte superior se escoge iniciar. Una vez se han marcado todos los servicios de deseo o no , carguen en el boot del sistema, se escoge la pestaña de guardar en Archivo.

Si se desea configurar para el nivel 3 por la pestaña de editar nivel de la parte superior, primero se escoge el nivel y luego se procede como en el caso anterior.



1.3.3. BAJANDO EL SISTEMA

Una forma sencilla de bajar el sistema, es desde la entrada gráfica, en el momento de dar login , se puede escoger la opción de apagarlo. Hay que tener cuidado pues por defecto cualquier usuario puede apagar el sistema , ya que no pregunta clave de superusuario.

Existen otras formas de bajar el sistema. A través de los comandos:

shutdown [-y -gseg -iestado]

donde:

- y:** Responde automáticamente **yes** a todas las preguntas.
- g:** Permite definir a los cuantos segundos se bajará el sistema. (defecto 60 seg) (periodo de gracia).
- i:** Permite identificar a que estado se llevará el sistema. (por defecto **s**).

La forma más rápida y sencilla es ejecutando el comando:

init 0

El cual ejecuta el proceso /etc/rc0, que ejecuta los shell encontrados en el directorio /etc/rc/rc0.d, que empiezan por **K**, e invocan los respectivos archivos en /etc/rc/init.d.

En el proceso de apagado del equipo se pueden tener varias situaciones para la cuales se pueden elegir ciertos comandos :

Se desea pasar la máquina a modo monousuario (solo consola texto y ningun otro usuario conectado) :

```
init 1
init s
shutdown -g0 -is
```

Se desea rebootear la máquina (bajar y subir el sistema)

```
init 6
reboot
```

1.3.3.1. PARA COMPLEMENTAR

Para mejorar la seguridad del sistema y evitar que cualquier usuario desde la consola gráfica, de la orden de apagar el sistema, que se debe configurar, o como se debe de corregir esto?

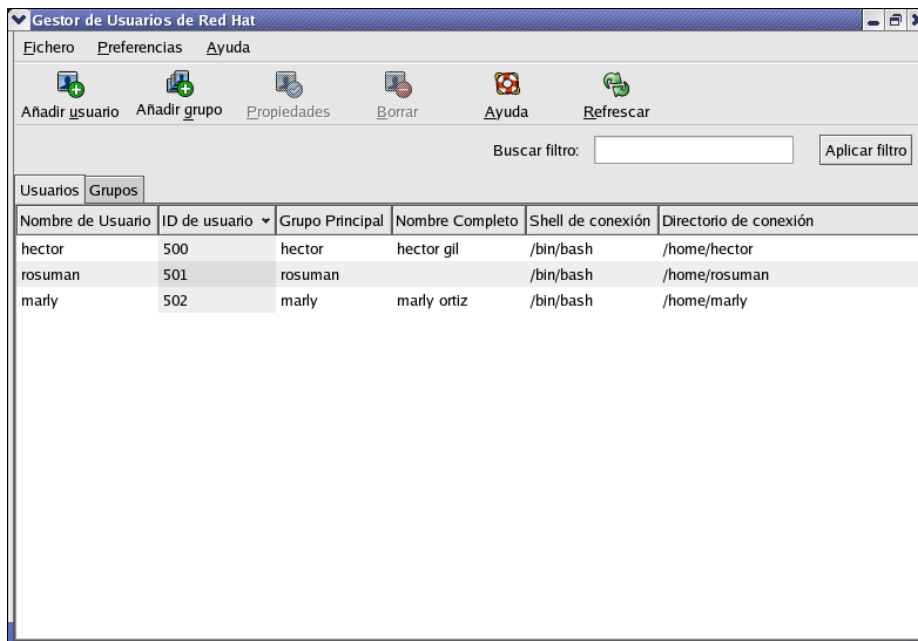
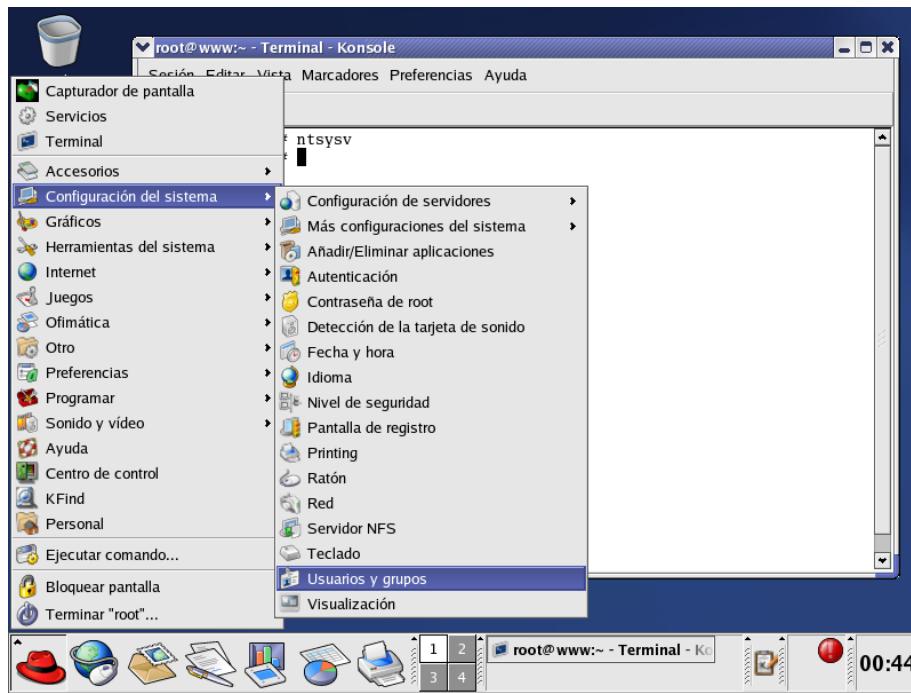
1.4. ALGUNAS TAREAS DE ADMINISTRACIÓN DEL SISTEMA

Aunque el enfoque de este módulo no es un curso de linux, existen algunas tareas que debemos conocer , pues serán requeridas dentro de los procesos de configuración de algunos servicios.

1.4.1.MANEJO DE USUARIOS Y GRUPOS

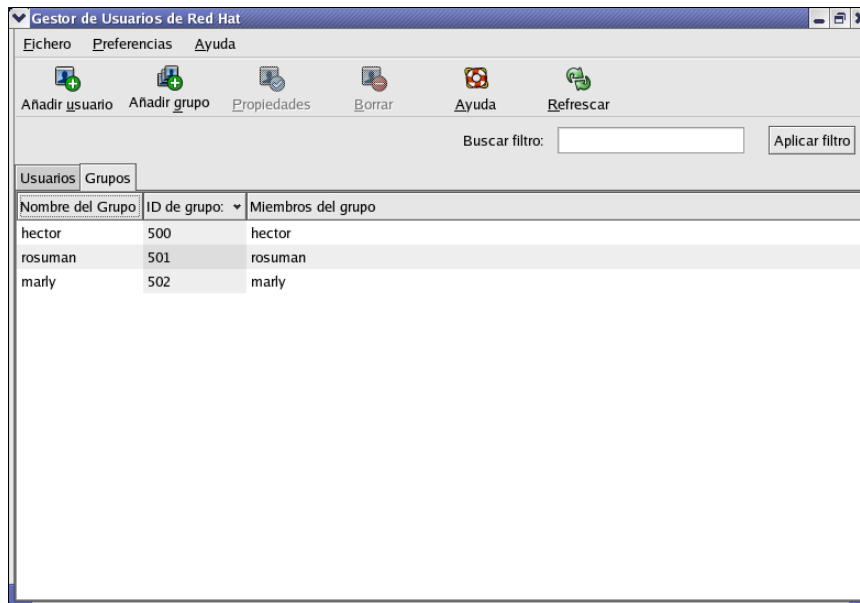
La administración de usuarios y grupos es muy sencilla mediante las herramientas gráficas.

Se puede realizar con el aplicativo webmin (tratado más tarde), en modo comandos, o Invocando el user manager.

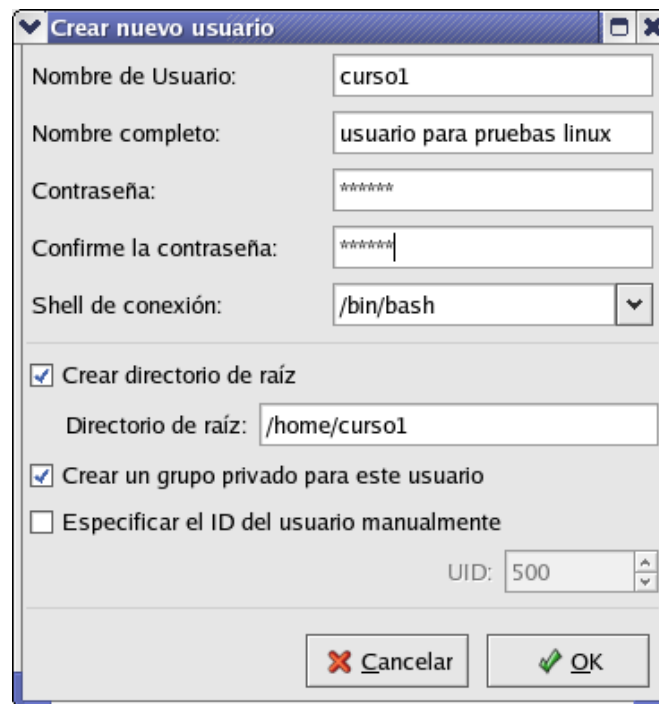


La anterior ventana ,lista tanto usuarios como grupos del sistema, pues la pestaña superior así lo indica.

Si se desea listar los grupos de la máquina se escoge la otra pestaña.

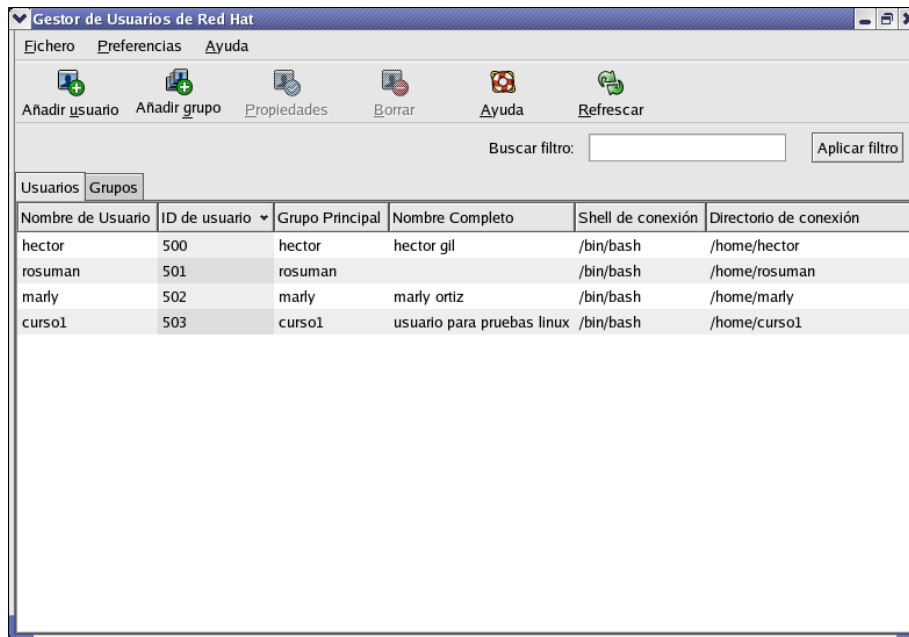


Para crear un nuevo usuario, se escoje añadir usuario en la parte superior.

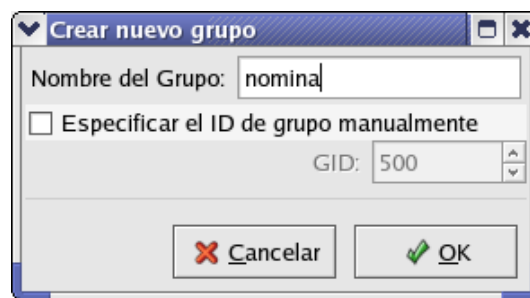


En la anterior pantalla se puede verificar el número de usuario, en este caso seria el usuario 500.

Para verificar si el nuevo usuario existe se regresa a la ventana de usuarios

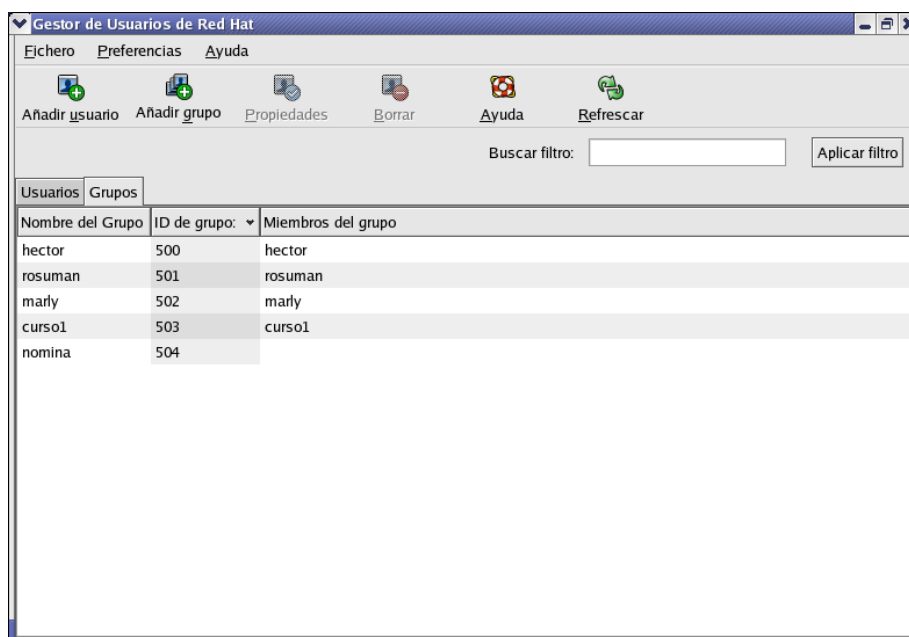


Para crear un grupo, por ejemplo nomina, se escoge añadir grupo.

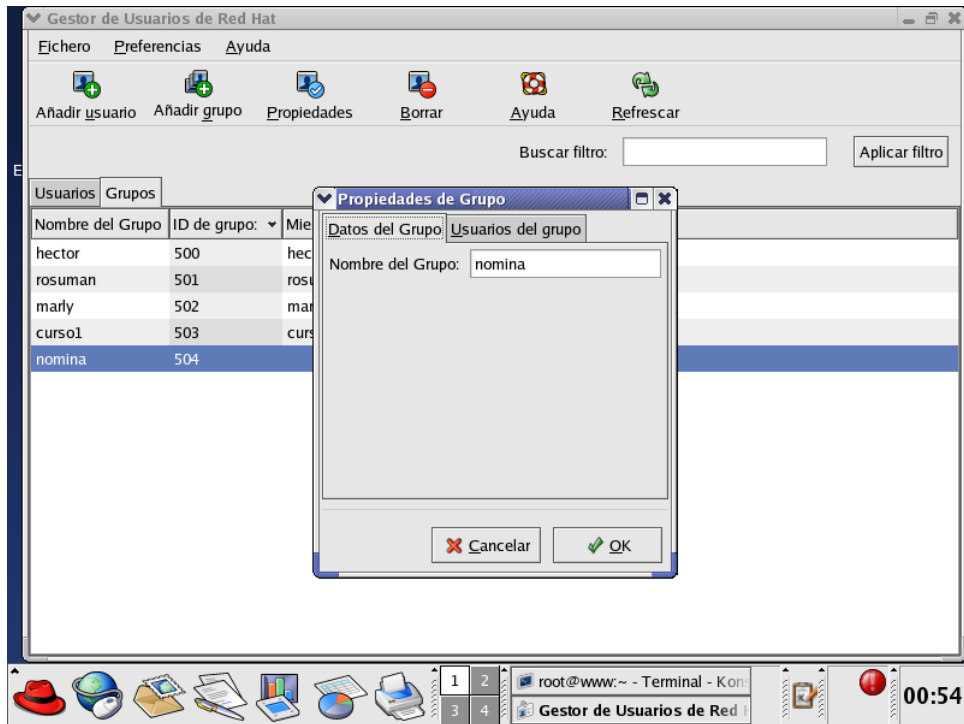


En esta pantalla se puede especificar el número del grupo que estamos creando.

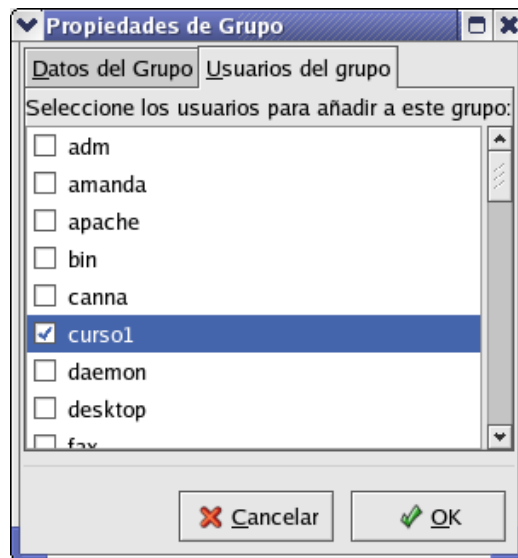
Para verificar si el grupo existe se retorna a la ventana se retorna a la ventana respectiva.



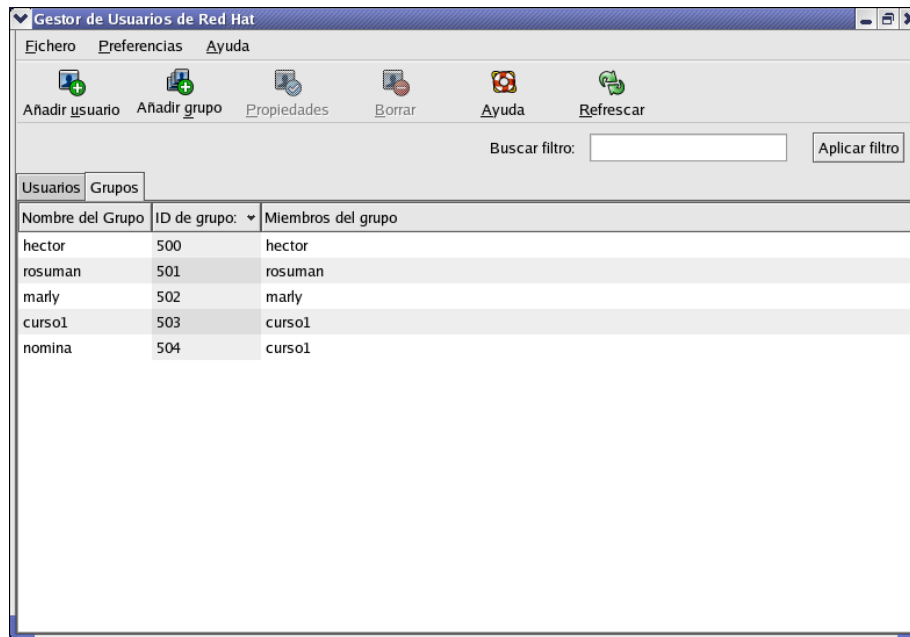
Para incluir un usuario a ese nuevo grupo, se selecciona el grupo y se escoge el icono propiedades en la parte superior.



Adicionar el usuario curso1 creado anteriormente, se escoge usuarios del grupo y se marca.



Para reflejar los cambios, volvemos al user manager



1.4.1.1. PARA COMPLEMENTAR

- Una vez instalado el aplicativo webmin para administración del sistema, proceder a crear un usuario por la pestaña de sistema y explorar las diferentes características o parámetros que se le pueden configurar en el momento de la creación, como tiempo de expiración, tiempo de inactividad, y otros.
- Hacer la creación de un usuario en modo comandos.
- Desde superusuario cambiarle la clave a un usuario sin conocer la anterior.
- Tratar de hacer lo mismo , estando logeado con un usuario normal.

2. REDES CON LINUX

Aquí solo citaremos algunos temas que ustedes ya han tratado en el transcurso de la especialización, y que son importantes para las actividades de este módulo. Es vital que recuerden estos conceptos o revisen la información pertinente.

- Que son redes ethernet
- Como es el paquete que viaja por una red ethernet (frame)
- Que es una red LAN
- Que es una red WAN
- Como pueden ser los paquetes que viajan por una red WAN. Tomar algún protocolo conocido.
- Que protocolos se manejan en este tipo de redes
- Protocolo TCP/IP y direcciones IP
- Transmission Control Protocol (TCP): protocolo a nivel de transporte.
- User Datagram Protocol (UDP).
- Telnet, FTP, SMTP, SNMP, HTTP, BIND, SMB, SSH.

2.1.CONFIGURACIÓN DE TCP/IP POR COMANDOS Y ARCHIVOS INVOLUCRADOS

Ustedes ya revisaron la configuración de algunos parámetros de red, mediante el uso del interfaz gráfico. Ahora mencionaremos los archivos involucrados.

/etc/hosts Contiene los nombres y las direcciones Internet de los Hosts involucrados. Para cada host se debe dar:

- Dirección internet.
- Nombre oficial del host.
- Alias o nombre con el que vamos a referenciar el host. El alias para el host local es seguido de la palabra "Localhost". Esta lista solo debe incluir la dirección de la máquina local ,y la dirección IP de la máquina, junto con su dirección IP, si se esta usando DNS. No deben porque aparecer entradas de otras máquinas.

Es importante que en este archivo se encuentre la IP y nombre completo de la máquina en una línea y en otra la dirección 127.0.0.1 localhost.localdomain localhost. Por ejemplo:

127.0.0.1	localhost.localdomain	localhost
192.168.45.35	pedro.uis.edu.co	pedro

Si este archivo pierde alguna de sus líneas, puede que los servicios de red o de internet no funcionen.

/etc/services Servicios disponibles y puertos asociados. Puede servir de guía para conocer los numeros de puertos asociados a los diferentes protocolos de red.

/etc/xinetd.d Archivos para los servicios de red.

/etc/resolv.conf Configuración del cliente DNS. Especifica el dominio y la máquina que actua con servidor de nombres. Además el orden en que sé resolveran los nombres. Ejemplo:

domain	hector.uis.edu.co
nameserver	192.168.45.36

/etc/sysconfig/network-scripts/ifcfg-eth0

Archivo con la configuración de la tarjeta de red eth0. Ejemplo:

```
[root@demos network-scripts]# cat ifcfg-eth0

GATEWAY=192.168.19.1
BOOTPROTO=none
PEERDNS=yes
IPV6INIT=no
TYPE=Ethernet
HWADDR= Aquí va la MAC
DEVICE=eth0
NETMASK=255.255.255.0
BROADCAST=192.168.19.255
IPADDR=192.168.19.2
NETWORK=192.168.19.0
USERCTL=no
ONBOOT=yes
```

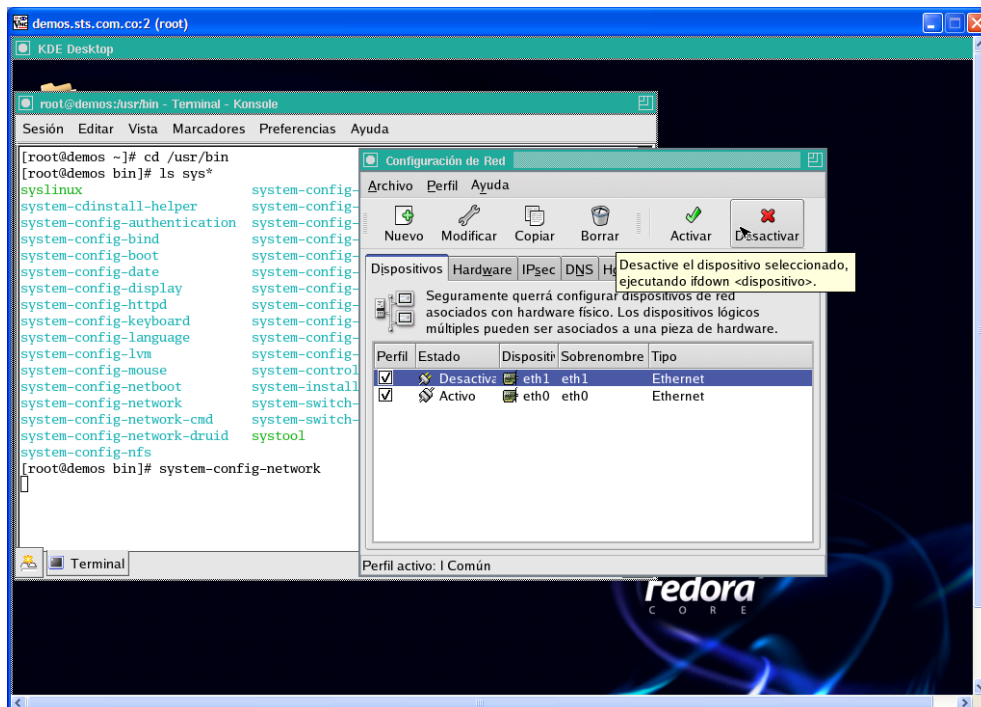
Si se desea cambiar la dirección IP, el gateway, si la tarjeta bootea con el sistema, la mascara.

2.2.ALGUNOS COMANDOS TCP/IP

Si se desea verificar que la dirección IP y otras características fueron definidas apropiadamente para la tarjeta de red, se puede usar comandos o herramientas de Red Hat como:

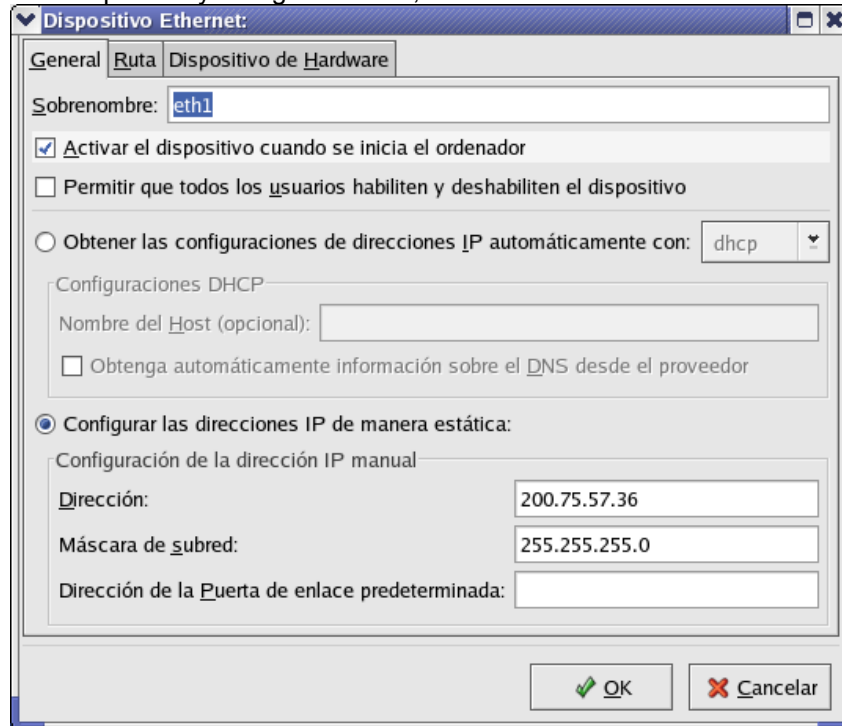
system-config-network

Y nos aparece una pantalla semejante a :

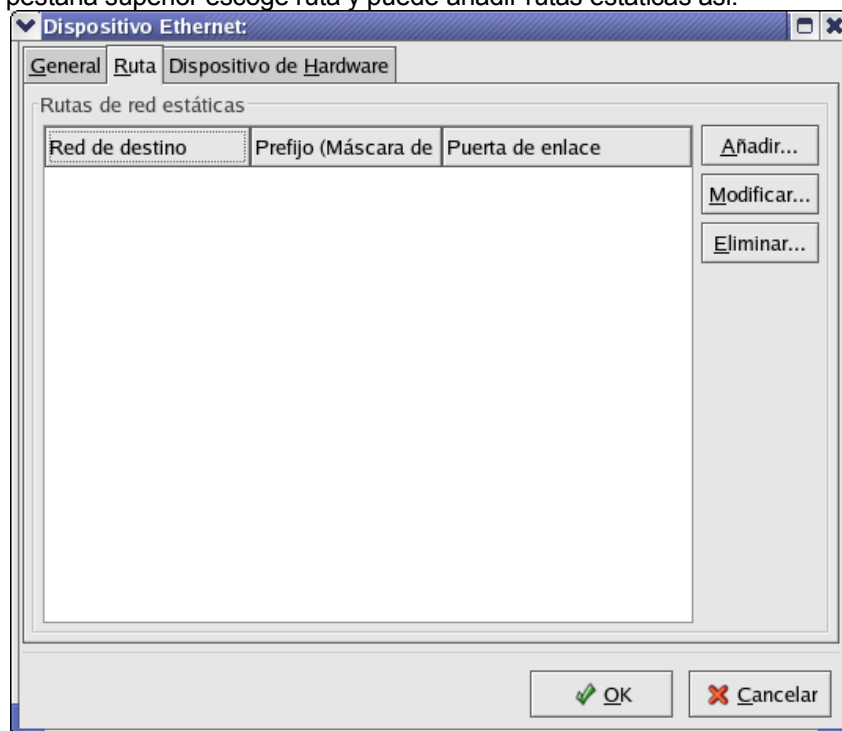


Para definir enrutador por defecto:

Se ubica sobre el dispositivo y escoge modificar, como se muestra a continuación



Luego en la pestaña superior escoge ruta y puede añadir rutas estaticas asi:



#netstat -i

Name	Mtu	Network	Address	Ipkts	lerrs	Opkts	Oerrs	Coll
ef0	1500	200.25.18	pelicano	13033995	1302	964346	39	32492
lo0	8304	loopback	localhost	1065823	0	1065823	0	0

#ifconfig ef0


```
ef0:  
flags=1c63<UP,BROADCAST,NOTRAILERS,RUNNING,FILTMULTI,MULTICAST,CKSUM>  
inet 200.25.18.4 netmask 0xfffffc0 broadcast 200.25.18.63
```

Con el netstat se puede observar el nombre de la interface de red. En este caso se llama ef0. Además información sobre paquetes entrantes, salientes y colisiones.

Con el comando ifconfig, se puede observar y modificar los parámetros cargados a las interfaces de red.

Existe un comando que permite revisar la conexión de los hosts, enviando una serie de caracteres al otro equipo y esperando recibir estos de nuevo. Es el comando "ping", cuyo formato es:

ping nombrehost

Si solo se da el nombre del host, se envía una paquete de caracteres y se espera recibir estos nuevamente, en forma indefinida hasta que el usuario detenga la emisión. Se presentan unas estadísticas sobre los caracteres perdidos para estudiar el estado de la conexión y del medio físico. Se puede definir el tamaño del paquete enviado y la cantidad de veces que se realiza esta operación.

TELNET : Permite hacer login en un host remoto. No se recomienda por no ser seguro.

La sintaxis del comando es la siguiente:

Telnet [nombre-host]

Si solo Telnet es digitado, el sistema lo situara en modo comandos, cuyo prompt es " Telnet> ". En este modo se pueden dar los siguientes subcomandos:

Open nombre-host	Para conectarse a un sistema.
close	Cierra la conexión.
quit	Salir de TELNET.
help	Ayuda .
status	Muestra información de la conexión actual .

En el momento que la conexión es hecha, se pasa a modo de transferencia de datos y se interactua con el hosts remoto para realizar Login.

FILE TRANSFER PROTOCOL (FTP): FTP permite realizar transferencia de archivos entre una máquina unix y otros equipos que corran TCP/IP. No se recomienda por no ser seguro.

Para permitir que a nuestra máquina Linux le puedan hacer FTP desde otra hay varias condiciones que se debe cumplir, que describiremos más adelante en la sección de configuración de este servicio.

La sintaxis del comando es:

ftp [opciones] [nombre-host]

donde la opciones pueden ser:

- d Habilita debug
- g Deshabilita el globbing (uso de wildcards)
- i Habilita prompt interactivos, es decir, pedir confirmación para cada archivo al trabajar con wildcars.
- n No pregunta por un usuario al establecer la conexión.

Este comando nos coloca en un subsistema cuyo prompt es "ftp>", en donde disponemos de los siguientes subcomandos:

! [comando] Ejecutar comando del sistema local . Sale al prompt de UNIX, donde se regresa con "exit".

append arch [arch-rem]: Agrega el contenido del archivo local (arch), al archivo remoto (arch-rem).

type ascii : Pasa el tipo de archivo a ASCII.

type binary Pasa el tipo de archivo a IMAGE.

type image Pasa el tipo de archivo a IMAGE.

bell Activa o desactiva sonido de campana al terminar copia de archivos.

bye Termina FTP y la sesión remota.

cd directorio Cambia el directorio de trabajo del host remoto .

close Termina sesión remota y permanece en FTP.

debug [on/off] Al activar debug (on), cada comando enviado al sistema remoto es mostrado precedido por el string -->

delete archivo Borra archivo en el host remoto.

dir [direct] [archivo] Lista el contenido del directorio del host remoto y sitúa este en el archivo del host local .

get arch-rem [arch-local] Transfiere archivo del host remoto al local.

glob Interpretación de wildcards. Si esta en "on", se pueden usar estos; si es "off", los wildcars son interpretados literalmente .

hash Impresión del símbolo "#", por cada bloque de datos transmitido (1024 bytes).

lcd directorio Cambia el directorio de trabajo del host local.

ls [directorio [archivo]] Muestra información abreviada del contenido del directorio remoto y sitúa esta en un archivo del host local.

mdelete archivos Borra archivos del host remoto.

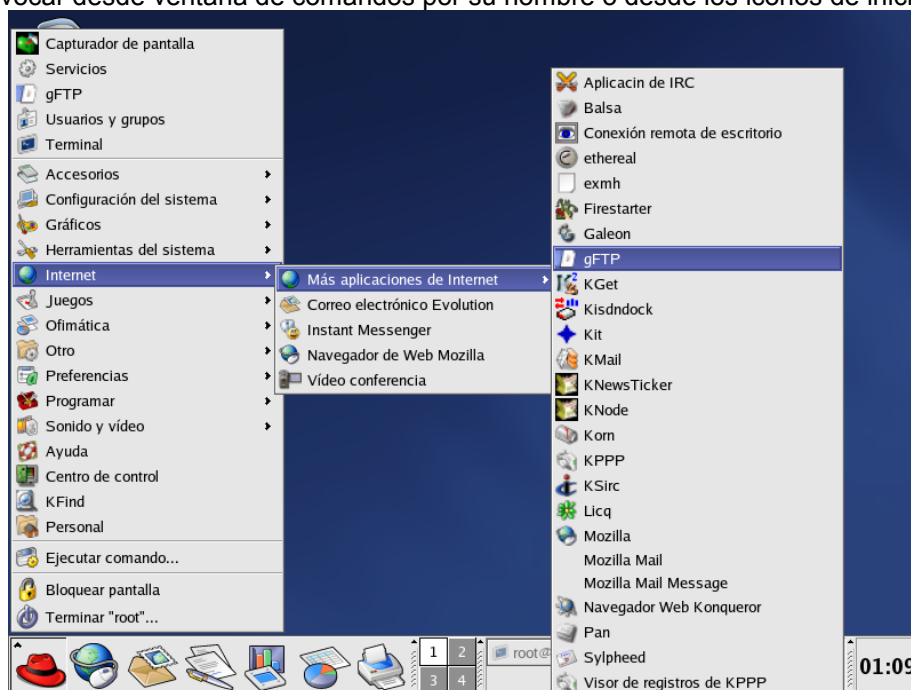
mkdir directorio Crea un directorio en el host remoto.

mget [archivos] Transfiere archivos, usando wilcards desde el hosts remoto.

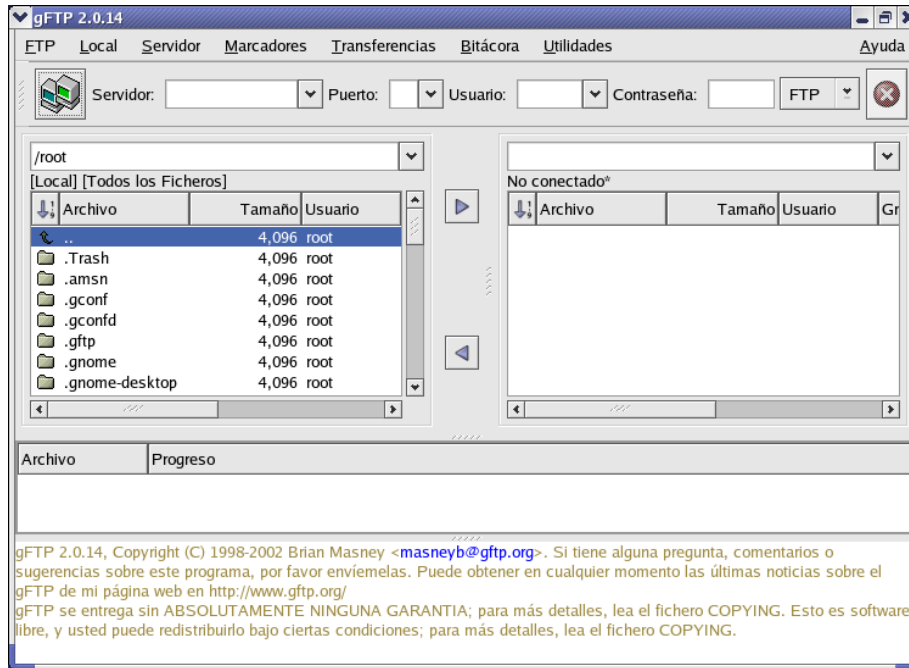
mput [archivos] Envía archivos al host remoto, usando wilcards.

- open nombre-host Establece conexión con el host remoto.
- prompt Si esta "off", múltiples archivos son procesados sin pedir confirmación para cada uno.
- put arch-local [arch-rem] Envía un archivo al host remoto.
- pwd Muestra el nombre del directorio actual del host remoto.
- quit Termina sesión de FTP.
- rename nombre1 nombre2 Cambia de nombre al archivo nombre1 del host remoto.
- rmdir directorio Borra directorio del host remoto.
- status Muestra los parámetros para transferencia de archivos .
- user [user-id [password]] Realiza login en el host remoto.

La mayoría de usuarios tiende a utilizar interfaces gráficas del FTP para realizar las tranferencias de archivos, que no detallaremos aquí por su sencillas. Por ejemplo el gftp. Se puede invocar desde ventana de comandos por su nombre o desde los iconos de inicio:



Su interfaz grafica es muy amigable como se puede ver a continuación.



Comando nslookup

Me permite averiguar la dirección IP de un nombre de máquina digitado, consultando a un servidor DNS. Sirve para probar un servidor DNS.

Sintaxis

nslookup nombre completo máquina

Comando arp

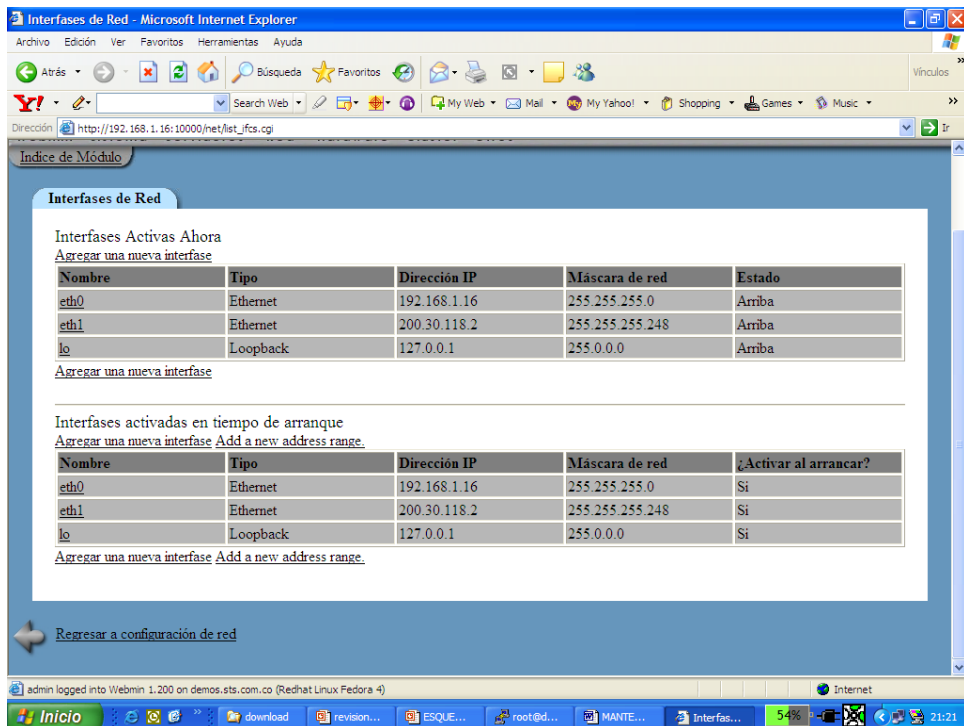
Me permite averiguar la dirección MAC de otras máquinas.

2.3. ASIGNACIÓN DE INTERFAZ LOGICAS

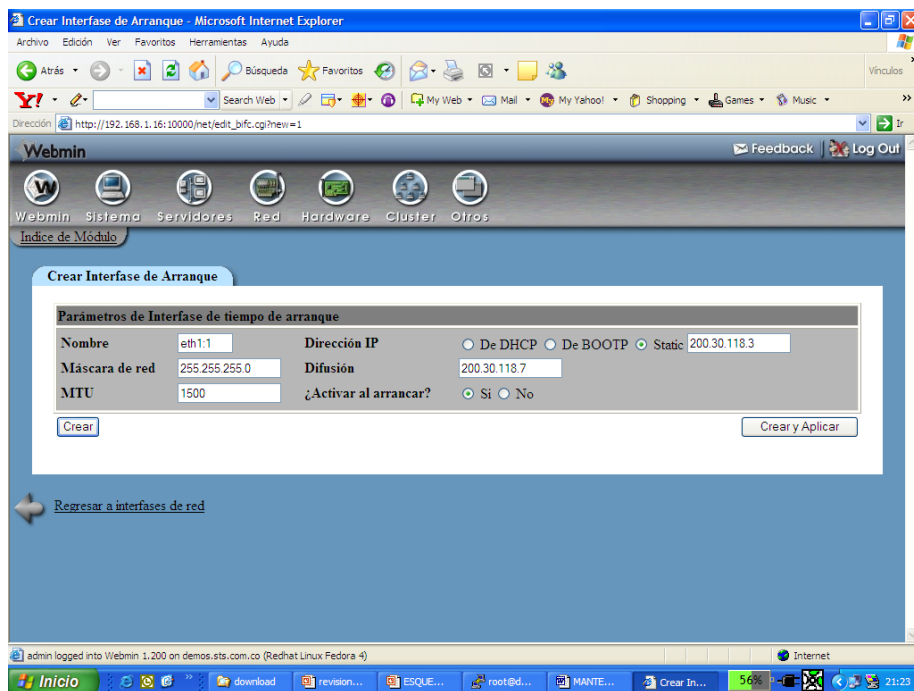
A una tarjeta de red en linux, se le puede asignar varias direcciones IP, para que esta responda como si fuese máquinas diferentes.

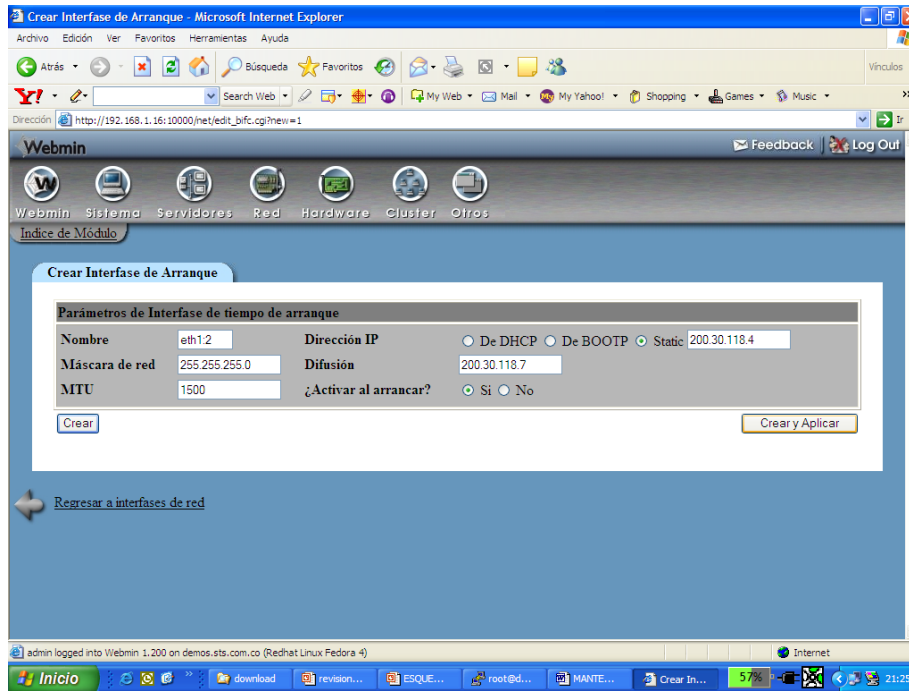
Para lograr esto se puede proceder de varias formas: desde el utilitario webmin, o por linea de comandos.

Por webmin (se tratará más adelante), en los iconos superiores de trabajando en red, se puede revisar las interfases:

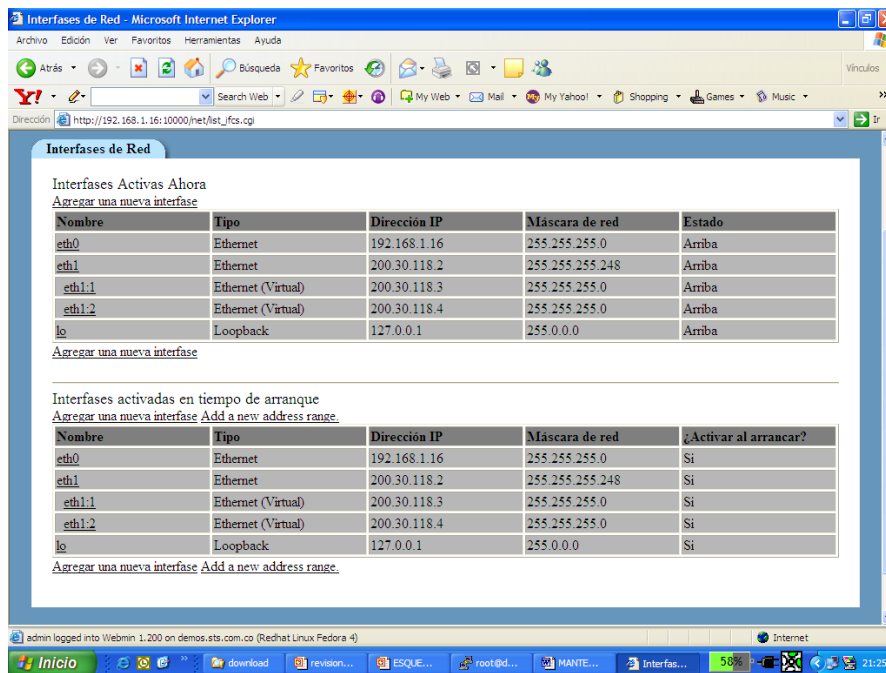


Para adicionar una interfaz de red virtual se crea por la opción de Agregar y en el nombre de la interfaz se usa la sintaxis: nombre:número, por ejemplo : eth1:1.





al revisar por webmin se ven:



por comandos:

```
[root@demos webmin-1.200]# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0B:6A:EC:3E:C6
      inet addr:192.168.1.16  Bcast:192.168.1.255  Mask:255.255.255.0
      inet6 addr: fe80::20b:6aff:feec:3ec6/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:29979 errors:0 dropped:0 overruns:0 frame:0
      TX packets:24883 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:12215696 (11.6 MiB)  TX bytes:8821894 (8.4 MiB)
      Interrupt:11 Base address:0xed00
```

```

eth1  Link encap:Ethernet HWaddr 00:40:F4:76:82:1C
      inet addr:200.30.118.2 Bcast:200.30.118.7 Mask:255.255.255.248
      inet6 addr: fe80::240:f4ff:fe76:821c/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1145 errors:0 dropped:0 overruns:0 frame:0
      TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:155499 (151.8 KiB) TX bytes:9032 (8.8 KiB)
      Interrupt:10 Base address:0xec00

eth1:1 Link encap:Ethernet HWaddr 00:40:F4:76:82:1C
      inet addr:200.30.118.3 Bcast:200.30.118.7 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      Interrupt:10 Base address:0xec00

eth1:2 Link encap:Ethernet HWaddr 00:40:F4:76:82:1C
      inet addr:200.30.118.4 Bcast:200.30.118.7 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      Interrupt:10 Base address:0xec00

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:1654 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1654 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:3412820 (3.2 MiB) TX bytes:3412820 (3.2 MiB)

[root@demos webmin-1.200]#
    
```

Una vez se grabe y activen los cambios , se puede probar desde una ventana de comandos o desde otra máquina que este en la misma red , dando un ping a la dirección que acabamos de incluir.

Las interfaz que aparece con la extensión :1 (ejm: eth1:1) es la virtual.

2.4. UTILITARIO DE ADMINISTRACIÓN WEBMIN

Para facilitar las labores de administración y operación del sistema, linux provee algunos utilitarios como las herramientas que se acceden por el inicio, para crear usuarios, manejo de disco, servicios, etc. Se pueden usar herramientas de terceros que se acceden via web como el Webmin.

En el CD se anexa un instalador de webmin, que se puede copiar a /opt/instaladores. En el proceso de instalación , puede preguntar por puerto por el cual atenderá las peticiones. Por default es el puerto 10000.

Desde /opt descomprimir el instalador de webmin-1200

```
[root@fw opt]# tar xvzf instaladores/webmin-1.200.tar.gz
```

Crea la carpeta respectiva y desde allí se corre el setup.sh

```

[root@fw opt]# cd webmin-1.200/
[root@fw webmin-1.200]# ./setup.sh
*****
*           Welcome to the Webmin setup script, version 1.200           *
    
```

```

*****
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-1.200 ...

*****
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: RHEL5

*****
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 SSLeay 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-1.200
..done

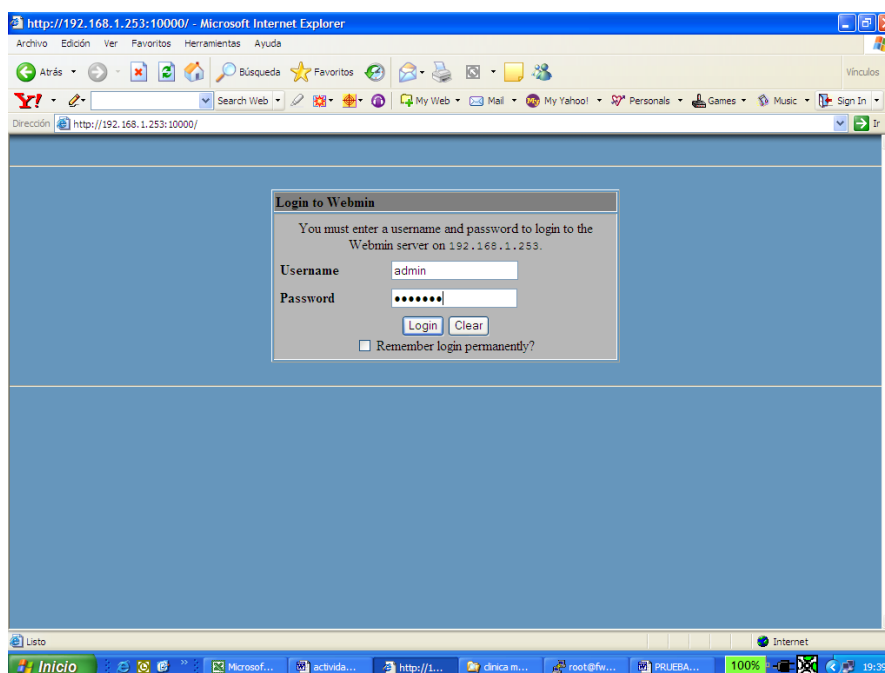
*****
Webmin has been installed and started successfully. Use your web
browser to go to

    http://fw.cmb.com.co:10000/

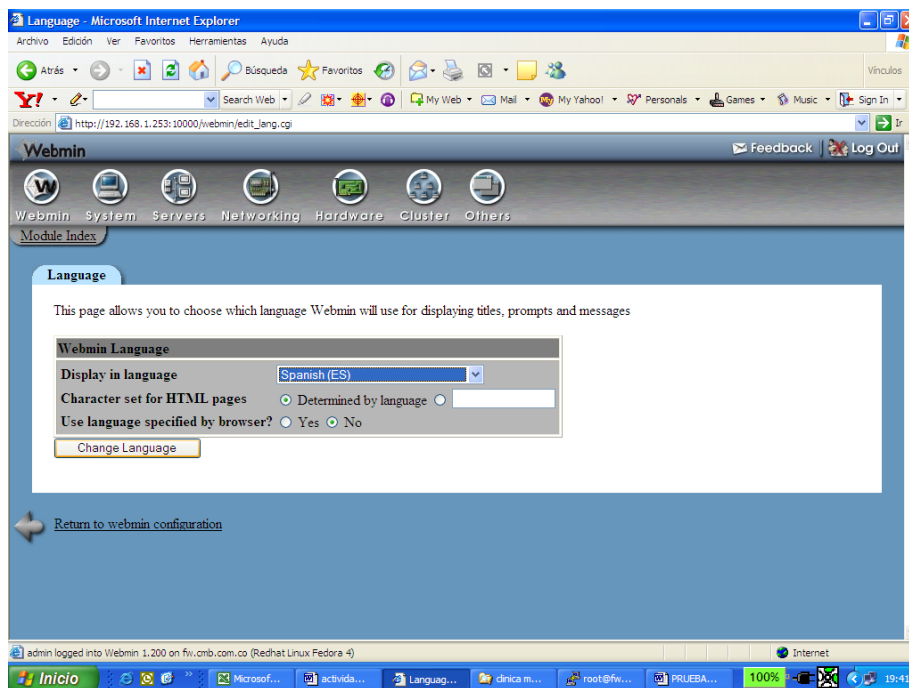
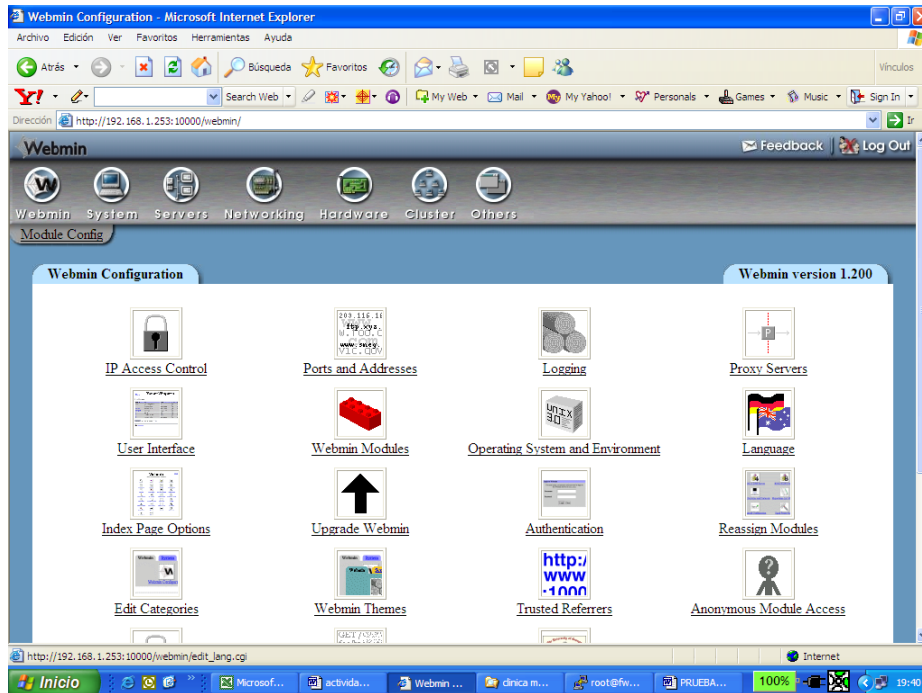
and login with the name and password you entered previously.

[root@fw webmin-1.200]#
    
```

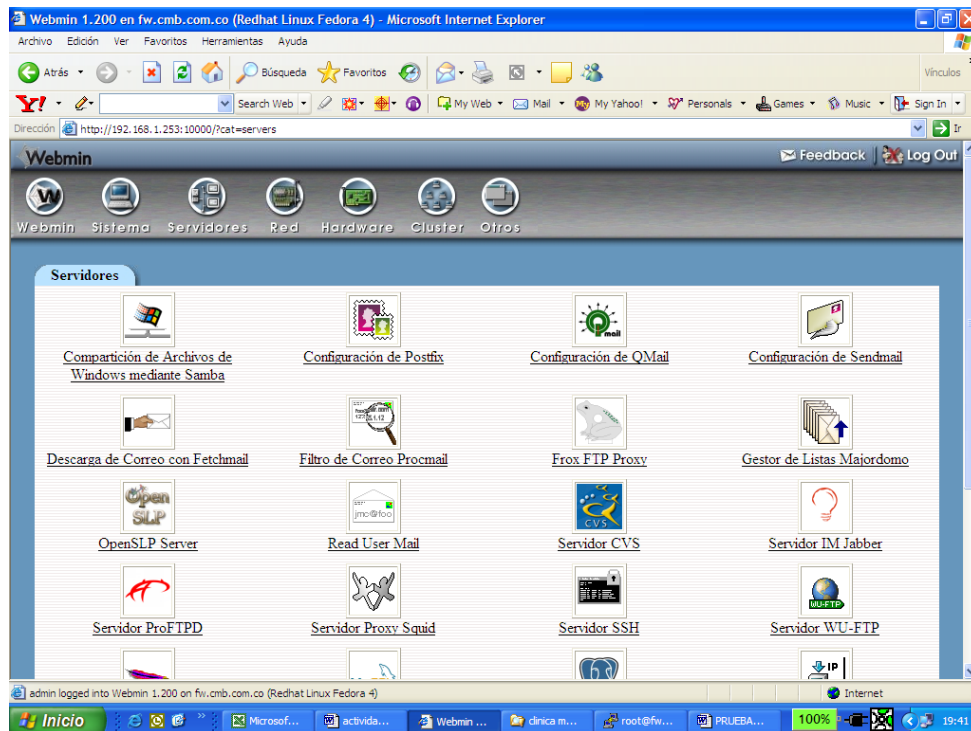
Probar invocándolo desde el PC (usuario admin, clave admin06), dando la dirección IP del servidor donde se instaló el webmin.



Luego personalizar el idioma (desde webmin configuration y luego Language):



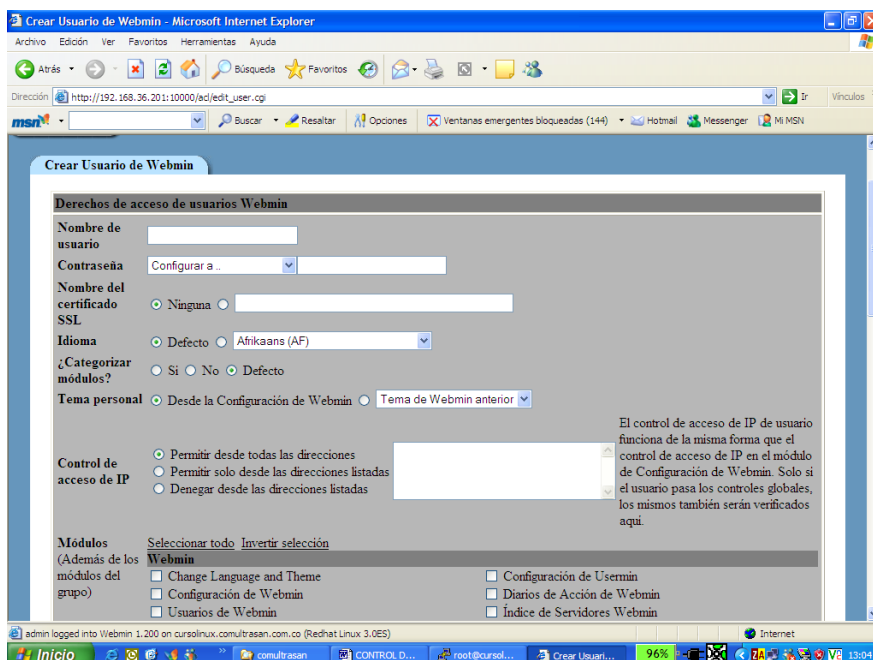
Una vez esta en español, para su mejor comprensión, se puede ver desde pestaña de servidores, todas las opciones que podemos tomar para configurar las diferentes aplicaciones que hay en el sistema (correo, samba, proxy, etc):



Realizaremos un breve recorrido por este entorno de trabajo.

2.4.1. CREACIÓN DE USUARIOS WEBMIN

Se pueden crear usuarios de webmin, para que solo tengan acceso a determinadas tareas o módulos:

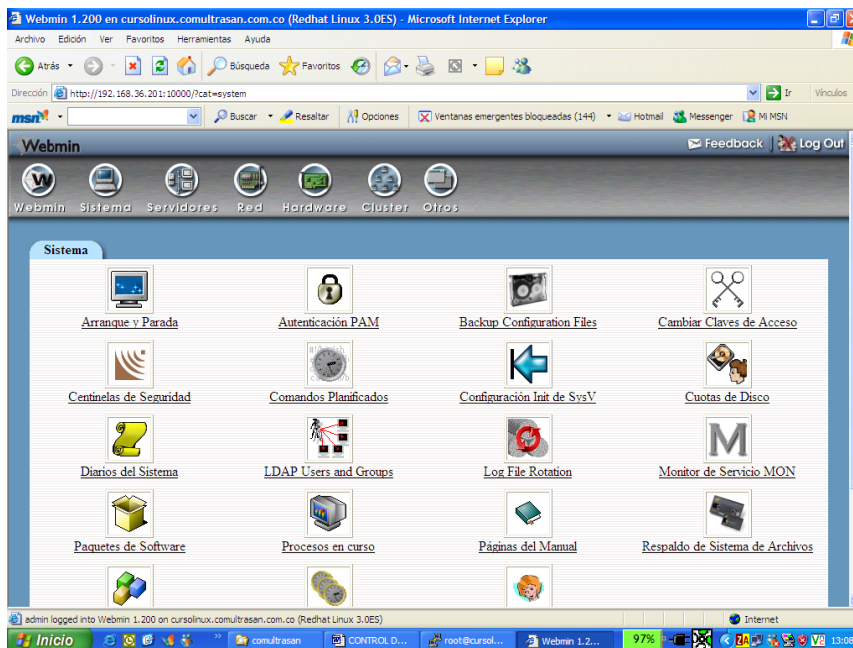




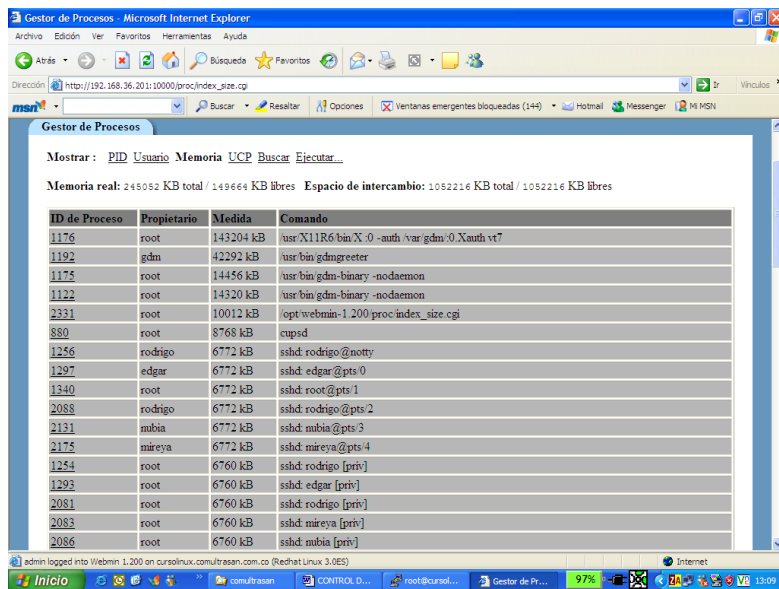
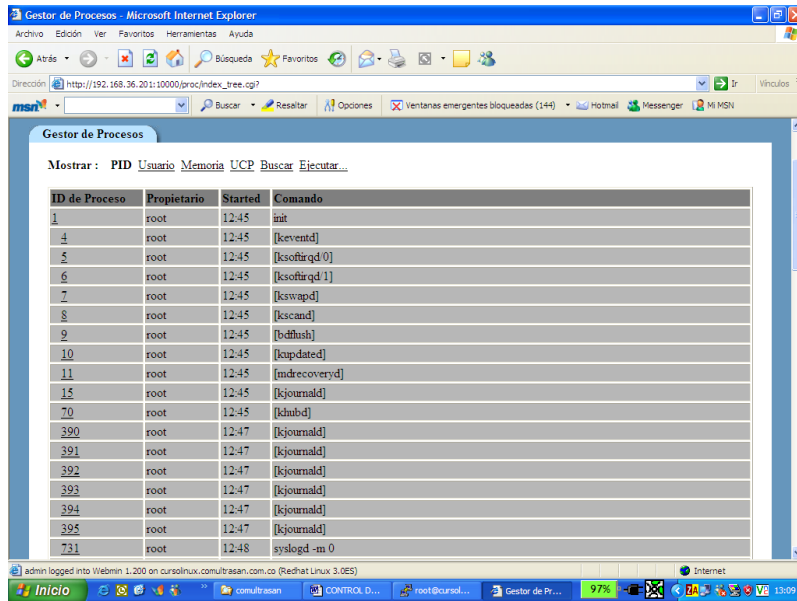
Como se puede observar, al crear al usuario en la parte final de la pantalla, se pueden escoger los módulos a los cuales ese usuario tiene acceso.

2.4.2. OPCIONES DEL MENU DE SISTEMA

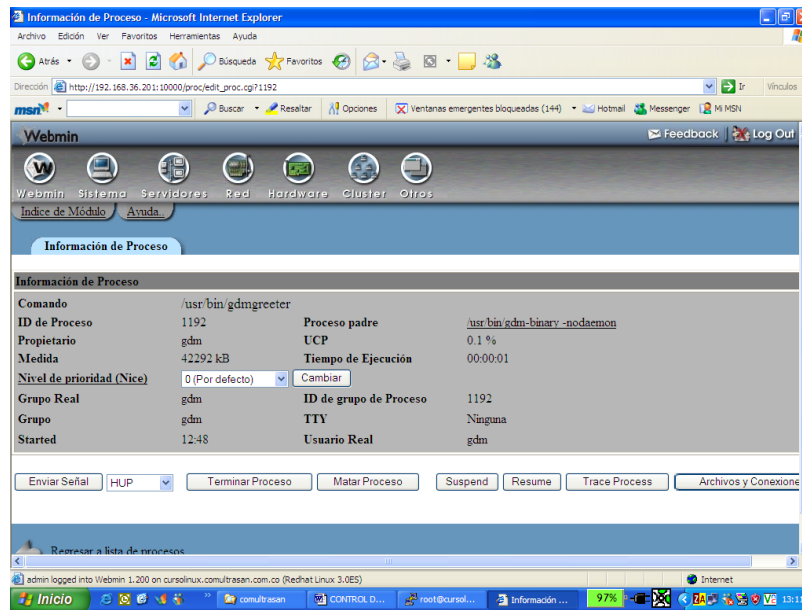
Si escogemos la opción o pestaña de sistema (en la parte superior), tenemos acceso a una serie de utilitarios para la administración de la máquina (apagado del sistema, planificación de trabajos, manejo de usuarios del sistema, etc.)



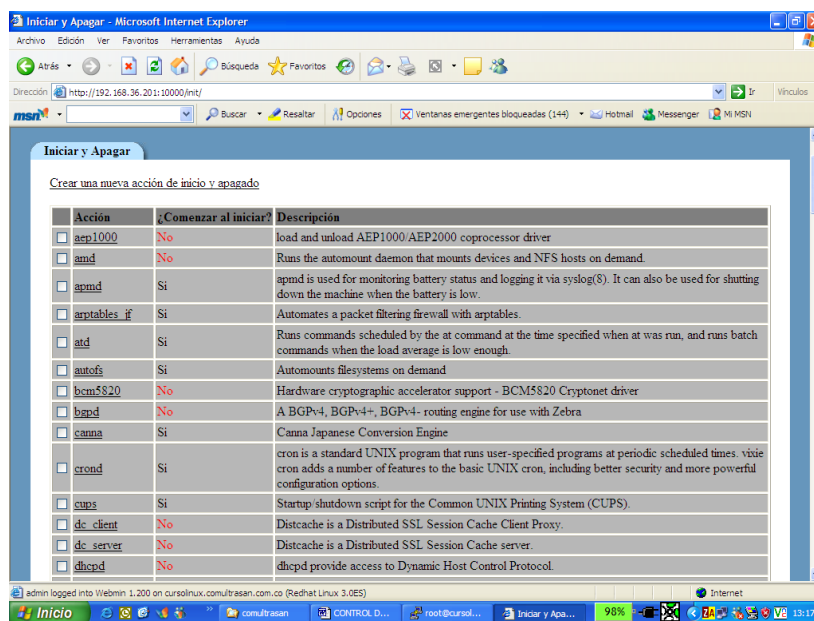
Por ejemplo se pueden observar y gestionar los procesos del sistema en curso (procesos en curso):

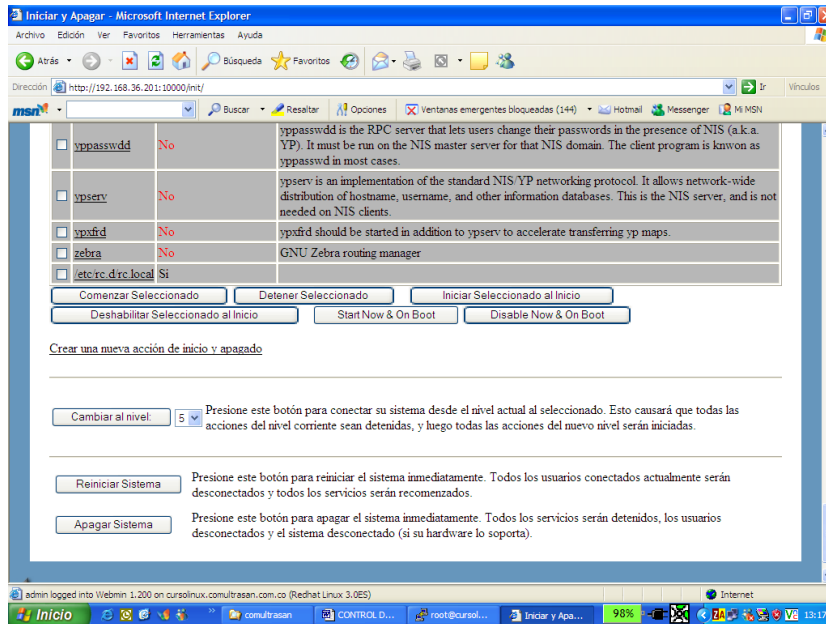


Se puede ver la información sobre un proceso en particular (inclusive cambiar la prioridad)

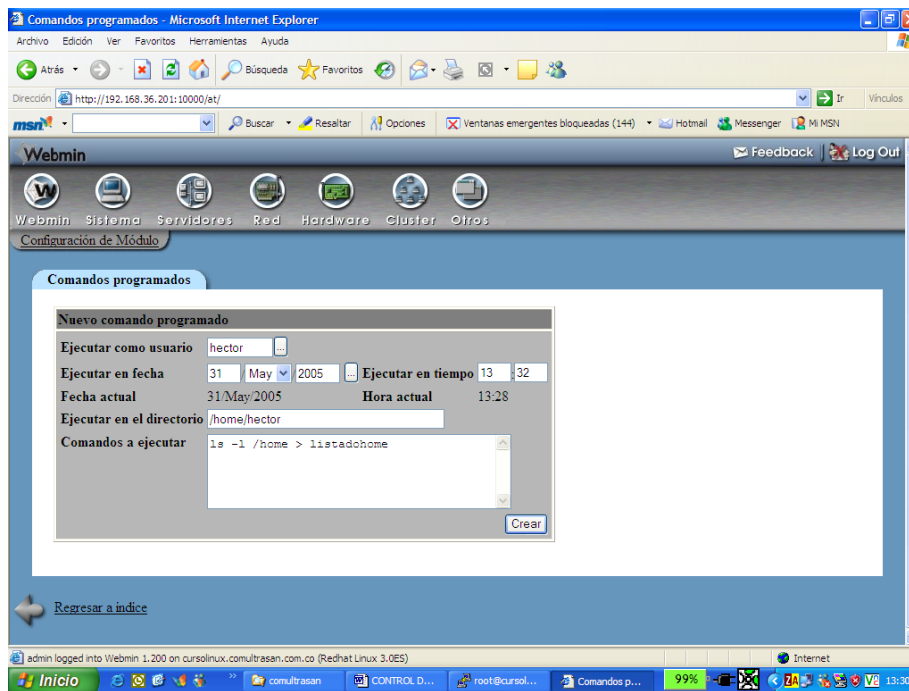


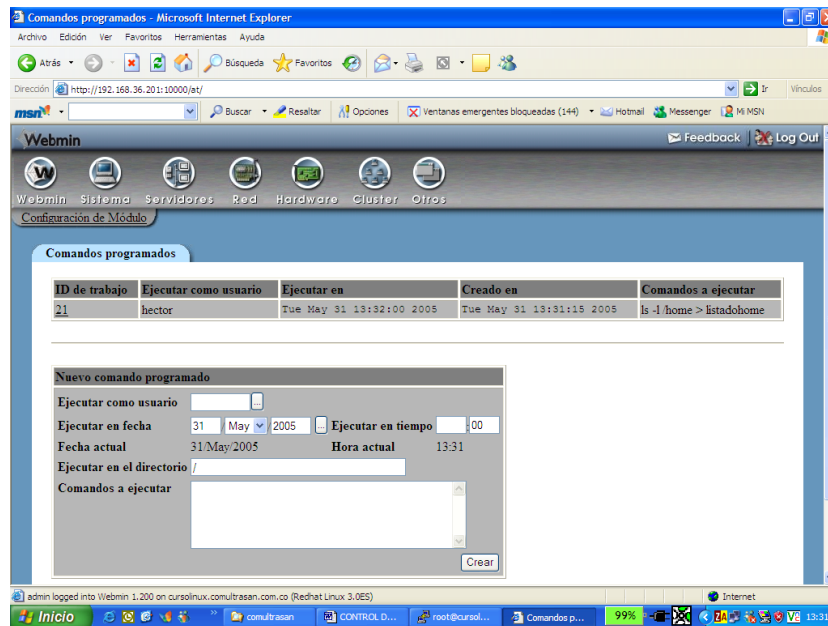
Se puede controlar los procesos que inician con el sistema (servicios) en cualquiera de los niveles de este (por arranque parada):





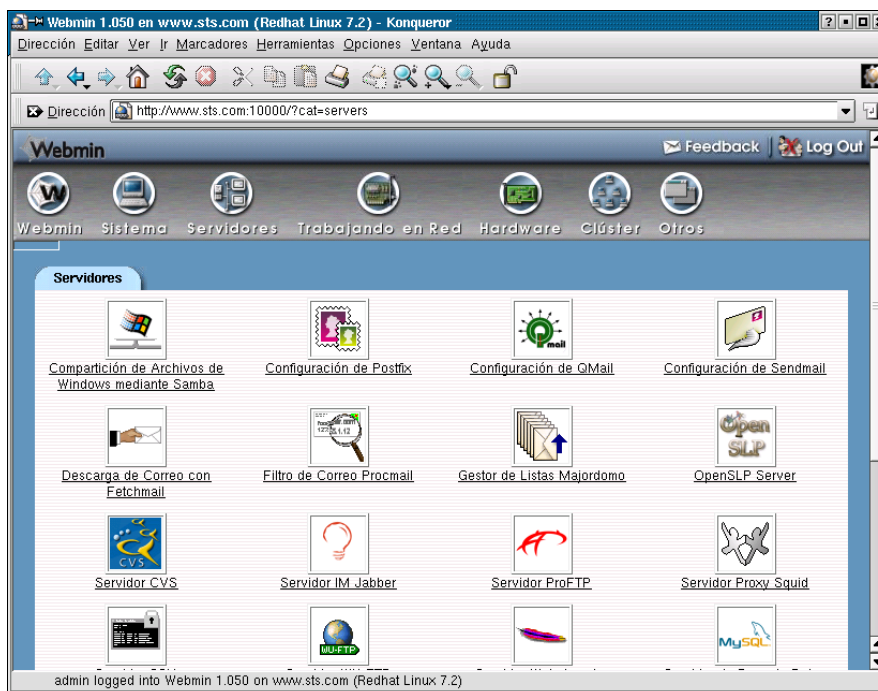
Programar tareas para que se ejecuten a determinada hora (comandos planificados), como se hace con el comando at:





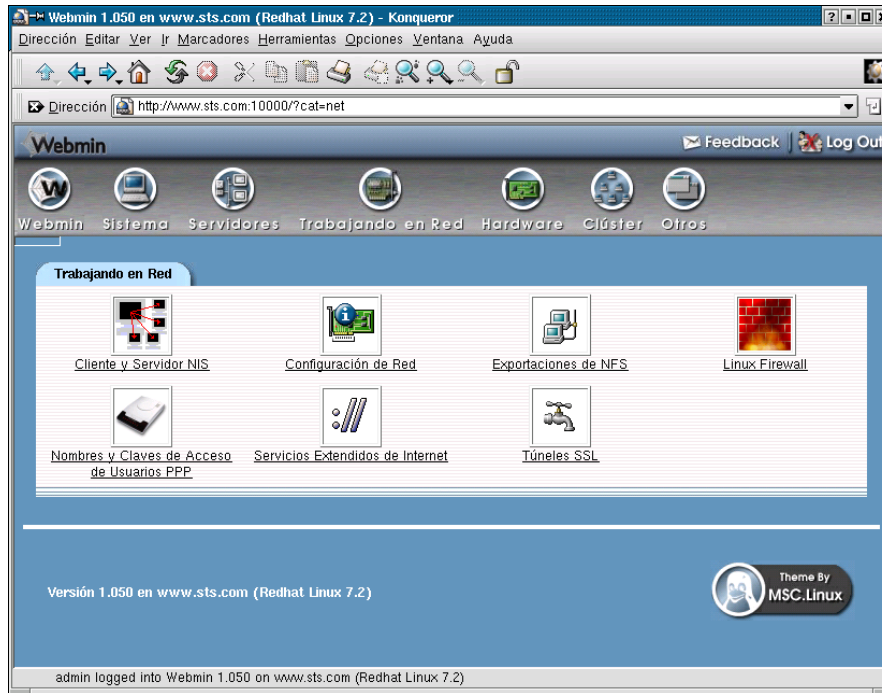
2.4.3. OPCIONES DE PESTAÑA DE SERVIDORES

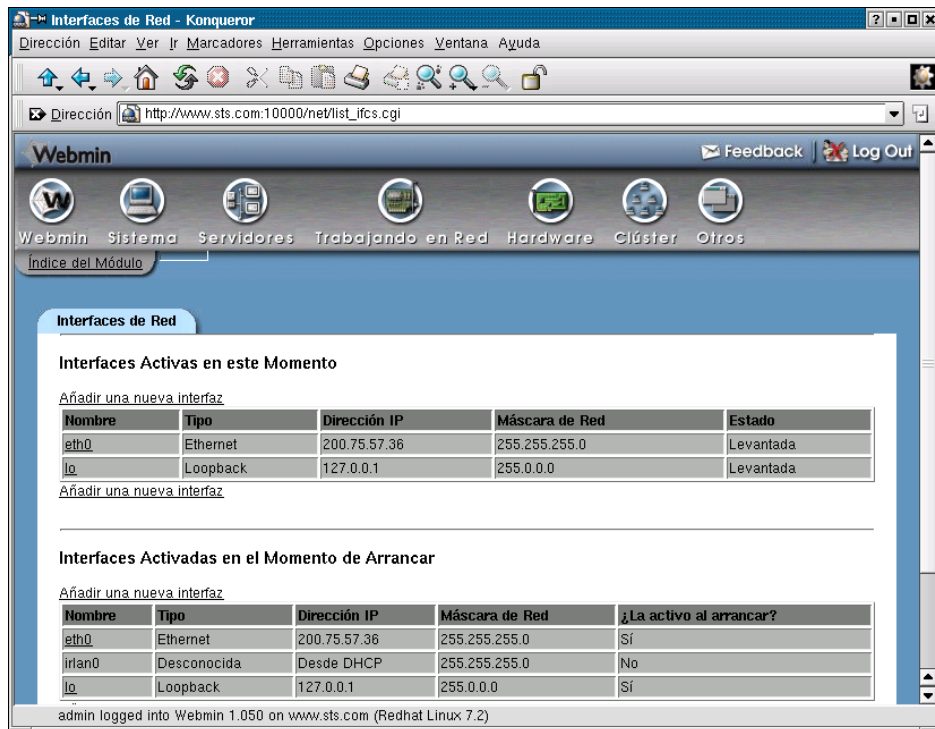
En la pestaña de servidores se tiene acceso a la configuración de los servicios de Linux disponibles, tales como : samba, sendmail , autenticación, ssh, DNS , ftp, postgresql, etc.



2.4.4. OPCIONES SISTEMA DE PESTAÑA DE RED

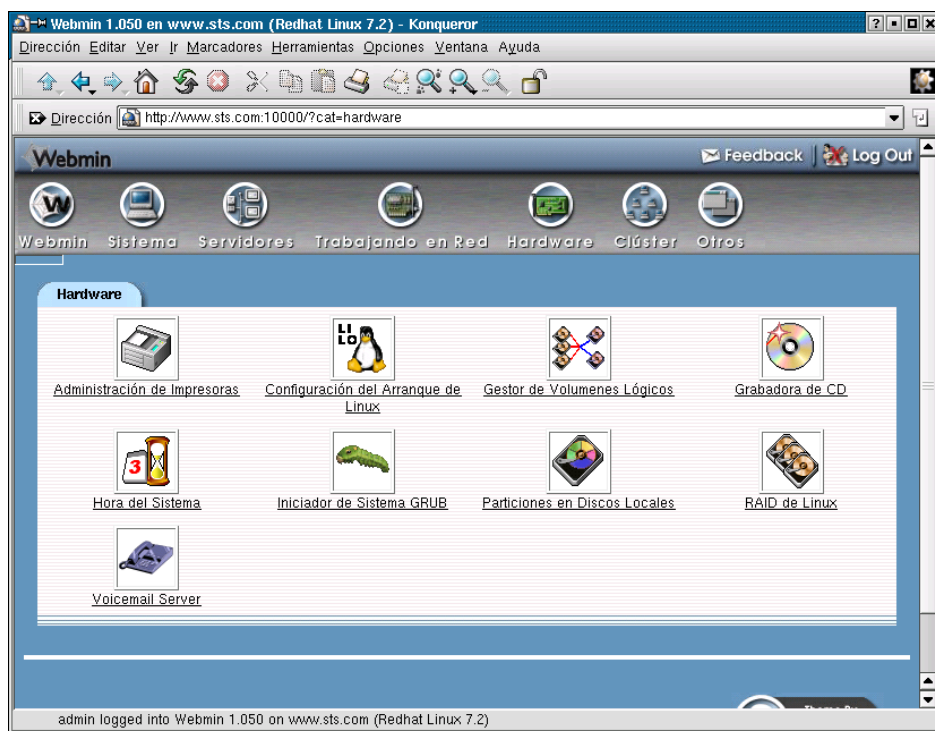
En la pestaña de trabajando en red, podemos hacer administración de los parámetros para trabajo con redes locales.





2.4.5. OPCIONES DE PESTAÑA DE HARDWARE

Desde pestaña de Hardware, podemos configurar impresoras, particiones de disco, manejo de arreglos de disco, etc.



2.4.6. PARA COMPLEMENTAR

Hacer un recorrido por las diferentes opciones del webmin, sistema, servidores y demás. Responder algunas preguntas :

- En que parte se pueden programar tareas para que corran periódicamente en el sistema.

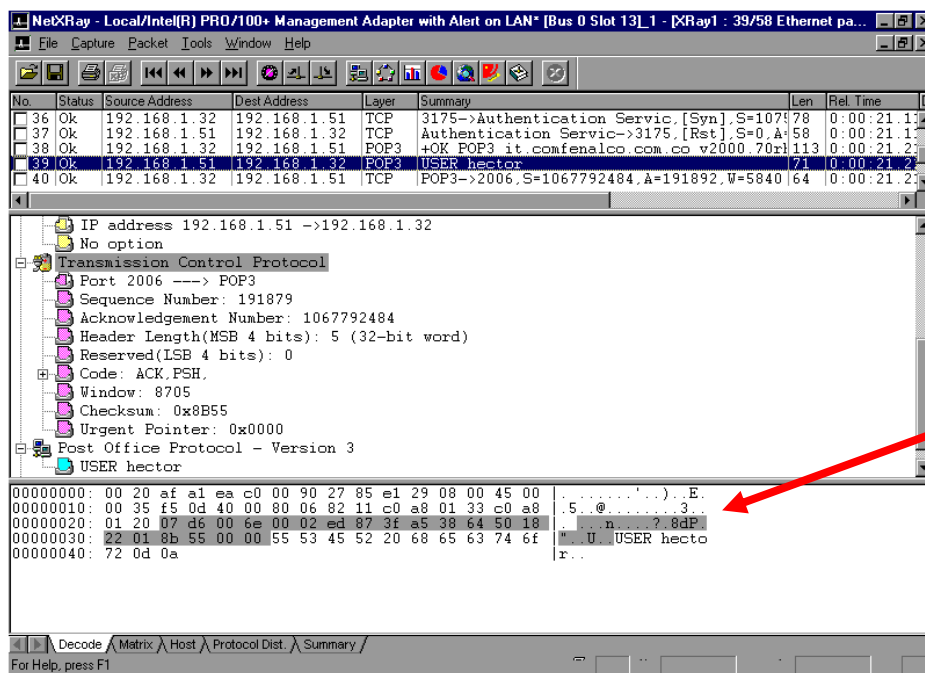
- Puedo limitar a que el acceso al webmin se haga solo desde algunas máquinas? En que parte?
- Como puedo hacer un backup programado de alguna partición del sistema.

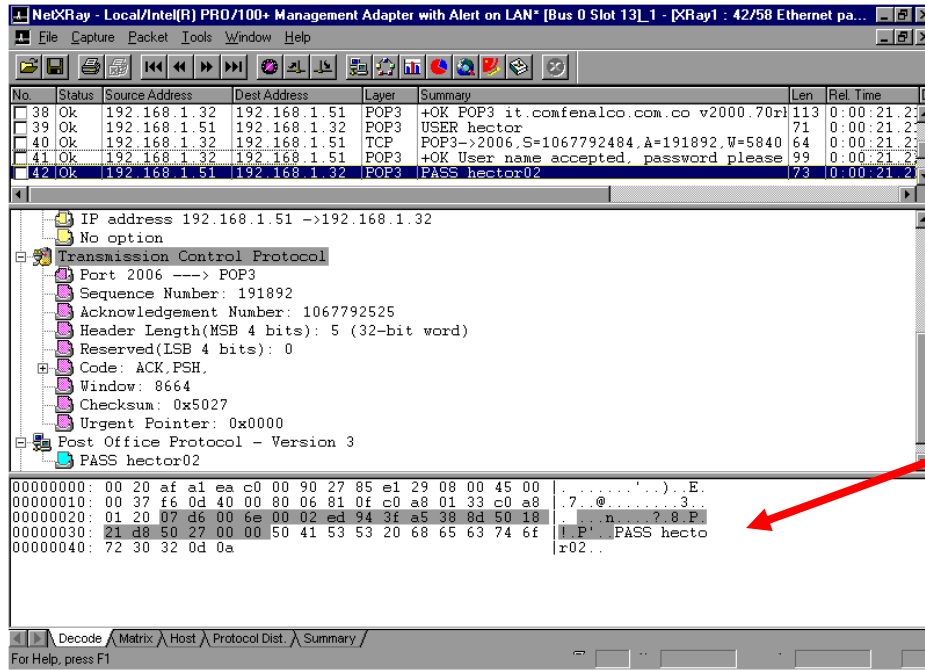
2.5. USO DE UN SNIFFER

El objetivo de este módulo no es explicar este tipo de herramientas, pero debemos conocer su función básica para algunas pruebas que realizaremos en los talleres. Cuando esta herramienta actúa como sniffer, puede ver el tráfico y contenido de los paquetes que viajan por la red, y así observar información que debería ser confidencial.

2.5.1. NETXRAY EN WINDOWS

Por ejemplo , si se desea ver el tráfico cuando los clientes se conectan al servidor para leer su correo electrónico, se puede con un sniffer detectar las cuentas y las claves respectivas, así como el contenido del correo en sí:



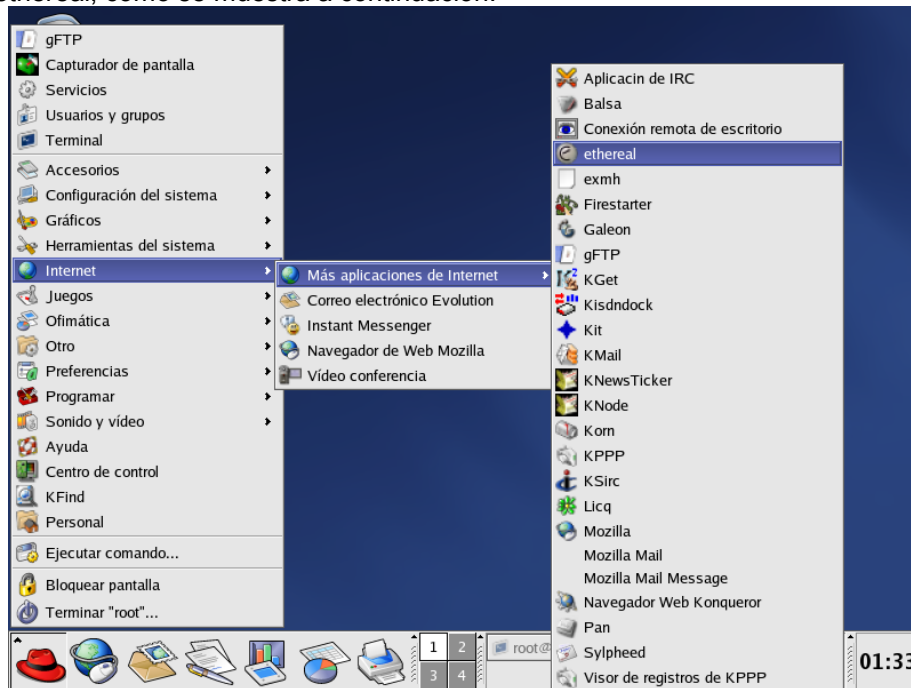


También podemos contar con el ethereal , cuyo instalador esta en el CD.

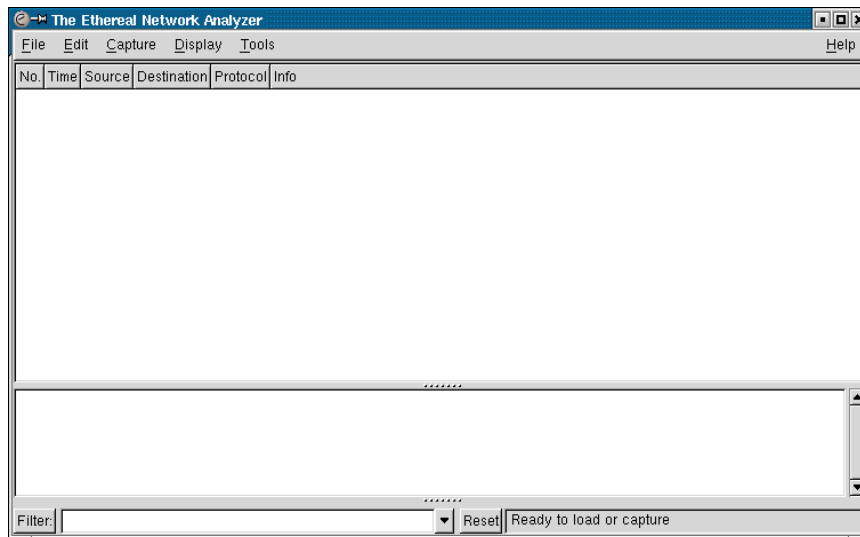
2.5.2. ETHEREAL EN LINUX

En linux disponemos del comando ethereal, que es una solución muy potente para hacer seguimiento de red ethernet, permitiendo capturar y analizar el tráfico de la red en modos de tiempo real o fuera de linea. Proporciona una interfaz GUI robusta para hacer más sencilla y eficiente la captura.

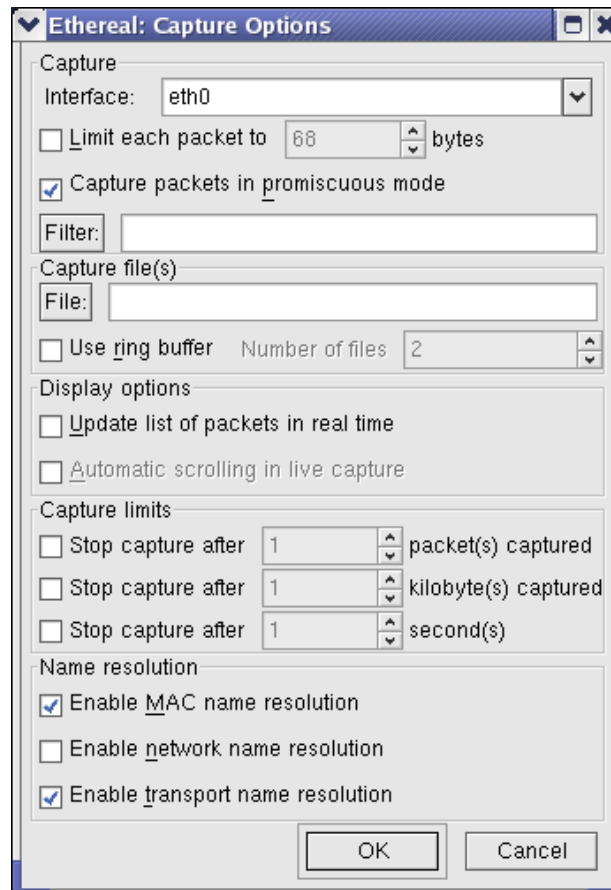
Para acceder la herramienta debemos ir a la opcion internet/mas aplicaciones de internet/ethereal, como se muestra a continuación.

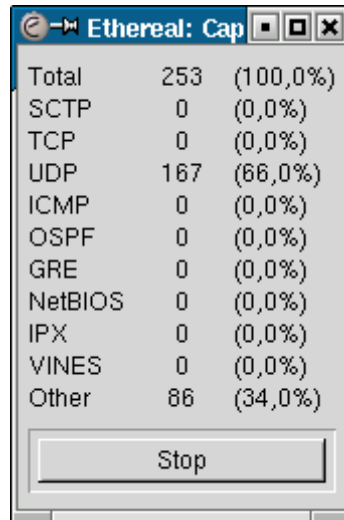


Se abre una ventana, desde la cual podemos iniciar la captura de paquetes.

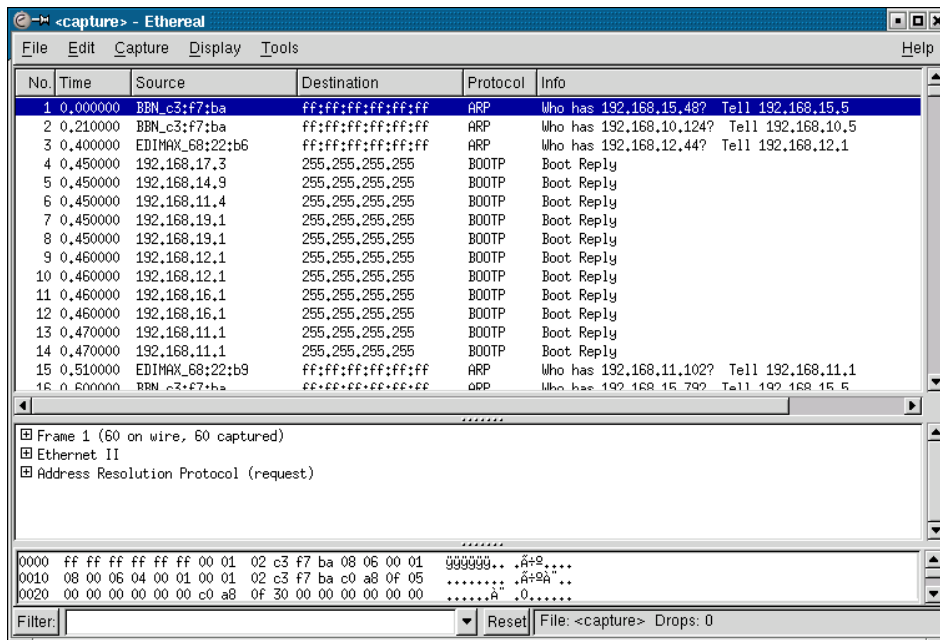


Al indicarle que arranque la captura de paquetes, aparece una nueva ventana, donde indicamos por cual interface vamos a revizar tráfico, y otras opciones. Al aceptar con OK, se inicia la captura y se van mostrando el contador de paquetes capturados, hasta que decidamos detener la captura.





AL detener la captura , se procesan los datos y se muestra una pantalla con la secuencia de paquetes y allí procedemos a revisarlos.



2.5.3. PARA COMPLEMENTAR

En Linux, por servicios, iniciar el servicio de telnet y vsftpd. Crear un usuario para que una persona desde otro equipo haga una conexión a la máquina linux, tipo telnet y ftp con el usuario y clave creado. Antes de que esto ocurra, abrir el sniffer y capturar datos. Cuando la conexión de telnet y ftp terminen, cerrar el sniffer y buscar donde queda registro del nombre del usuario y clave digitada.

3.CONFIGURACION DE SERVICIOS DE INTERNET EN LINUX

3.1. QUE ES INTERNET

Internet es la Red de Redes, una poderosa herramienta de comunicación. Puede ser un prototipo de una gran red que reúne la mayoría de redes del mundo y conforman la llamada “Superautopista de Información” y puede entregar temas de educación, negocios, ventas, entretenimiento, etc a sus usuarios en sus propios Computadores.

3.2. COMO FUNCIONAN LOS DIFERENTES SERVICIOS EN INTERNET

Internet funciona totalmente con esquema cliente-servidor y así trabajan todos los servicios que ofrece. Siempre hay un servidor que escucha los requerimientos del usuario (cliente) y le entrega la información relacionada con el requerimiento.

Hay una gran gama de servicios a través de internet, pero vamos a tratar los principales o más comunes.

3.3. DOMAIN NAME SERVICE (SERVIDORES DNS)

En vez de utilizar la dirección IP completa de 32 bits, muchos sistemas adoptan nombre más significativos para sus dispositivos y redes. Por lo general los nombres de las redes reflejan el nombre de la organización (ejm. Procalculo.com). Los nombre individuales de los dispositivos de la red pueden ir desde nombre descriptivos en redes pequeñas (como laser1, oracle1, servnt), a convenciones de asignación de nombres complejos en redes más grandes. La conversión entre estos nombre y las direcciones IP sería prácticamente imposible a escala total de internet.

A fin de resolver el problema de los nombres de red, el NIC mantiene una lista de los nombres de red y de las direcciones correspondientes de los enrutadores de la red. Este sistema creció desde una lista sencilla (archivo plano) en la cual se buscaban coincidencias a un sistema más complejo conocido como Sistema de Nombre de Dominio (Domain Name System - DNS), cuando las redes se hicieron demasiado numerosas para que el sistema de archivo plano funcionara eficazmente.

El DNS utiliza una arquitectura jerárquica, muy parecida al sistema de archivos UNIX. El primer nivel de asignación de nombre divide las redes en categoría de subredes, como com para comercial, mil para militar, edu para educativo, etc. Por debajo de cada una de estas se encuentra otra división , que identifica a la subred individual, por lo general una para cada organización. Esta se conoce como nombre de dominio y es única. El administrador de sistemas de la organización puede dividir aún más las subredes de la empresa según desee, con cada red identificada como subdominio.

Inicialmente, el NIC ha establecido seis nombres de dominio de primer nivel. Estos eran :

.arpa	Una identificación ARPAnet-Internet
.net	Para proveedores
.com	Empresa comercial
.edu	Institución educativa
.gov	Cualquier organización gubernamental
.mil	Militar
.org	Cualquier otra cosa que no caiga en ninguna de las categorías anteriores.

En la actualidad se han adicionado más categorías de nombres de dominio.

El NIC permite agregar un indicador de país. Hay indicadores para todos los países, como .CA para Canadá, .UK para el reino unido, .CO para Colombia.

El DNS utiliza dos sistemas para establecer y controlar los nombres de dominio. En cada red un resolver de nombres examina la información incluida en un nombre de dominio. Si no puede determinar la IP completa, consulta a un servidor de nombres que tiene disponible toda la información del NIC. Ese resolver de nombres trata de completar la información de direccionamiento mediante su propia base de datos, la cual actualiza de una forma muy parecida a la del sistema ARP, cuando se debe consultar a un servidor de nombres. Si el servidor de nombres que se consulta no puede convertir la dirección, consulta a otro servidor de nombres y así sucesivamente, a través de toda la internet. El resolver es la parte cliente del DNS.

Cada servidor de nombres DNS administra un área distinta de una red (o todo un dominio si la red es pequeña). El conjunto de máquinas administradas por el servidor de nombres se conoce como zona. Un servidor de nombre puede administrar varias zonas. En el interior de cada zona casi siempre hay asignado un servidor de nombre secundario o de respaldo, ambos (primario y secundario) conteniendo información duplicada. Los servidores de nombre dentro de una zona se comunican mediante un protocolo de transferencia de zona.

DNS opera con un conjunto de zonas anidadas. Cada servidor de nombre se comunica con el que esta encima de él (y, si lo hay, con el servidor de nombre bajo él). Cada zona tiene por lo menos un servidor de nombre responsable de conocer la información de direcciones de cada máquina dentro de dicha zona. Cada servidor de nombre también conoce las direcciones de por lo menos otro servidor de nombre. Los mensajes entre servidores de nombre por lo general utilizan el Protocolo de Datagrama de Usuario (UDP) porque su método sin conexión da un mejor rendimiento. Sin embargo, debido a su confiabilidad, para las actualizaciones de las bases de datos se emplea TCP.

Cuando una aplicación de usuario necesita convertir un nombre simbólico a una dirección de red, la aplicación envía una consulta al proceso de conversión, el que enseguida comunica la consulta al servidor de nombre. Este a su vez consulta sus propias tablas y devuelve la dirección de red correspondiente al nombre simbólico.

Cuando un servidor de nombre recibe una consulta de un resolver, hay varios tipos de operaciones que aquel puede realizar : recursivas y no recursivas. Una operación recursiva es aquella en la cual el servidor de nombre debe acceder otro servidor de nombre para obtener la información.

Las operaciones no recursivas realizadas por el servidor de nombre incluyen una respuesta correcta a la solicitud echa, una referencia a otro servidor de nombre o un mensaje de error.

Cuando se requiere una operación recursiva, el servidor de nombre entra en contacto con otro servidor de nombre con la solicitud del resolver. El servidor de nombre remoto contestará a la solicitud ya sea con una dirección de red o con un mensaje negativo indicando la falla. Las reglas del DNS prohíben a un servidor de nombre remoto enviar una referencia a otro servidor de nombre.

Registro de recursos.

El servidor de nombre mantiene en un conjunto de registros de recursos, la información que se requiere para convertir nombres simbólicos ; dichos recursos (a menudo abreviados RR), son entrada en una base de datos y contienen información en formato ASCII. El formato de los registros de recursos aparece en la siguiente tabla :

Nombre (Longitud variable)
Tipo (16 bits)

Clase (16 bits)
TTL (32 bits)
Longitud de datos (16 bits)
Datos (Longitud variable)

El campo de nombre es el nombre del dominio de la máquina a la cual se refiere el registro. Si no se ha especificado el nombre, se sustituye con el nombre previamente utilizado. El campo tipo identifica el tipo de registro de recurso. Los registros de recurso se utilizan para diferentes fines, como nombres para mapeo a direcciones y zonas definitorias. Este tipo se identifica mediante un código mnemónico o un número, los cuales aparecen a continuación.

Número	Código	Descripción
1	A	Dirección de Red
2	NS	Servidor de nombre con autoridad
3	MD	Destinatario de correo, ahora se conoce como MX
4	MF	Remitente de correo, ahora se conoce como MX
5	CNAME	Nombre de alias canónico
6	SOA	Inicio de autoridad de zona
7	MB	Nombre de dominio de buzón
8	MG	Miembro de buzón
9	MR	Dominio de cambio de nombre de correo
10	NULL	Registro de recurso nulo
11	WKS	Servicio bien conocido
12	PTR	Apuntador a nombre de dominio
13	HINFO	Información de anfitrión
14	MINFO	Información de buzón
15	MX	Intercambio de correo
16	TXT	Cadenas de texto
17	RP	Persona responsable
18	AFSDB	Servicios tipo AFS
19	X.25	Dirección X.25
20	ISDN	Dirección ISDN
21	RT	Enrutar a través de

El campo de clase en el diseño de registro de recursos contiene un valor para la clase de registro. Si no se especifica ningún valor se sustituye la última clase utilizada. Los servidores de nombre internet normalmente emplean el código IN. El campo de tiempo de vida (TTL) especifica la cantidad de tiempo en segundos que el registro de recursos es válido en el caché. Si se emplea el valor de 0, el registro no se deberá añadir al caché.

La sección de datos del registro de recursos contiene dos pares, formadas por la longitud de registro y por los datos mismos. El campo de longitud de datos especifica la longitud de la sección de datos. Los datos son un campo de longitud variable (de ahí la necesidad de un valor de longitud) que describe de alguna forma la entrada. El empleo de este campo difiere según los distintos tipos de registro de recursos.

El formato de registro de recursos inicio de autoridad (SOA) se utiliza para identificar las máquinas que están dentro de una zona. Existe un sólo registro SOA en cada zona. El formato del campo de datos SOA aparece en la siguiente tabla. Los campos en el registro de recursos SOA se emplean principalmente para administración y mantenimiento del servidor de nombres.

Nombre de Dominio (MNAME)
Nombre del responsable (RNAME)
Serie
Tiempo de regeneración
Tiempo de reintento
Tiempo de expiración

Tiempo mínimo

El campo MNAME es el nombre del dominio de la fuente de los datos para la zona. El campo RNAME es el nombre del dominio del buzón del administrador de la zona. El campo serie contiene el número de versión de la zona. Se incrementa al cambiarse la zona ; de lo contrario, se conserva el valor para todos estos mensajes.

El tiempo de regeneración es el número de segundos entre la regeneración de datos para la zona. El tiempo de reintento es el número de segundos a esperar entre solicitudes de regeneración no exitosas. El tiempo de expiración es el número de segundos después de los cuales la información de zona ya no tiene validez. Finalmente el tiempo mínimo es el número de segundos que se utilizara en el campo de tiempo de vida de los registros de recursos en el interior de la zona.

In-addr-arpa

Los campos de dirección , como el tipo de registro de recursos de dirección, utilizan un formato especial llamado IN-ADDR-ARPA . Esto permite el mapeo inverso, de la dirección al nombre del anfitrión, así como el mapeo de la dirección del anfitrión. A fin de comprender esto, es útil empezar con un registro de recursos de formato estándar. Uno de os tipos de registro de recursos más sencillo corresponde a la dirección (tipo A), ejm :

hgt	IN	A	200.3.244.20
opr	IN	A	200.3.244.21
sgi	IN	A	200.3.244.2
router	IN	A	200.3.244.1

Cada línea del archivo presenta un registro de recursos. En este caso todas son entradas simples que contienen el nombre simbólico de la máquina, la clase de la máquina (IN para internet), A para mostrar que se trata de un registro de recursos de dirección, y la dirección internet.

Este tipo de archivo facilita el mapeo nombre a dirección. El servidor de nombre simplemente busca una línea que tenga el nombre simbólico solicitado por la aplicación y devuelve la dirección internet en el extremo de dicha línea.

La búsqueda partiendo de la dirección hacia el nombre no es tan fácil. Si los archivo de registros de recursos son pequeños, los retrasos de tiempo para una búsqueda manual no serán apreciables ; pero en zonas grandes podrían existir decenas de miles de entradas . El índice está por nombre y debido a ello la búsqueda de una dirección resultará un proceso lento. IN-ADDR-ARPA se desarrolló para resolver este problema de mapeo inverso. IN-ADDR-ARPA utiliza la dirección del anfitrión como índice para la información del registro de recursos del anfitrión. Cuando se localiza el registro de recursos apropiado, se puede extraer el nombre simbólico.

IN-ADDR-ARPA utiliza el tipo de registro de recursos PTR, para apuntar de la dirección al nombre. Puede haber uno de estos índices de apuntador en cada servidor de nombre. A continuación se muestra un ejemplo de un archivo de número a nombre .

20.244.3.200	PTR	hgt.www.psa.com.
21.244.3.200	PTR	opr.www.psa.com.
2.244.3.200	PTR	sgi.www.psa.com.
1.244.3.200	PTR	router.www.psa.com.

No es necesario colocar la dirección completa de las máquinas , ya que en el archivo de definición se coloca una entrada para IN-ADDR-ARPA con la dirección invertida de la red. Se podría tener el mismo archivo así :

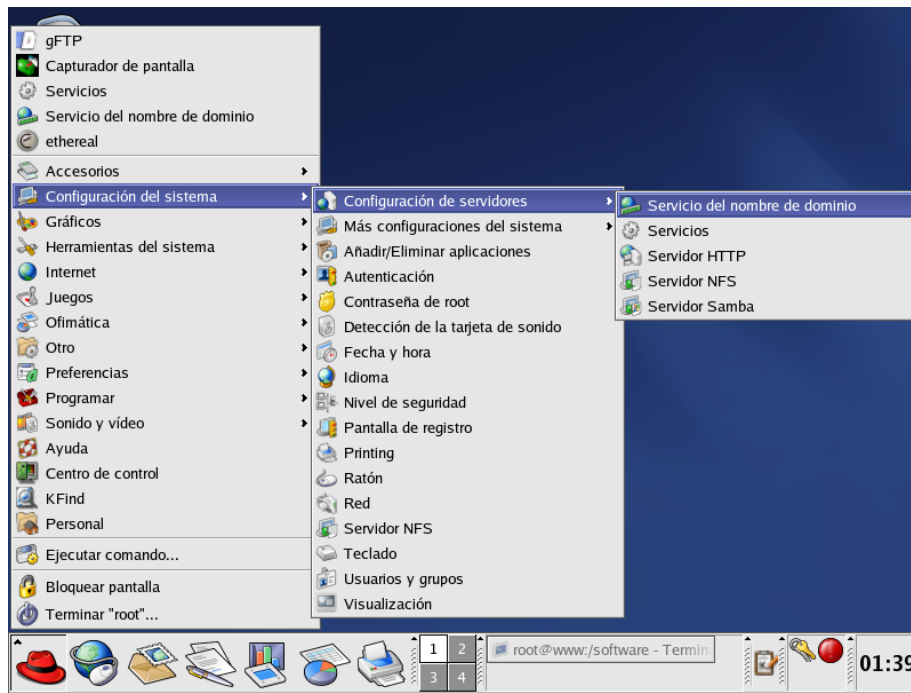
20	PTR	hgt.www.psa.com.
21	PTR	opr.www.psa.com.
2	PTR	sgi.www.psa.com.
1.	PTR	router.www.psa.com.

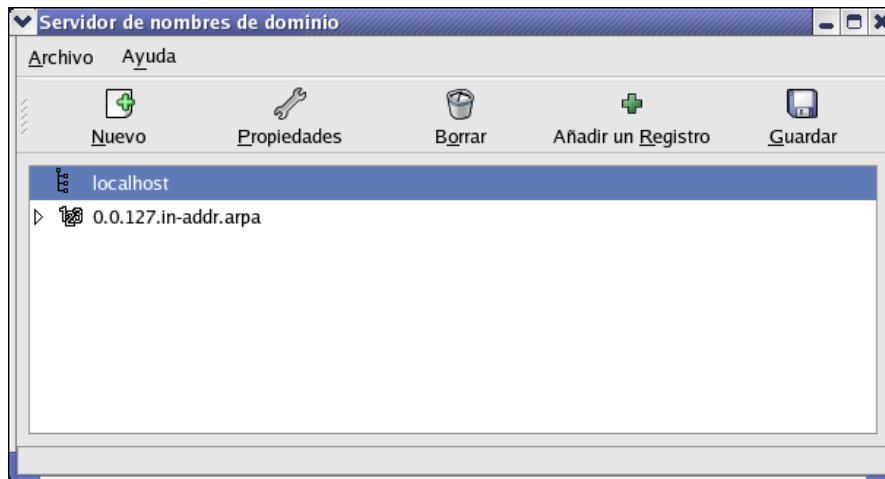
Afortunadamente , ya existen muchos interfaz gráficos que facilitan la configuración de estos servicios, y no hay que hacer manipulación directa de los archivos, aunque es muy importantes conocerlos, pues en algunas labores , es más rápido hacer las actualizaciones directamente sobre estos.

3.3.1.CONFIGURACIÓN DEL SERVIDOR DNS

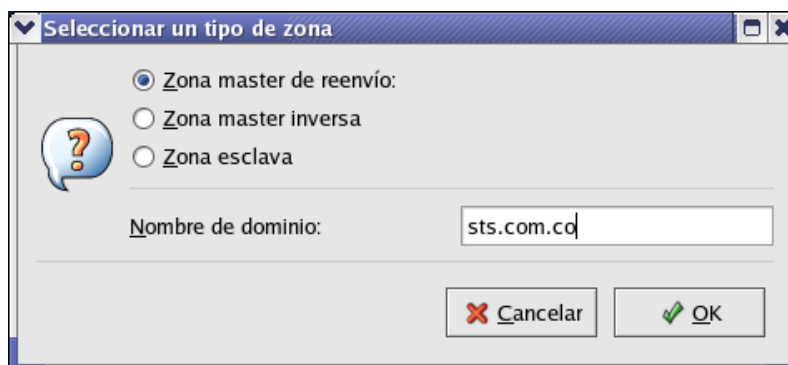
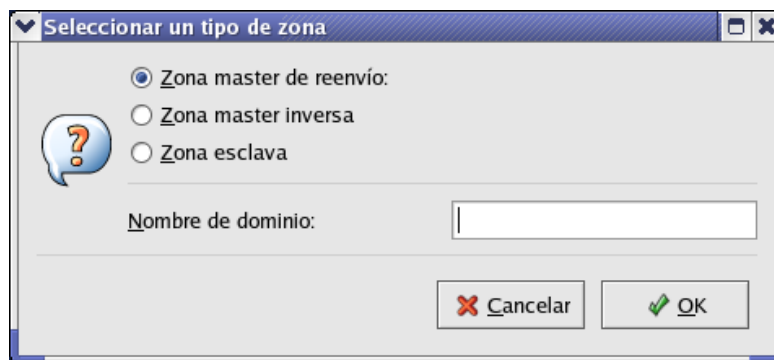
Para configurar este servicio se puede hacer desde :

- Configuración del Sistema
 - Herramienta Webmin
 - Manipulación directa de los archivos
- Configuración del Sistema (Servicio de Nombre de Dominio)

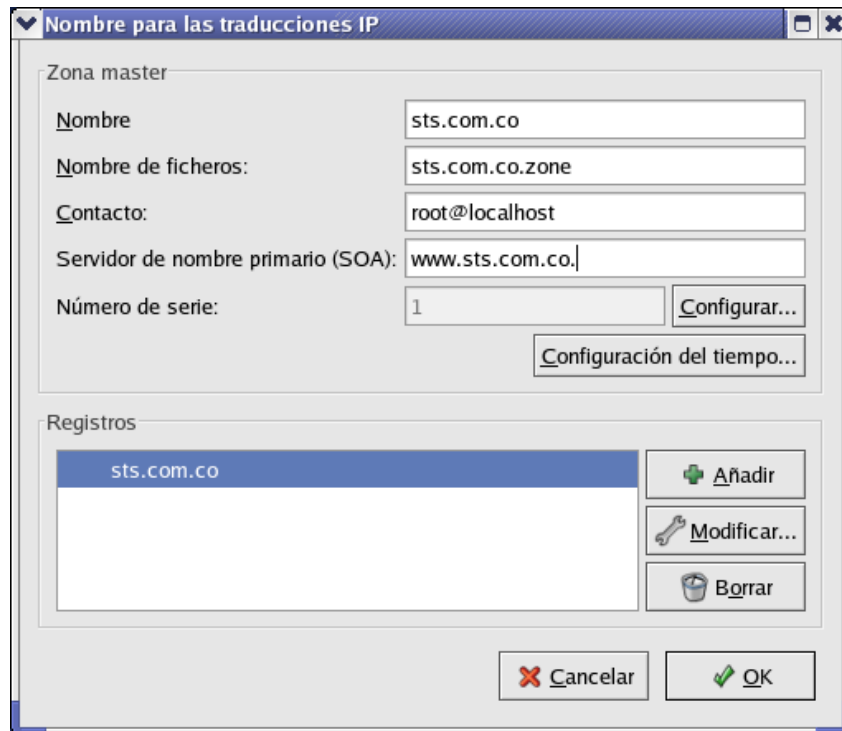




Inicialmente solo aparece la zona inversa del interfaz loopback. Se debe proceder a crear la zona maestra del dominio y la zona inversa. Se escoge añadir:

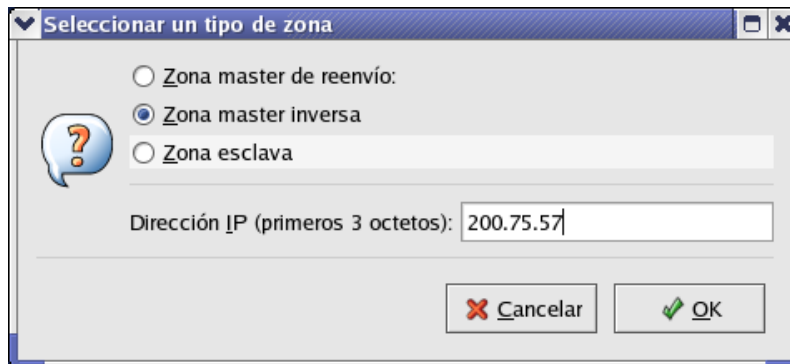


Luego se selecciona Zona maestra de envío. Se debe suministrar la información del nombre del dominio que se va a resolver (ejm: www.sts.com), se puede aceptar el nombre por defecto para la lista de registros de esta zona , se debe dar la dirección del administrador de esta zona (en esta caso se dejó a root), y se le indica quién va a ser la máquina servidora de nombres para este dominio. Por ejemplo, la máquina www.sts.com, será la servidora de este dominio.

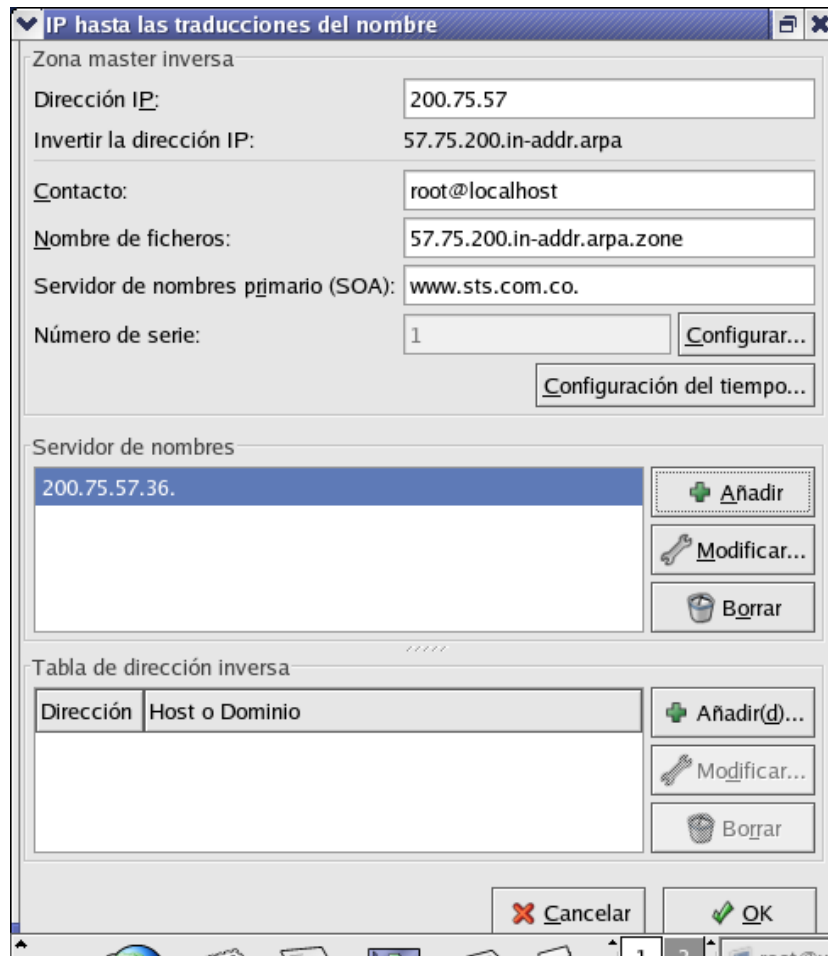


Luego se procede a crear la zona inversa, de nuevo entrando por añadir (la misma pantalla anterior), pero escogiendo la Zona maestra inversa.

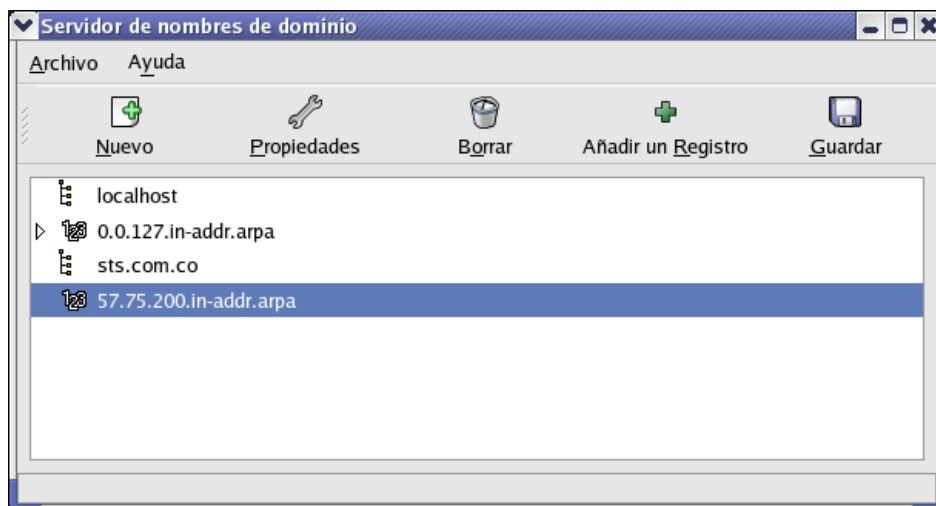
En lugar de dar el nombre del dominio se digita los tres primeros dígitos de la dirección de la red. Por ejemplo : 200.75.57



De nuevo hay que indicarle a esa zona quien es el servidor de nombres de la misma, por ejemplo : www.sts.com.



Deben de quedar las dos zonas configuradas.

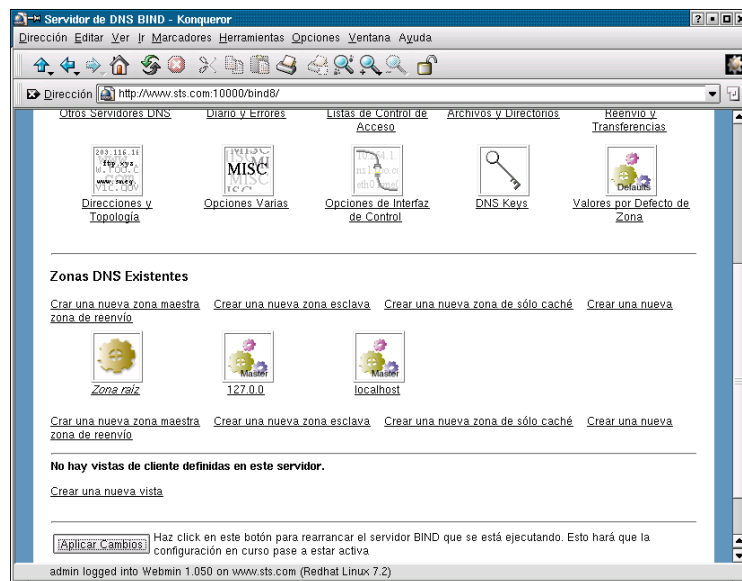
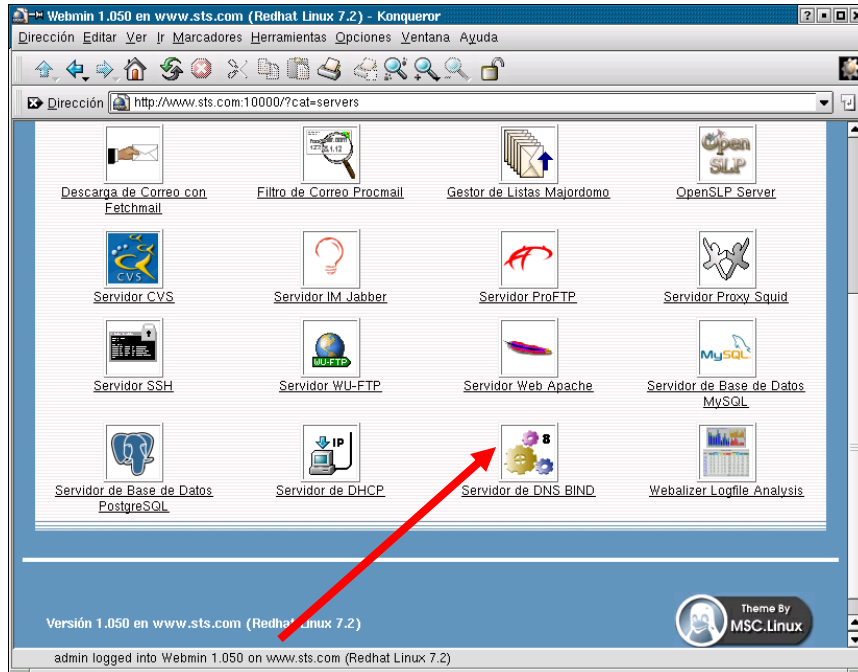


Se puede proceder a entrar a la zona creada y añadirle nombres de máquinas que pertenecen a la zona. Las pruebas respectivas las citaremos más adelante.

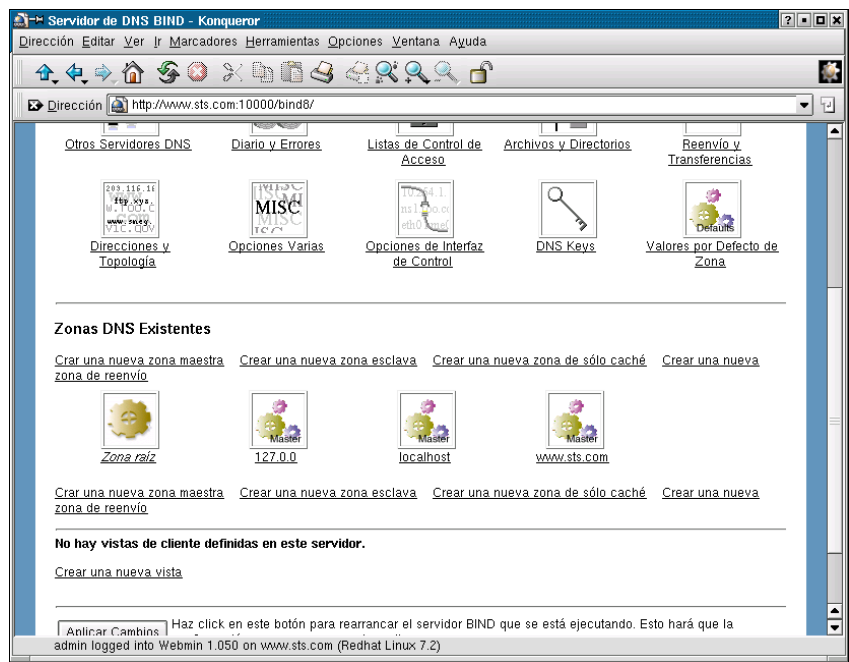
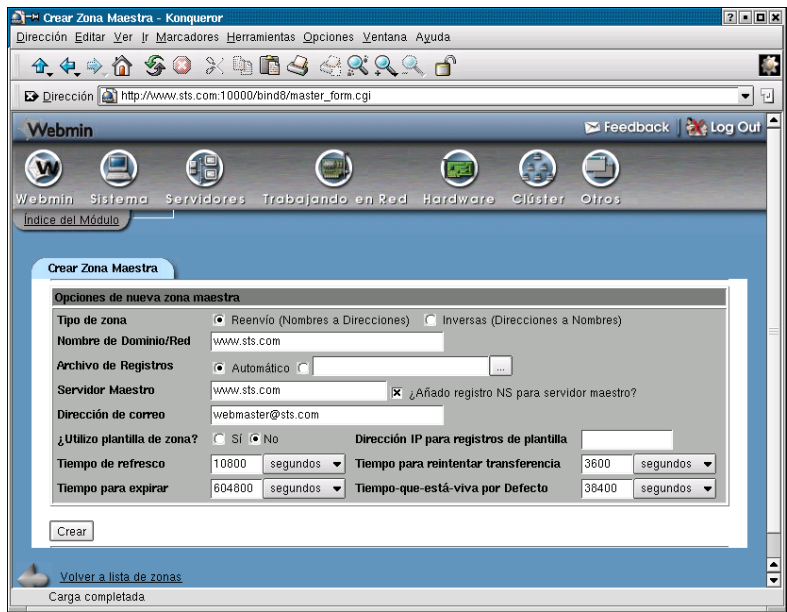
- **A través del interfaz Web Webmin**, por servidores , configuración de DNS (Bind 8)

El procedimiento es el mismo que por el panel de control. Se deben crear las zonas de reenvío y la inversa.

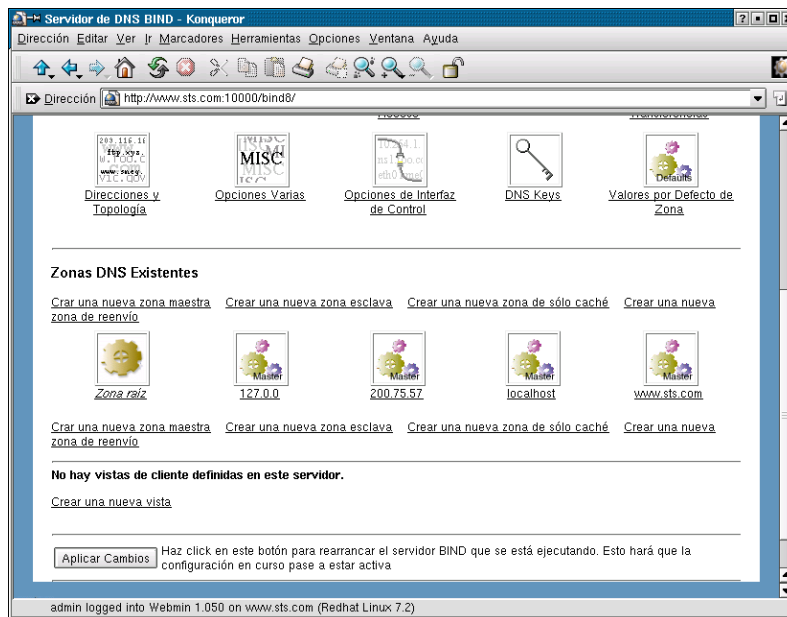
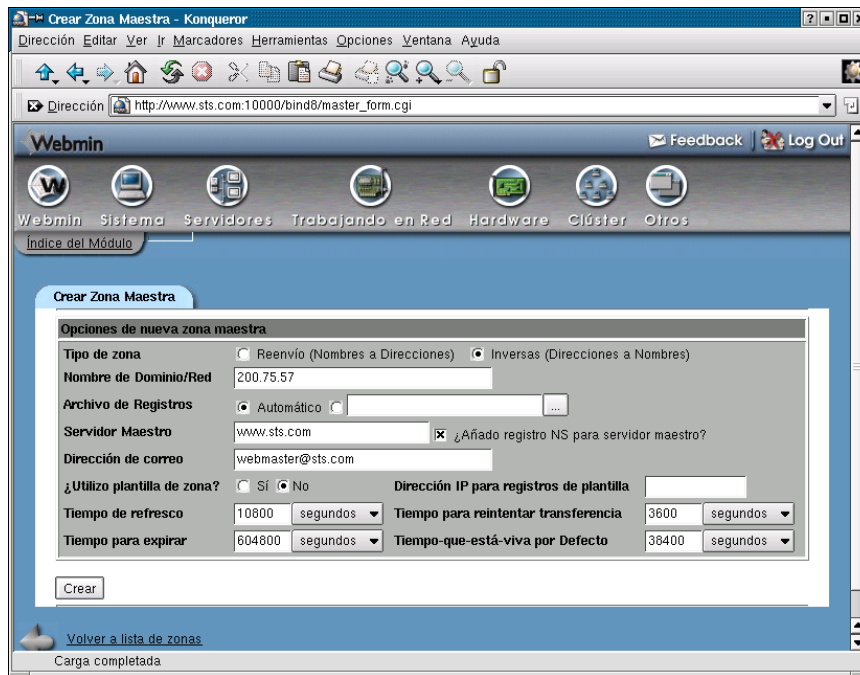
Para entrar al webmin, se debe dar en el navegador el nombre completo de la máquina y el puerto por el que escucha este interfaz. En esta máquina se dejó instalado y escuchando por el puerto 10000 (se accede con <http://192.168.1.1:10000>) . Se debe ir a servidores y luego a DNS (Bind 8). Allí aparece al final de la pantalla la lista de zonas creadas y las opciones de crear una nueva zona. Se escoge crear una zona maestra.



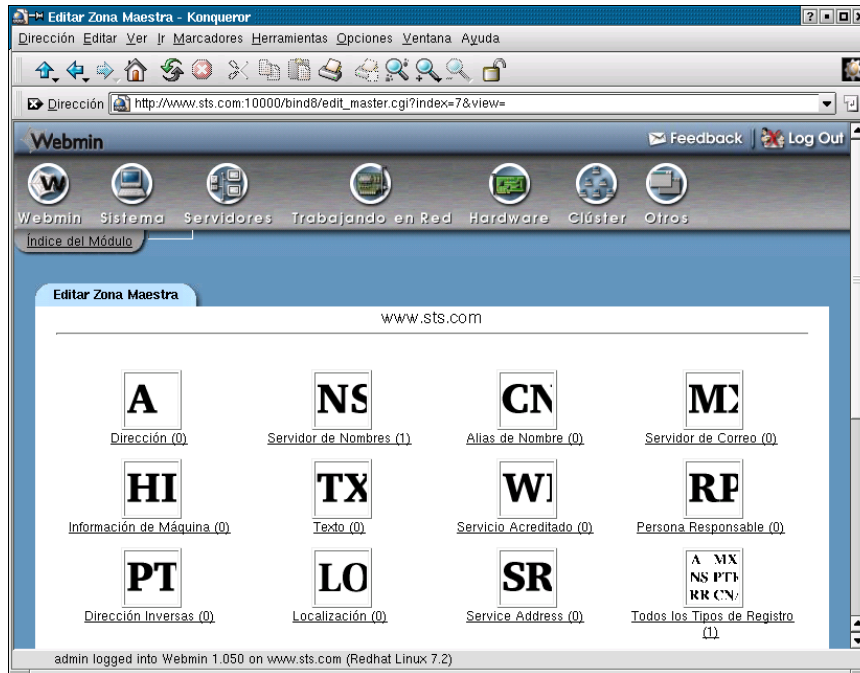
Se selecciona que la zona es de reenvío, se digita el nombre del dominio a trabajar (por ejemplo www.sts.com) , y se da el nombre del servidor (www.sts.com) , así como la cuenta de correo del administrador del DNS ([root@ www.sts.com](mailto:root@www.sts.com)) . Lo demás se deja por defecto.



Para la la creación de la zona inversa , se entra por la misma pantalla, pero se escoge botón de Inversa (al lado derecho superior) y se da los tres primeros dígitos de la IP de la red (200.75.57) en lugar del nombre del dominio.



Una vez creadas las zonas, para adicionar registros, nos situamos en la zona deseada y podemos escoger que tipo de registro adicionar:

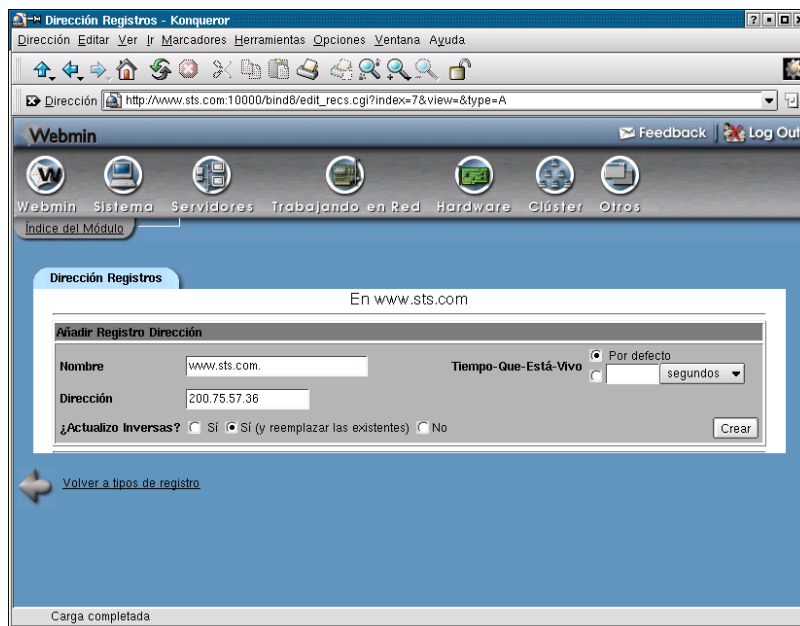


En el caso de la zona maestra, los nombre de máquinas se adicionan con registros tipo A , ya que estos son para adicionar nombres de máquinas y direcciones IP que pertenecen a la zona y que deseo resuelva el DNS.

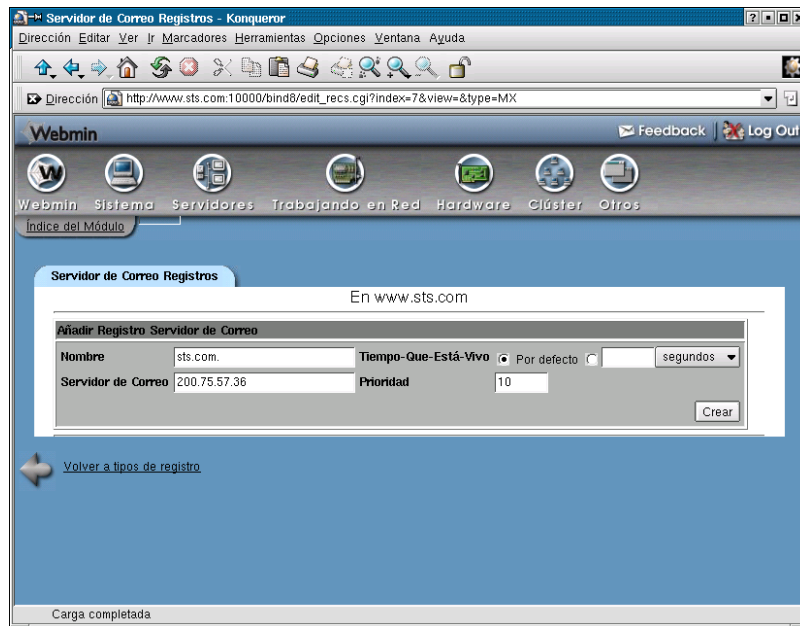
Los registros CNAME (icono CN) permite crear alias entre máquinas
 Los registros NS permiten definir el servidor DNS que atiende la zona.
 Los registros MX permiten definir el servidor de correo de esa zona (MX).

Como la zona inversa ya esta creada se le puede indicar que la actualice automáticamente con los registros correspondientes a esas entradas.

Se procede a crear un registro para el servidor www con la IP 200.75.57.36.



También se crea un registro de dominio para el servidor de correo (registro MX)



3.3.2. CONFIGURANDO LA PARTE CLIENTE DEL DNS

A nuestra máquina www y a las demás que vayan a utilizar como DNS a la máquina 200.75.57.36, hay que especificarle quien será el servidor DNS que la atiende en sus requerimientos (configurar parte cliente del DNS), y se hace por el interfaz webmin en la sección de trabajando en red o por linuxconf o editando el archivo /etc/ resolv.conf . El archivo debe quedar:

```
[root@it root]# cd /etc
[root@it etc]# hostname
www.sts.com
[root@it etc]# cat resolv.conf
domain sts.com
nameserver 200.75.57.36
```

Para reiniciar el servicio DNS se digita desde una ventana de comandos:

```
# service named stop
# service named start

o

# service named restart
```

3.3.3. PRUEBAS

Para poder probar que el DNS esta funcionando, debemos hacer dos cosas:

- Comprobar la resolución de nombres usando como servidor de nombres a www.sts.com (con el comando nslookup)
-

```
[root@it etc]# nslookup www.google.com
```

Note: nslookup is deprecated and may be removed from future releases.

Consider using the `dig` or `host` programs instead. Run nslookup with the `-sil[ent]` option to prevent this message from appearing.

Server: 200.75.57.36
Address: 200.75.57.36#53

Non-authoritative answer:

Name: www.google.com
Address: 216.239.37.101

Desde el comando nslookup se puede comprobar el correcto funcionamiento de varios servidores DNS, pues una vez invocado el comando, se puede definir cual es el servidor DNS con el que se desea trabajar. Se invoca el comando nslookup sin argumentos. Luego se define cual es el servidor DNS a usar y por ultimo se pregunta por la traducción de nombres de máquinas.

```
[root@www vsftpd]# nslookup
```

Note: nslookup is deprecated and may be removed from future releases.

Consider using the `dig` or `host` programs instead. Run nslookup with the `-sil[ent]` option to prevent this message from appearing.

```
> server 192.168.1.1
```

```
Default server: 192.168.1.1
```

```
Address: 192.168.1.1#53
```

```
> www.sts.com.co
```

```
Server: 192.168.1.1
```

```
Address: 192.168.1.1#53
```

```
Name: www.sts.com.co
```

```
Address: 200.114.1.72
```

3.3.4. ARCHIVOS INVOLUCRADOS

Los archivos de configuración involucrados en esta configuración residen en /etc y en /var/named y son (las nuevas versiones, mapean los archivos de /var/named a /var/named/chroot/var/named):

El archivo principal de configuración del servidor.

/etc/named.conf

```
[root@www etc]# cat named.conf
```

```
// generated by named-bootconf.pl
```

```
options {
    directory "/var/named";
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
};

//
// a caching only nameserver config
//
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
```

```

zone "." IN {
    type hint;
    file "named.ca";
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};

include "/etc/rndc.key";

zone "www.sts.com" {
    type master;
    file "/var/named/www.sts.com.hosts";
};

zone "57.75.200.in-addr.arpa" {
    type master;
    file "/var/named/200.75.57.rev";
};

```

Archivo /var/named/chroot/var/named/sts.com.hosts (de la zona maestra)

```

[root@www named]# cat sts.com.co.hosts

$ttl 38400
www.sts.com. IN      SOA   www.sts.com. webmaster.sts.com. (
                    1050378490
                    10800
                    3600
                    604800
                    38400 )
www.sts.com. IN     NS    www.sts.com.
www.sts.com. IN     A     200.75.57.36
sts.com. IN         MX    10 200.75.57.36

```

Archivo /var/named/ chroot/var/named/200.75.57.rev (de la zona inversa)

```

# cat 200.75.51.rev
$ttl 38400
57.75.200.in-addr.arpa. IN      SOA   www.sts.com. webmaster.sts.com. (
                              1050378541
                              10800
                              3600
                              604800
                              38400 )
57.75.200.in-addr.arpa. IN     NS    www.sts.com.

```

36.57.75.200.in-addr.arpa.	IN	PTR	www.sts.com.
----------------------------	----	-----	--------------

Una vez con el servicio DNS funcionando se puede proceder con el correo, web y otros. El registro del DNS debe estar activo y funcionando en la universidad de los Andes, para el caso de los dominios .co.

3.3.5 TALLER DE CONFIGURACIÓN DE SERVIDOR Y CLIENTES DNS

Teniendo en cuenta las direcciones de la sala, y nombres de algunas de las personas de los grupos de trabajo, se dividirá la sala en dos secciones: los de la izquierda que representarán al dominio izquierdo.edu.co y los de la derecha derecho.edu.co. Cada grupo debe configurar un servidor DNS que resuelva los nombres de los equipos de su sección. Los nombres finales de las máquinas, ante los DNS deben ser de la forma : carlos.derecho.edu.co (teniendo en cuenta escoger un nombre de alguno de los dos integrantes). Recordar que cada una de las máquinas también será cliente de ella misma. Al final el primer DNS que este funcionando correctamente , se tomará como DNS oficial para esa sección.

3.3.6. PARA COMPLEMENTAR

- En algunas situaciones se requiere que el servidor DNS , pase las peticiones que se le hagan y que el no pueda resolver a otro servidor DNS (hacer un forward). Como se puede hacer esto, por medio del webmin y editando el archivo principal. Que pruebas se pueden hacer?

3.4. CONFIGURACIÓN DEL SERVICIO WEB (WWW)

Word Wide Web: En este momento es el líder de los servicios internet. Es también conocido como WWW y permite acceder todos los servicios internet, de una forma gráfica. Se tiene acceso a vídeo, audio, etc. Es el servicio que más usuarios tiene.

Los Web Sites son colecciones de documentos que pueden ser hipertexto, gráficas, sonido, videos, y más. Frecuentemente ellos contienen enlaces a otros documentos web, o a otros web sites. Todos los web sites en el mundo están conocidos bajo el nombre de World Wide Web.

En este momento los servidores WWW se están convirtiendo en el mayor punto de presencia para los negocios en internet.

La Web "Home Page", que es la primera cosa que un usuario ve al entrar a un servidor web, mezcla el hipertexto para hacer atractiva la presentación y tentar al usuario a incursionar más en los temas presentados allí.

Los servidores WWW son accedidos usando un software llamado browser. Los mas populares son el Explorer de Microsoft y el Netscape. Linux posee uno llamado Konqueror.

3.4.1.CONCEPTOS BÁSICOS DEL WEB

El web esta basado en una relación cliente - servidor. El programa cliente (un browser web) hace una petición de información, y el programa servidor la entrega.

Un protocolo es una secuencia de pasos que el computador toma cuando intercambia información con otro. El protocolo básico para internet es TCP/IP, pero para los diferentes servicios en internet existen protocolos que trabajan sobre el modelo TCP/IP.

Cuando los clientes en internet se conectan a servidores para enviar Email, grupos de lectura, o visitar web sites, ellos se comunican utilizando protocolos adicionales al TCP/IP. Cuando se usan múltiples protocolos en la comunicación, se organizan generalmente en niveles. TCP/IP es el nivel inferior en la comunicación internet y especifica exactamente como todos los datos son transferidos de un computador a otro. El siguiente nivel puede ser HTTP (HyperText

Transport Protocol), el cual especifica que tipo de comunicación e información se esta enviando entre un web site y su browser. HTTP es el que hace que web servers y web browsers hablen el mismo lenguaje. TCP/IP asegura que los mensajes sean enviados y devueltos.

Otros protocolos que trabajan sobre TCP/IP son :

- SMTP (Simple Mail Transfer Protocol for email).
- FTP (File Transfer Protocol for transferring files)

Los diferentes protocolos son manejados transparentemente por los clientes y servidores. Una persona puede ver que protocolo esta utilizando cuando digita la internet address, llamada URL, dentro del campo respectivo del browser (dirección)

Uniform Resource Locators (URLs) tiene el formato :

protocol ://computer/directory/file . Un ejemplo es :

http ://www.sts.com

La mayoría de los archivos en el web tienen la extensión html (HyperText Markup Language)

El protocolo para acceder el web es HTTP, tal que todas las URLs empiezan por http :// , como se ve en el ejemplo anterior y muchos browser lo toman como el protocolo por defecto.

Pero si se desea acceder un servidor FTP, se puede digitar:

<ftp://www.sts.com>

Los Web server son equipos que entregan paginas o actúan como servidores de clientes que hacen las respectivas peticiones. Este computador puede hacer esto pues esta corriendo un programa que habla HTTP y esta físicamente conectado a una red TCP/IP.

Cuando se instala un programa para que realice esta función, como el apache, o internet information server , usted especifica un directorio que contiene todos los archivos o páginas que se van a entregar a los clientes. Todos los directorios y subdirectorios debajo del contenido principal , también esta disponible para los clientes. Como se mencionaba anteriormente el tipo de contenido básico de un web site son los archivos HTML. Adicionalmente los web sites pueden contener programas que ejecuten tareas especiales para la gente que los visita. Por ejemplo un programa que revise un stock de elementos y precios, basado en la información previamente llenada por el usuario en una forma HTML.

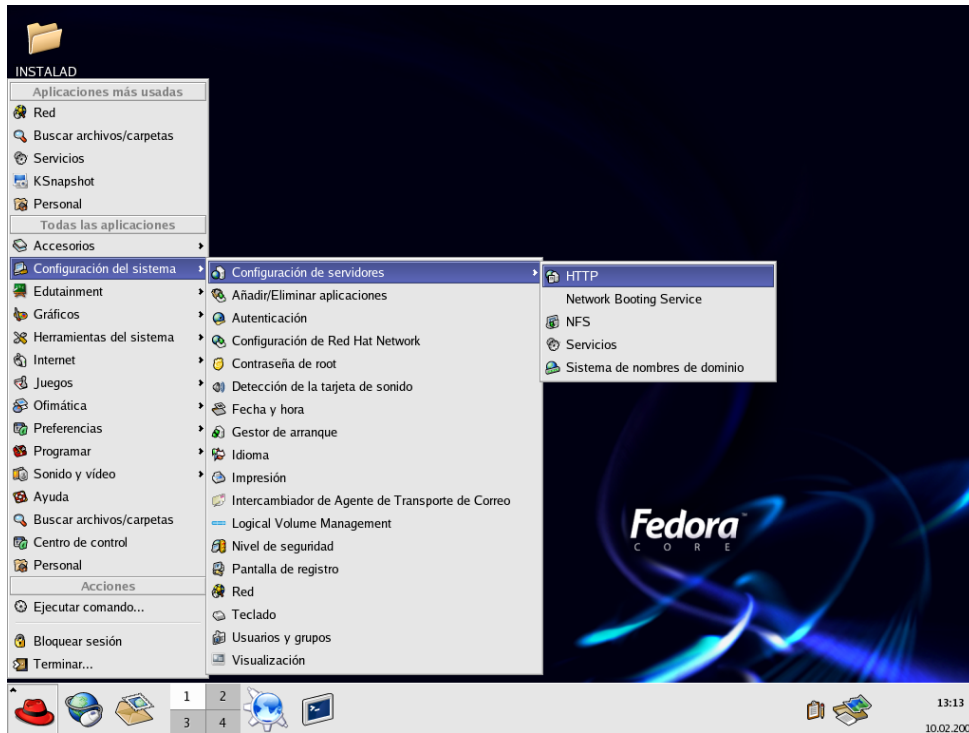
3.4.2. CONFIGURACIÓN DEL SERVIDOR WEB APACHE

Semejante al servicio DNS, se puede configurar de varias formas:

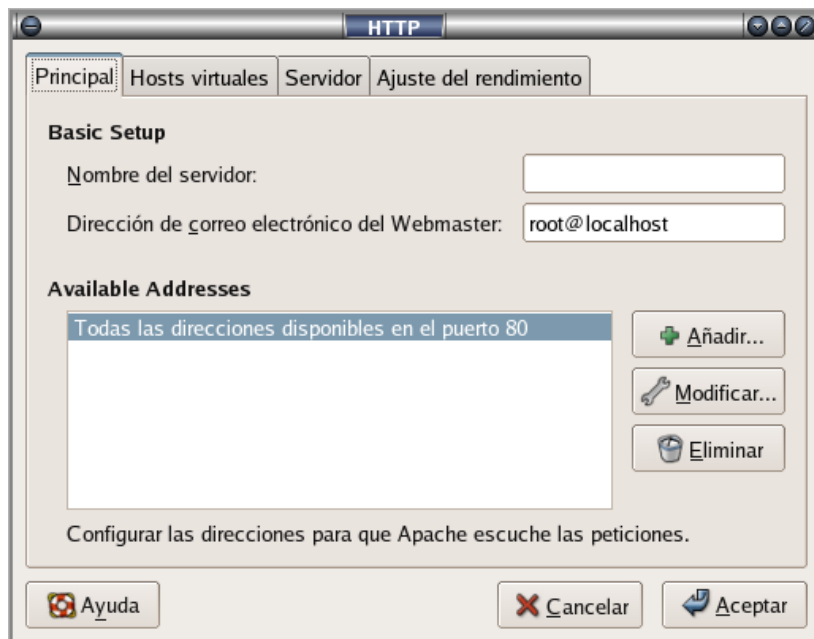
- Por las herramientas propias del sistema
- Por el webmin
- Manipulación directa de los archivos

3.4.2.1. POR HERRAMIENTAS PROPIAS DEL SISTEMA

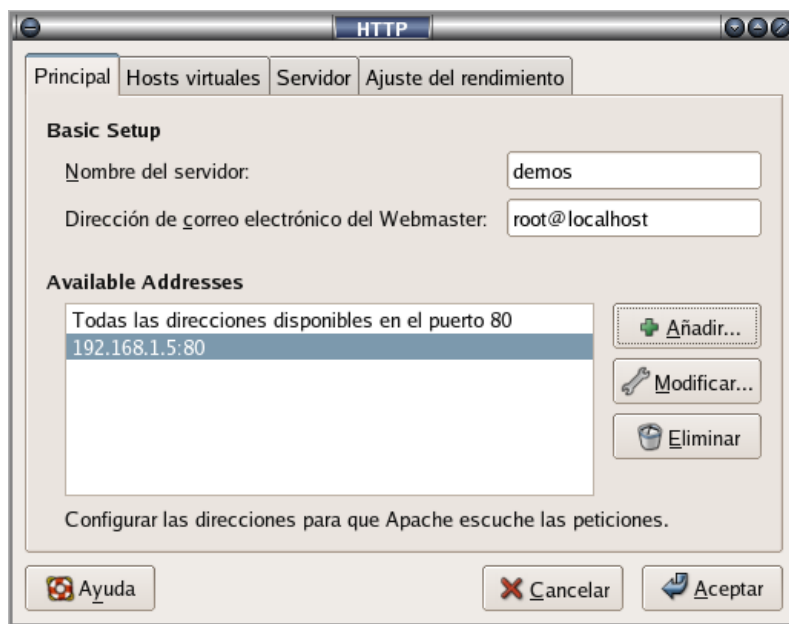
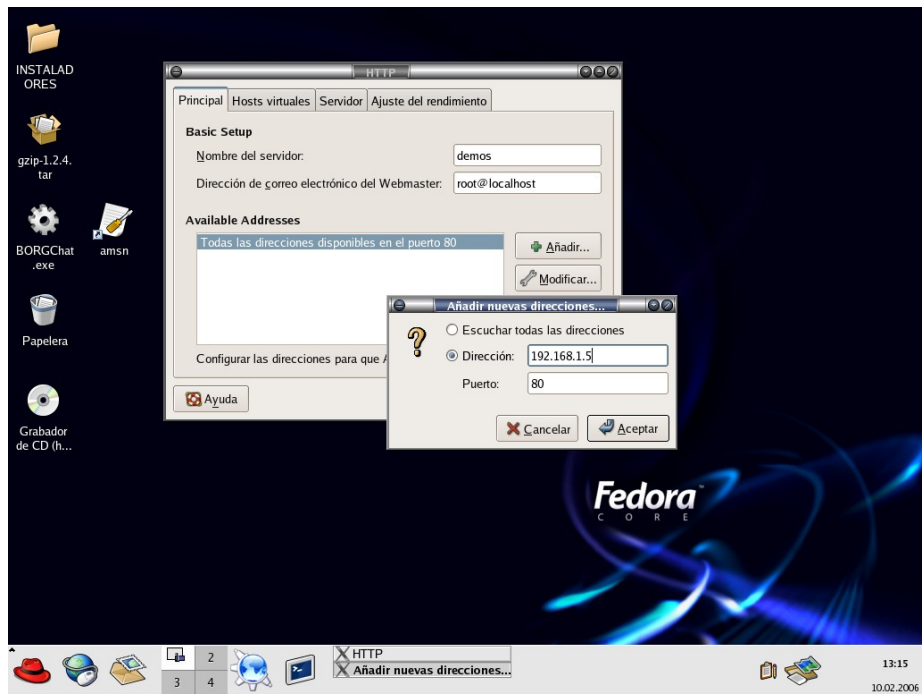
Se puede ingresar por el inicio, configuración del sistema, configuración de servidores y httpd.



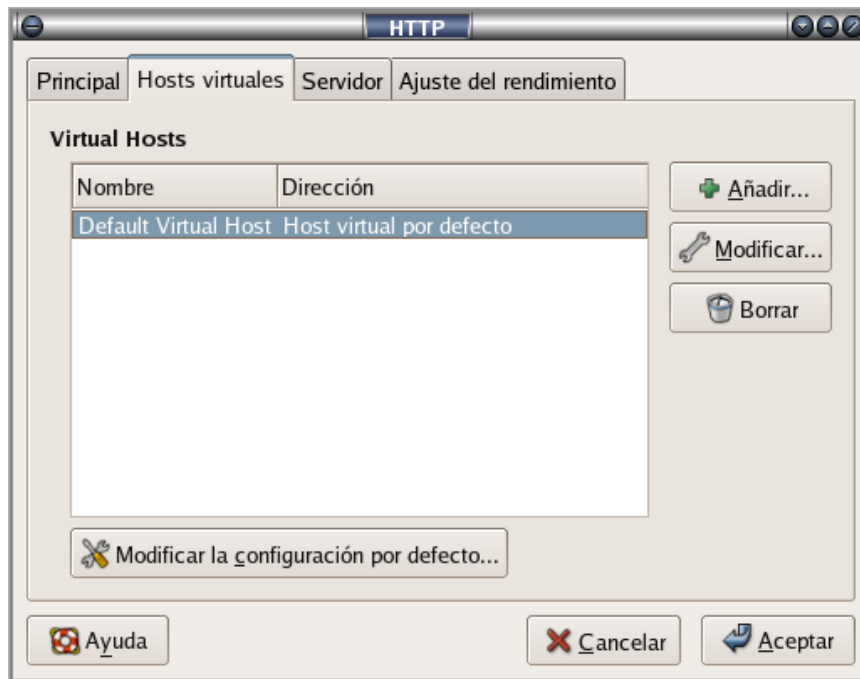
Esto mismo se puede lograr con el comando `system-config-httpd`.



Aquí, se puede hacer la configuración básica del servidor web. Si se le indica adicionar un servidor, se debe dar el nombre al que responderá, la dirección ip y el puerto.



Se pueden manejar host virtuales, y hacer ajustes en parámetros de rendimiento.



3.4.2.2. POR MANIPULACIÓN DE LOS ARCHIVOS

Se puede realizar mediante la edición directa del archivo `/etc/httpd/conf/httpd.conf` y modificando las líneas que a continuación menciono:

- **ServerRoot "/etc/httpd"** : Se indica el directorio que contiene todos los archivos de configuración del servidor , tales log de errores, configuración , etc . Se puede dejar por defecto.
- **MaxClients 150** : Número máximo de equipos clientes conectados haciendo peticiones.
- **ServerAdmin root@localhost**: Dirección del administrador del servidor, al cual se le remitirán vía email, las notificaciones del servidor.
- **ServerName www.sts.com:80** Nombre completo del servidor web y el puerto por el cual escucha. Es importante que ya este funcionando un servidor DNS que resuelva el nombre de esta máquina.
- **DocumentRoot "/var/www/html"**: Nombre del directorio donde reside la página principal del servidor web. El nombre de los posibles archivos que el tomará como página principal, se declara más adelante. Existe otra directiva de configuración con esta función: `<Directory "/var/www/html">`, para los permisos y accesos a este sitio.
- **UserDir public_html**: Permite que los usuarios linux publiquen sus propias páginas, desde su directorio de trabajo. Estas páginas deben residir dentro del directorio `public_html` en su home. Para ver la página publicada se invoca el nombre del servidor seguido de `/~` y el nombre del usuario . Por ejemplo : [http:// www.sts.com/~hector](http://www.sts.com/~hector)
- **DirectoryIndex index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi**: Se le indica los posibles nombres que puede tomar el archivo principal o página de inicio a buscar en el document root o `public_html` o alias.
- **Alias /prueba "/var/www/paginas/"**: Permite crear manipulación de contenido por directorio. Se crea un alias entre la palabra `/prueba` dada en el URL y el directorio físico en linux `"/var/www/paginas/"`. Se va a ese directorio y se corre la página de inicio.

Si se efectúan cambios en el archivo de configuración se debe resetear el servicio:

```
#/etc/rc.d/init.d/httpd stop

# /etc/rc.d/init.d/httpd start
```

```
o
service httpd restart
```

3.4.3. TALLER DE PUBLICACIÓN DE PAGINAS EN EL SERVIDOR WEB

El proceso de publicación de páginas, es muy sencillo. Primero debemos configurar el servidor para saber en que directorios deben residir las páginas que deseamos publicar.

Se debe configurar el servidor web de la siguiente forma:

Se debe crear un usuario llamado taller , cuyo directorio de trabajo sea /home/taller y su contraseña taller2005. La Página que se coloque en cada sitio , debe mostrar un simple texto que diga “prueba de XXX en maquina YYY” donde XXXX es el item que estén probando y YYY es el nombre de la máquina.

- La página que siempre se debe acceder por defecto, en todos los casos se debe llamar default.html. Obviamente cambiando el texto que muestra, según sea el ejercicio solicitado.
- Se debe ubicar la página principal en un directorio debajo de la raíz llamado www. (/www). El docente debe poder ver la página de inicio, simplemente digitando como URL <http://sumáquina.izquierdo.edu.co>. Para los del dominio derecho, deben de cambiar el nombre. No se debe digitar el nombre de la página.
- Se debe crear un alias llamado clave , que nos muestra las páginas publicadas en el directorio /privado. El docente debe poder ver la página de inicio, simplemente digitando como URL <http://sumáquina.izquierdo.edu.co/clave>.
- Se debe crear un alias llamado comun , que nos muestra las páginas publicadas en el directorio /todos. El docente debe poder ver la página de inicio, simplemente digitando como URL <http://sumáquina.izquierdo.edu.co/comun>.
- Se debe permitir a los usuarios publicar paginas dentro de su directorio de trabajo, si crean un subdirectorio llamado web en su home directory. Para probar el docente debe poder ver la página del usuario taller, simplemente digitando como URL <http://sumáquina.izquierdo.edu.co/~taller>.

3.4.4. CONSIDERACIONES DE SEGURIDAD EN EL SERVIDOR APACHE

Si deseamos que alguna parte de nuestro sitio web tenga acceso restringido, podemos pensar en :

3.4.4.1. PROTEGER CON CONTRASEÑA

Pedir un nombre de usuario y clave de acceso para entrar a determinadas áreas de su web site. Por ejemplo deseamos proteger el ingreso al área /clave del sitio web configurado. Para esto debemos seguir los siguientes pasos.

- Permitir en el archivo httpd.conf para el directorio virtual deseado, que se revise el archivo .htaccess

```
Alias /clave "/privado"
<Directory "/privado">
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
```

- Crear un archivo .htaccess en el directorio deseado (el contenido de este archivo , pued ir también en la sección de Directory del alias o área correspondiente.

```
Alias /interno "/intranet"
```

```
<Directory "/intranet">
  AllowOverride All
  Order allow,deny
  Allow from all
</Directory>
```

Ejemplo de .htaccess

```
AuthUserFile /intranet/usuarios
AuthName "area Protegida"
AuthType Basic
require user hector
```

- Crear archivo de usuarios

```
# htpasswd -c /intranet/usuarios hector
```

Se pregunta por una clave y se verifica. Para probar , de nuevo se accesa al alias /clave y debe preguntarse por el usuario y clave en una caja de dialogo.

Si se requiere que se pueda ingresar con varios usuarios creados, se cambia la línea del .htaccess:

```
require valid-user
```

3.4.4.2. RESTRINGIR EL ACCESO DESDE UNA MÁQUINA

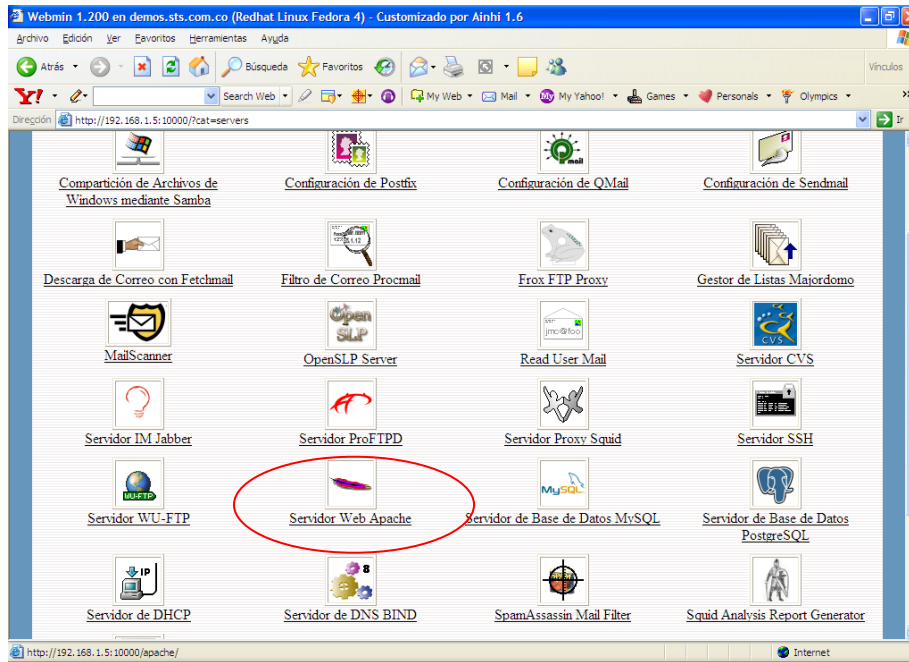
En la sección de permisos del directorio deseado , se puede restringir el acceso desde una red, un dominio o una máquina. Esto se logra editando el archivo de configuración del apache.

```
Alias /clave "/privado"
<Directory "/privado">
  AllowOverride All
  Order allow,deny
  Allow from 192.168.45.37
</Directory>
```

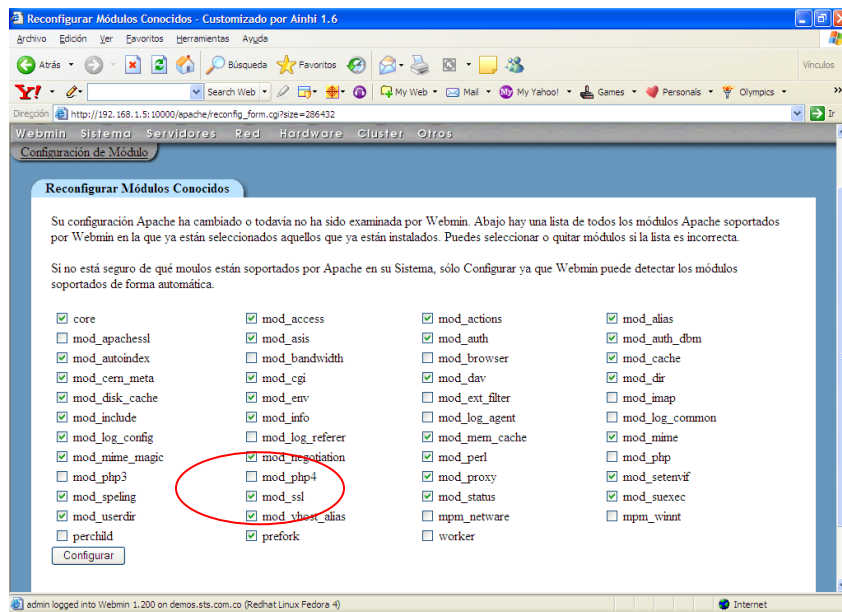
También podemos desear que el intercambio de información entre el cliente y el servidor se haga encriptado.

3.4.4.3. CONEXIONES SEGURAS (ENCRIPADAS)

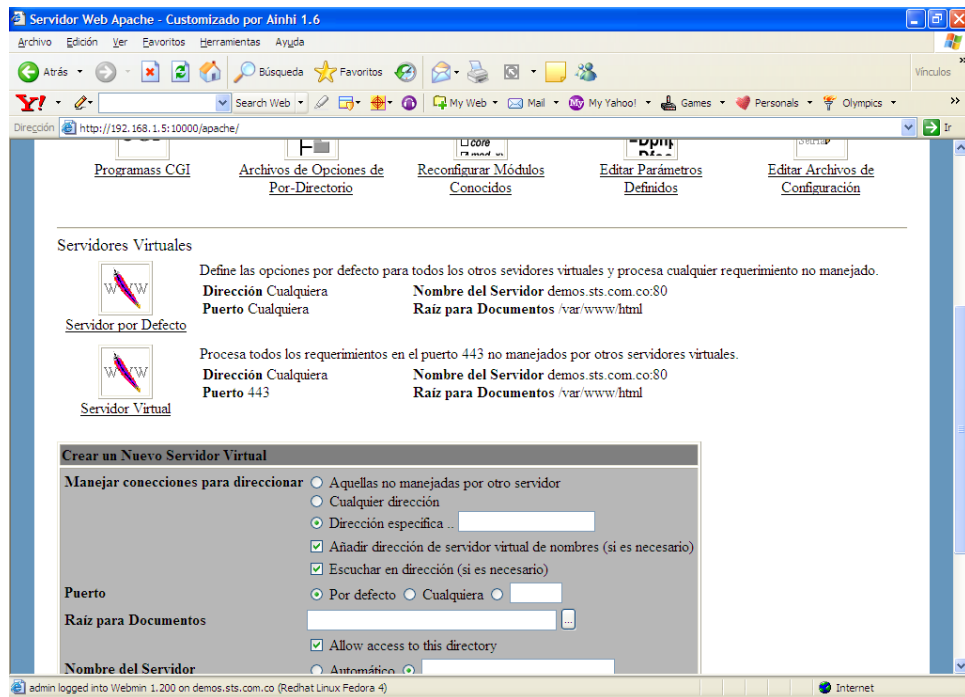
Si trabajamos con el webmin, primero debemos activar el uso del modulo ssl del apache. En esta versión ya está instalado y listo para ser usado.



Se ingresa por el webmin, luego apache, y se indica configuración.



Se escoge configurar, pues el SSL ya esta activo.



Se observa si esta el servidor virtual que escucha por el puerto 443, que es el encriptado y que apunte al mismo directorio del servidor normal.

Simplemente accedamos el servidor : <https://www.sts.com>

La letra “s” adicionada al http es la que indica que se usará acceso web con SSL.

3.4.5. TALLER DE SERVIDOR WEB Y ALGUNOS ASPECTOS DE SEGURIDAD

Proteger con usuario y clave el alias del sitio web de cada maquina, llamado “/comun” que carga las paginas encontradas en el directorio “/todos” (al menos colocar un página de entrada a ese sitio). Solo se permitirán conexiones web que provengan de su misma máquina o de la máquina del docente y que ingresen con el usuario “profe” , con clave “profe05” o el usuario “hector” con clave “hector05. Además la conexión y transferencia de datos debe ser encriptada.

NOTA:

Para el final del módulo, se debe investigar y montar en sus máquina, como podríamos proteger, un alias llamado manuales, que apunta a un directorio que contiene información que solo le compete a los estudiantes de este módulo de la especialización. La creación de los usuarios habilitados para entrar a ese módulo se debe de hacer de forma automática corriendo algún shell, que lea de un archivo plano entregado por el docente, los nombres de los usuarios y la clave. Por ejemplo:

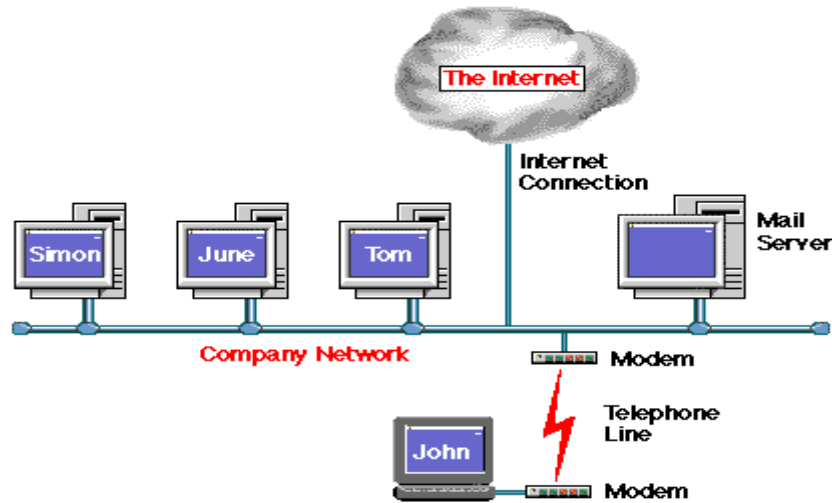
```
hectorgil hector2005
leydibarco leydi2005
.....
.....
.....
```

3.4.5.1. PARA COMPLEMENTAR

Deseamos que siempre que los usuarios se conecten a mi servidor web lo hagan de forma segura (usando SSL), pero que el usuario no tenga que explícitamente escribir https://, si no que lo haga normal y que el servidor web cuando reciba la petición la direcciones automáticamente al servidor encriptado. Que archivos se deben editar y que se debe cambiar o configurar?. Hacer pruebas.

3.5. CONFIGURACIÓN DE SERVICIO DE CORREO ELECTRONICO

E-MAIL: Es de las más populares aplicaciones. El correo electrónico permite a los usuarios intercambiar mensajes con cualquier persona del mundo de una forma rápida. Para los negocios, este a sido un gran avance en comunicación.



El proceso de envío de un mensaje de correo, consistía originalmente En un usuario escribiendo el mensaje en un programa de aplicación llamado cliente de correo, en contraposición con el servidor de correo, que consistía de un editor de texto, posiblemente un corrector ortográfico, una base de datos de la forma de una libreta de direcciones, un administrador de archivos (los mensajes recibidos o no enviados) y un módulo de comunicaciones para poder transferirlos.

El mensaje quedaba almacenado en el mail-server hasta que el usuario destinatario usando su cliente de correo se conectara con él y solicitara los mensajes que le tuviera reservados, el proceso inverso de envío de mensajes era muy parecido cuando el usuario terminara de escribir su mensaje, especificando la dirección de el destinatario, se conectaba con el servidor a fin de depositar el archivo hasta que el destinatario lo solicitara. Cuando el servidor está conectado a sólo una red la única limitación de la dirección de destino, además de no permitir espacios en blanco en la dirección, era que cada dirección debía identificar de forma unívoca a cada usuario, con una LAN esta restricción es fácil de implementar pero con más de una ya pasa a ser un problema mayor; así se introducen los dominios de los usuarios que representan a que servidor pertenecen y que tienen la forma de una dirección válida, es decir sin espacios en blanco ni caracteres prohibidos, para diferenciar el nombre del usuario de su dominio se adoptó en carácter "@" que significa "en" (at) entonces la dirección Bruno@Servidor.A se puede leer como "Bruno en Servidor.A"

El formato de la dirección para el e-mail en internet es de la forma:

Nombre-usuario @organizacion.dominio

Ejemplo hectorgil@intercable.net.co

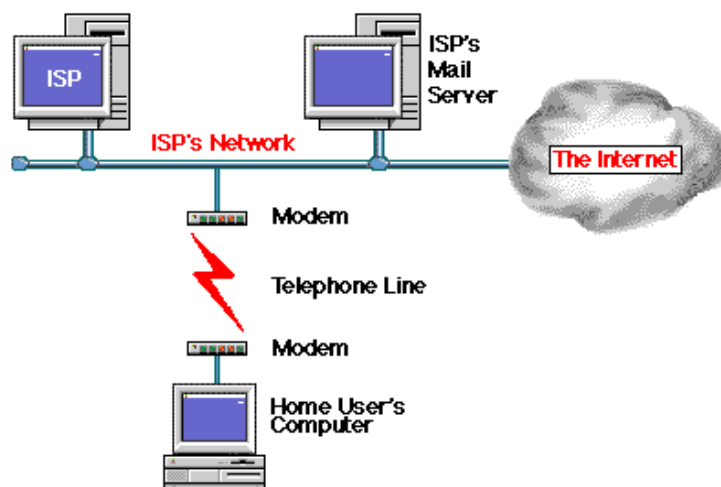
Donde la organización es el nombre de una compañía, agencia del gobierno, institución de educación, etc.

Un problema surgió cuando se intentaron, conectar servidores de correo que utilizaban productos comerciales distintos, que aunque conceptualmente hacía lo mismo eran totalmente incompatibles. El hecho era que hasta el momento no existía un estándar que reglamentara cómo debían implementar los productos este servicio. La necesidad de un estándar se hizo más patente cuando redes totalmente distintas comenzaron a conectarse mediante la INTERNET. Una compañía, posiblemente multinacional, que tuviera asiento en distintos países

del mundo y quisiera intercambiar e-mail tenía que contratar a un ISP (INTERNET SERVICE PROVIDER) y así tener acceso ilimitado a la INTERNET.

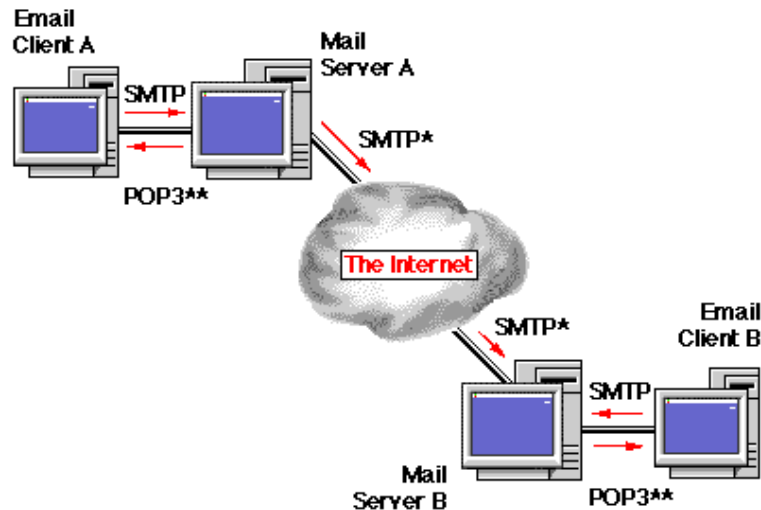
SMTP vs X.400²: Como solución a este caos de variedades de mensajes de e-mail totalmente incompatible, surgieron dos soluciones, dos estándares, aunque parezca contradictorio, el primer estándar es el de facto de la INTERNET y publicó en 1982 bajo la forma de la RFC 821 y se denominó SMTP (simple mail transfer protocol), el protocolo simple de transferencia de mail, y como su nombre lo indica la intención de la gente que hizo el estándar era que conservara la simplicidad de sus predecesores; uno par de años más tarde, y quizá demasiado, llegó el estándar oficial de la CCITT para el manejo de mensajes en INTERNET y se llamó X.400 este estándar nunca llegó a imponerse en la INTERNET debido a su complejidad, lo poco flexible de las direcciones y a que llegó un poco demasiado tarde, el hecho es que el estándar de INTERNET para la transferencia de correo es el SMTP que se usa aún hoy ampliamente en toda la red, con algunas excepciones, que debido a su formato de transferencia el SMTP no soporta los caracteres extendidos que son imprescindibles en idiomas como el francés y el alemán, en particular los gobiernos de Francia y Canadá impulsaron el X.400 como estándar ya que se adaptaban mucho mejor a sus necesidades, ahora estos dos países son los únicos que soportan estos protocolos y debido a esto se necesitó la creación de pasarelas de conversión de un sistema al otro.

EL POP: Estos protocolos funcionan adecuadamente cuando los destinatarios están permanentemente conectados a la INTERNET como en la figura pero unos años después de la publicación de los estándares se hizo más común la INTERNET para usuarios domésticos que desde sus casa se conectaban, mediante un MODEM, esporádicamente a la INTERNET. Estos usuarios tienen un contrato con un ISP que está siempre conectado a la red y al llegar aun mensaje de correo para un usuario de ese ISP el mail-server del ISP debe guardar el mensaje hasta que el usuario se conecte y lo solicite.



Este ambiente se requirió la especificación de otro estándar para estos usuarios, de esta manera apareció en escena el protocolo de oficina postal, POP, que actualmente se encuentra en su versión 3. Este protocolo complementa perfectamente con el SMTP, en la forma en que este último se encarga del envío de correo y su tránsito por la INTERNET hasta el mail-server destino y el POP se encarga de el transporte de los mensajes almacenados en el servidor a usuarios que esporádicamente se conecta a él. Nótese que no es necesario que los clientes estén conectados permanentemente en cambio los servidores si.

² Monografías.com (correo electrónico)



Existe diversidad en las aplicaciones que pueden trabajar como servidores de correo electrónico y mencionaremos algunas en la sección correspondiente.

3.5.1. CONFIGURACIÓN DE CORREO ELECTRÓNICO BASICO EN LINUX

Las máquinas linux, traen un producto de correo nativo como es el sendmail. En estas versiones de Linux, se incorporan una serie de utilidades para configurar y mejorar la seguridad del correo, evitando SPAM, relay, etc.

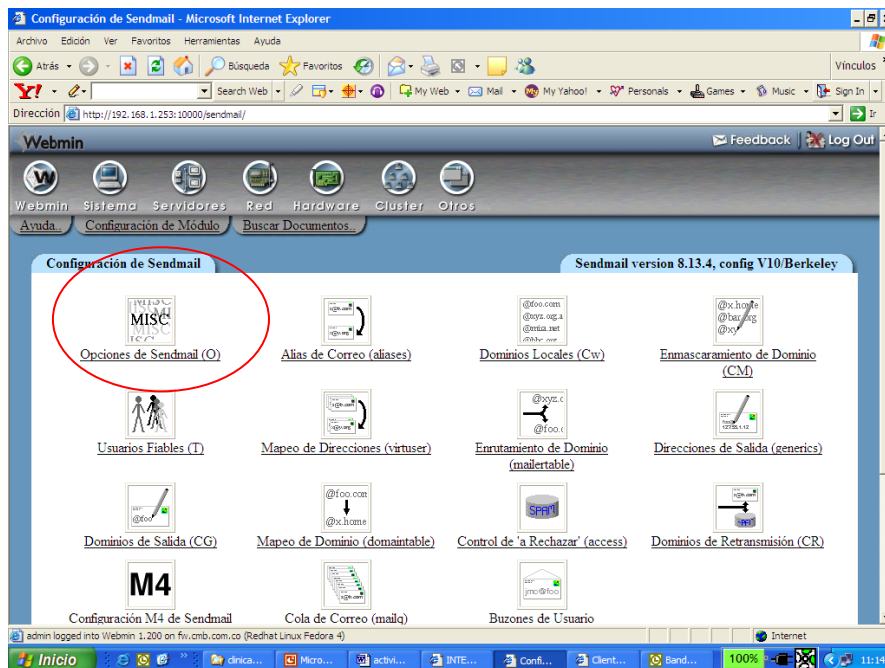
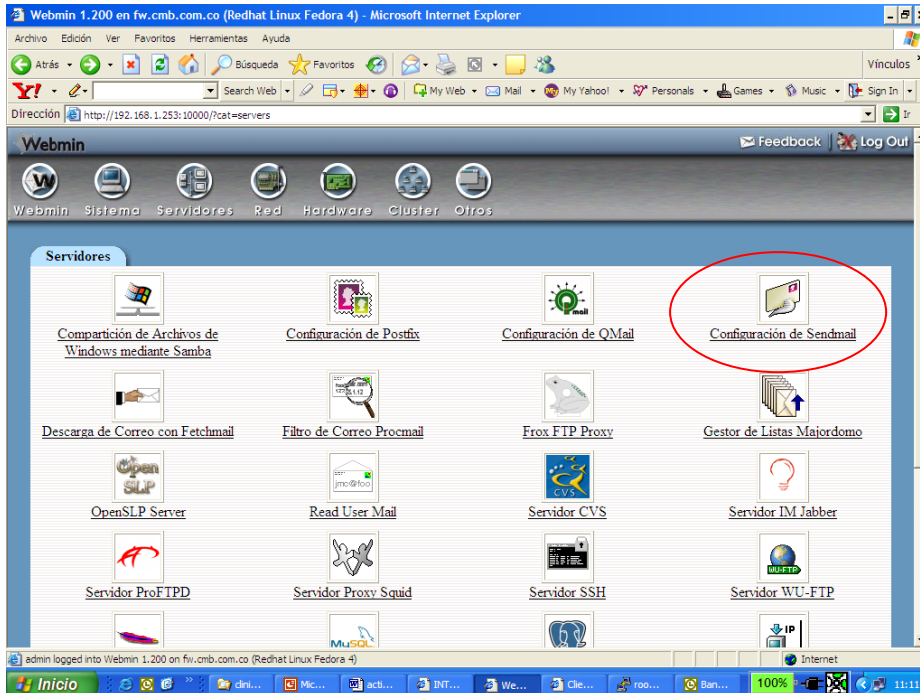
NOTA: Antes de proceder con cambios en la configuración es conveniente ubicar el archivo original de sendmail y sacar copia:

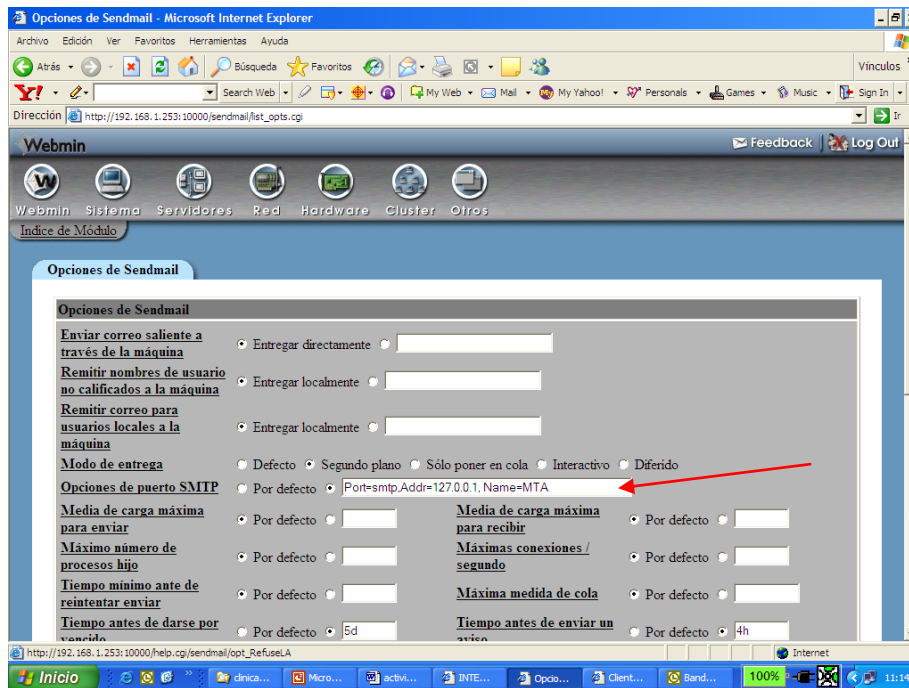
```
[root@original webmin-1.580]# which sendmail
/usr/sbin/sendmail
[root@original webmin-1.580]# ls -l /usr/sbin/sendmail
lrwxrwxrwx 1 root root 21 feb  1 12:42 /usr/sbin/sendmail -> /etc/alternatives/mta
[root@original webmin-1.580]# ls -l /etc/alternatives/mta
lrwxrwxrwx 1 root root 27 feb  1 13:09 /etc/alternatives/mta ->
/usr/sbin/sendmail.sendmail
[root@original webmin-1.580]# ls -l /usr/sbin/sendmail.sendmail
-rwxr-sr-x 1 root smmsp 806460 nov 28 2006 /usr/sbin/sendmail.sendmail
[root@original webmin-1.580]# cp /usr/sbin/sendmail.sendmail
/usr/sbin/sendmail.sendmail.orig
[root@original webmin-1.580]# ls -l /usr/sbin/sendmail.sendmail*
-rwxr-sr-x 1 root smmsp 806460 nov 28 2006 /usr/sbin/sendmail.sendmail
-rwxr-sr-x 1 root root 806460 feb  1 19:13 /usr/sbin/sendmail.sendmail.orig
[root@original webmin-1.580]#
```

El sendmail como tal debe ya estar configurado en la máquina, y si no esta, se procede a generar un archivo sendmail.cf desde el interfaz webmin. Este archivo reside en : /etc/mail

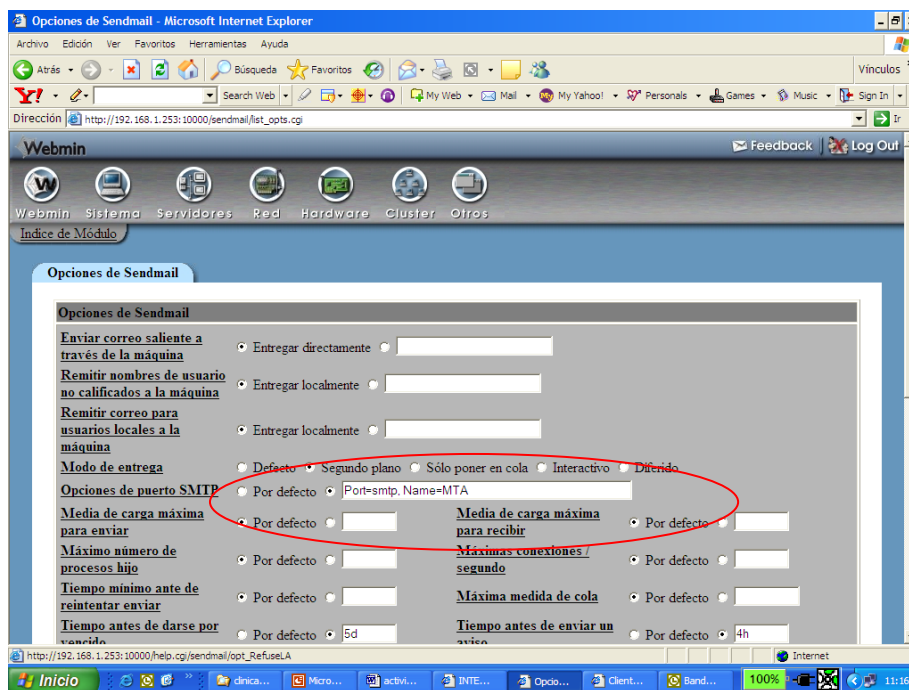
```
[root@original etc]# cd /etc/mail
[root@original mail]# ls
access      local-host-names  sendmail.cf.bak  submit.mc
access.db   mailertable       sendmail.mc      trusted-users
domaintable mailertable.db   spamassassin    virtusertable
domaintable.db Makefile          submit.cf        virtusertable.db
helpfile    sendmail.cf      submit.cf.bak
[root@original mail]#
```

Se ingresa por servidores y se escoge sendmail , luego por opciones:

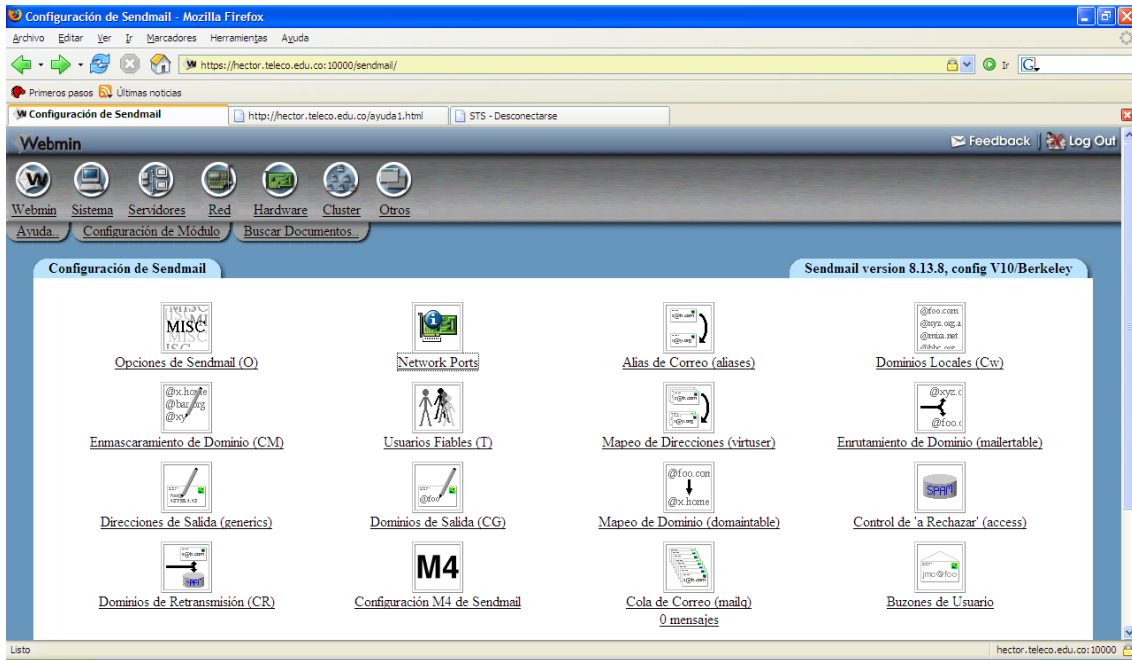




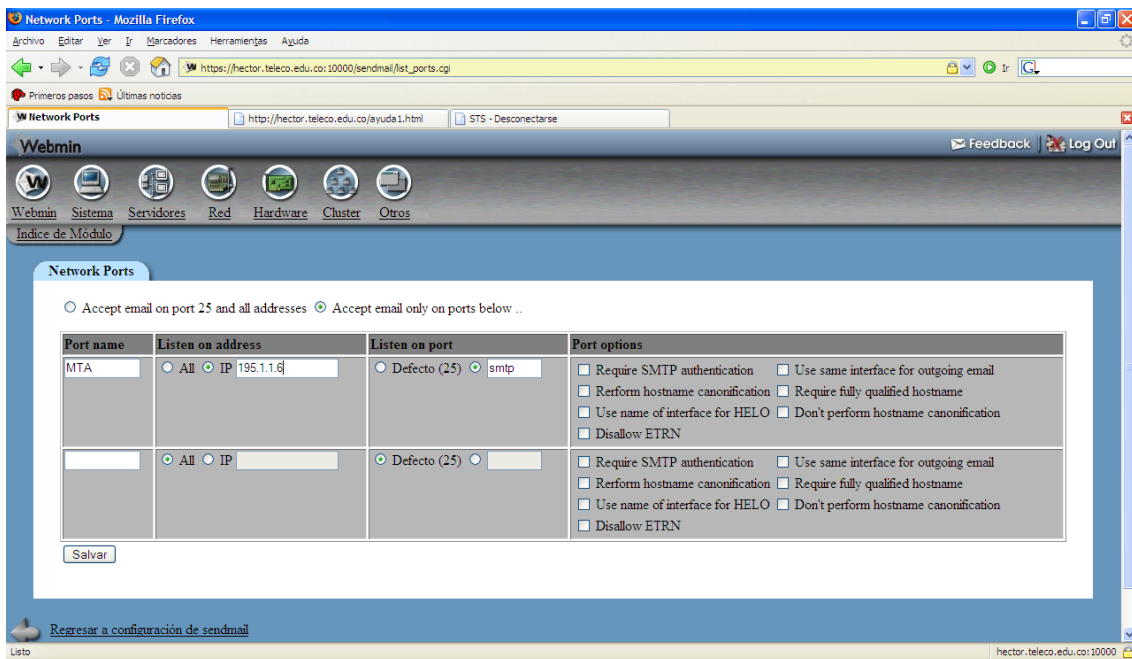
Para que se pueda enviar correo a sitios en internet, se debe modificar la opción del puerto SMTP, quitando la dirección 127.0.0.1. Debe quedar así:



En la versión de Redhat 5.x se debe cambiar las opciones de puerto por :

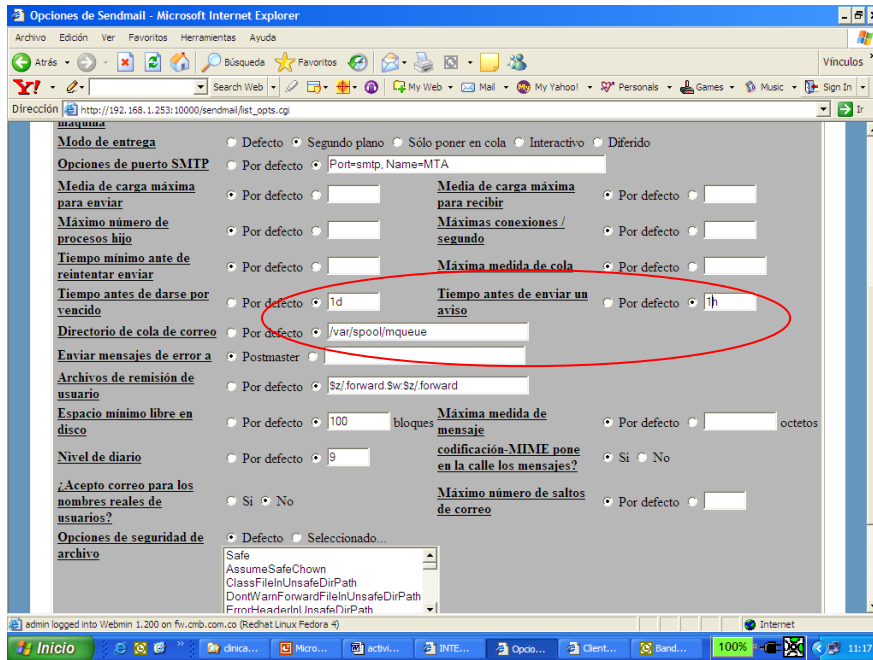


Network ports (cambiar el 127.0.0.1 en listen por la IP del servidor)

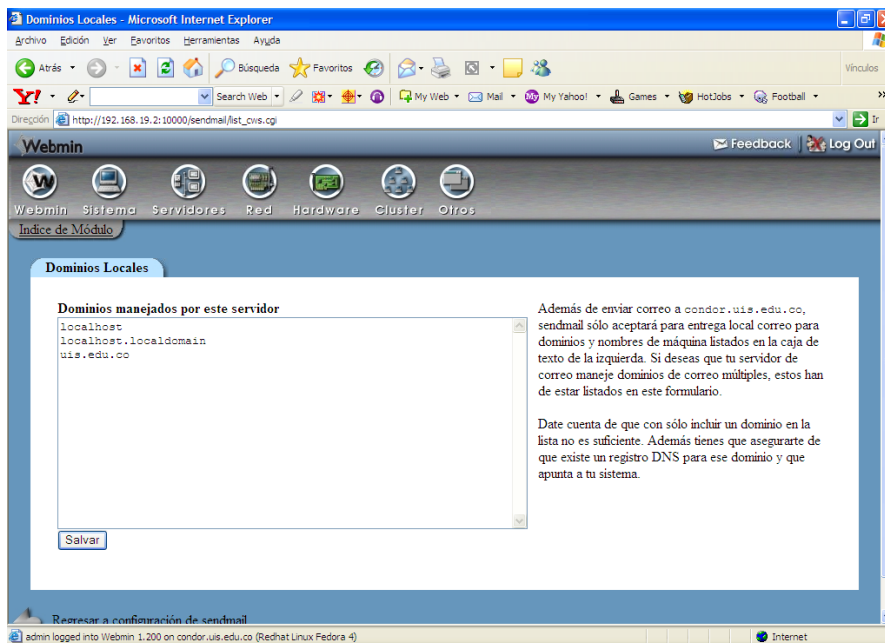


Continuando con opciones.

El tiempo de permanencia de los correos en cola se va a bajar a 1 día y 1 hora:



Se le debe de indicar al servidor de correo, que dominio o para que dominios va a recibir:



Luego al final de esta ventana hay un botón de salvar y aplicar.

Se puede detener el servicio sendmail por comandos:

```
[root@condor ~]# service sendmail stop
Apagando sendmail:                [ OK ]
Desactivaci3n de sm-client:        [ OK ]
[root@condor ~]# service sendmail start
Iniciando sendmail:                [ OK ]
Inicio de sm-client:               [ OK ]
[root@condor ~]#
```

Se verificó que el servicio escuche por el puerto 25:

```
[root@condor ~]# nmap 192.168.19.2

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-01-27 23:23 COT
Interesting ports on condor.uis.edu.co (192.168.19.2):
(The 1658 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
111/tcp   open  rpcbind
10000/tcp open  snet-sensor-mgmt

Nmap finished: 1 IP address (1 host up) scanned in 0.313 seconds
[root@condor ~]#
```

Por razones de seguridad, si más adelante se implementaran productos que interactúen con el sendmail, se debe sacar una copia del programa de sendmail. La copia se sacó al archivo real, no a los enlaces

```
[root@condor ~]# which sendmail
/usr/sbin/sendmail
[root@condor ~]# ls -l /usr/sbin/sendmail
lrwxrwxrwx 1 root root 21 ene 27 21:28 /usr/sbin/sendmail -> /etc/alternatives/mta
[root@condor ~]# ls -l /etc/alternatives/mta
lrwxrwxrwx 1 root root 27 ene 27 21:28 /etc/alternatives/mta -> /usr/sbin/sendmail.sendmail
[root@condor ~]# ls -l /usr/sbin/sendmail.sendmail
-rwxr-sr-x 1 root smmsp 774264 may 6 2005 /usr/sbin/sendmail.sendmail

#cp /usr/sbin/sendmail.sendmail /usr/sbin/sendmail.sendmail.ori

[root@condor ~]# ls -l /usr/sbin/sendmail.sendmail*
-rwxr-sr-x 1 root smmsp 774264 may 6 2005 /usr/sbin/sendmail.sendmail
-rwxr-sr-x 1 root root 774264 ene 27 23:25 /usr/sbin/sendmail.sendmail.ori
```

Si ya se dispone de usuarios de correo, podemos hacer una prueba básica de envío y recepción de correo, directamente desde comandos unix (con el comando mail), que fue la forma nativa de hacerlo:

Por ejemplo estando como usuario root, podemos enviar un correo al usuario webmaster de la forma:

```
# mail webmaster
```

Se preguntará por quién recibirá copia del email y el subject y luego el mensaje. Se termina el dialogo con ctrl.-C.

Luego entrando con el usuario webmaster verificamos :

```
[root@www root]# su - webmaster
[webmaster@www webmaster]$ id
uid=501(webmaster) gid=501(webmaster) grupos=501(webmaster)
[webmaster@www webmaster]$ mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/spool/mail/webmaster": 1 message 1 new
>N 1 root@www.sts.com Mon Apr 14 22:56 13/389 "prueba de correo"
& 1
Message 1:
From root Mon Apr 14 22:56:38 2003
```

```
Date: Mon, 14 Apr 2003 22:56:38 -0500
From: root <root@www.sts.com>
To: webmaster@www.sts.com
Subject: prueba de correo
```

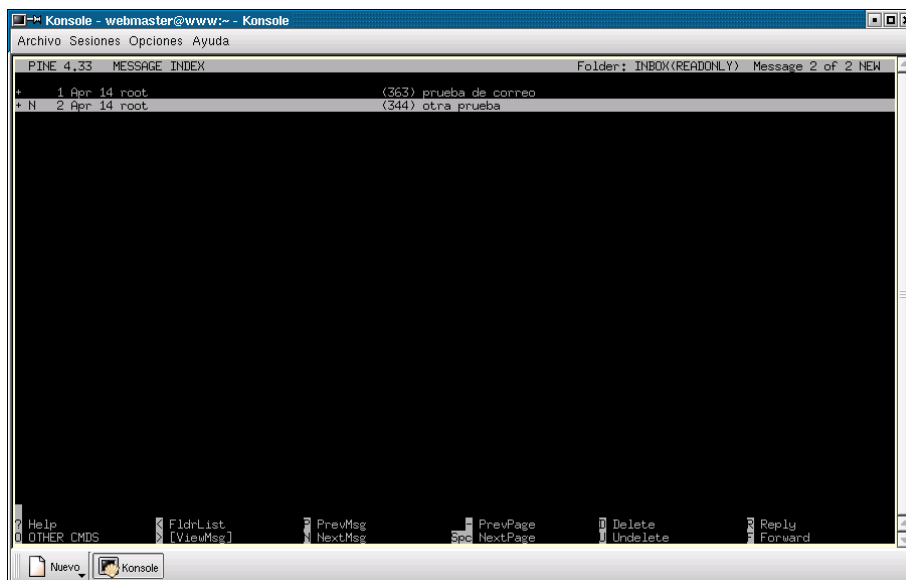
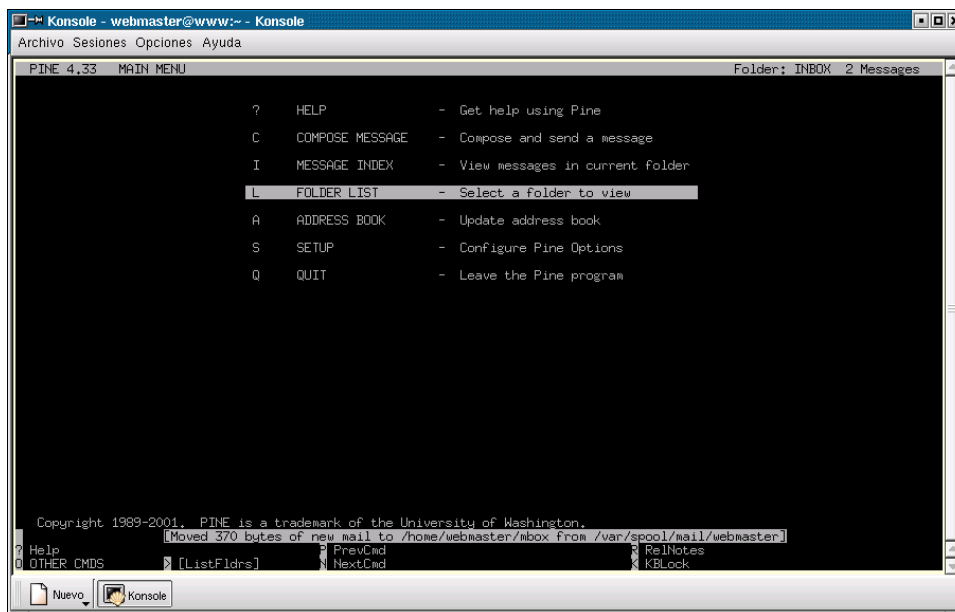
esta es una prueba

& q

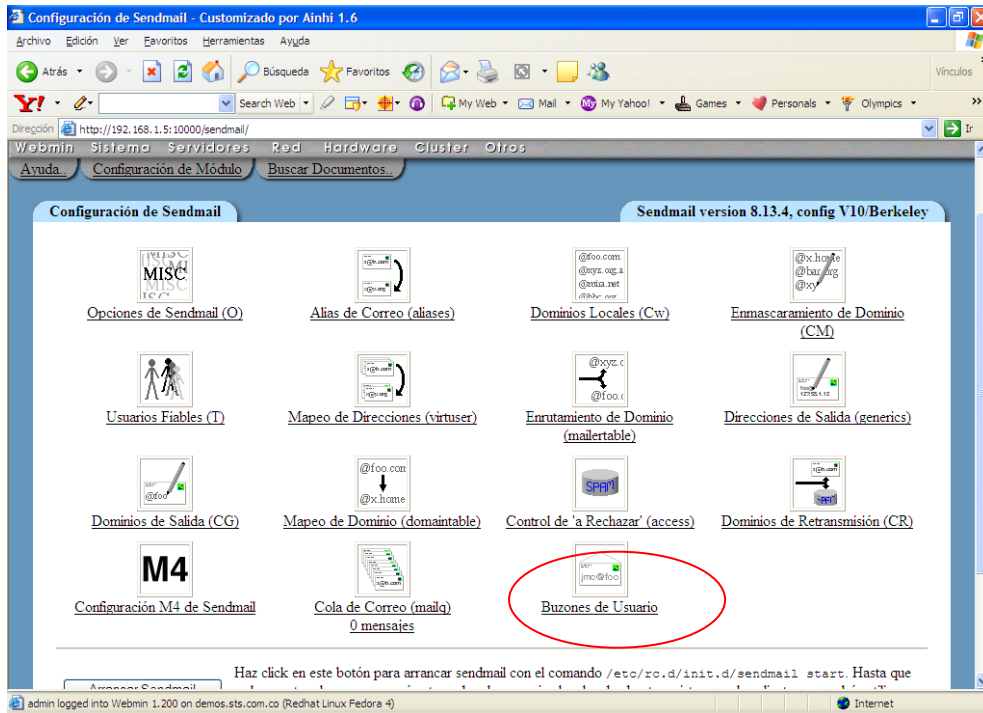
Saved 1 message in mbox

[webmaster@www webmaster]\$

Este comando no es muy amigable, y existe diversas formas de recuperar o enviar correo. Otra forma texto de hacerlo es con el comando pine (no viene preinstalado con el sistema):



Las pruebas se pueden hacer con el webmin o un utilitario gráfico. Por servidores, sendmail, buzones de usuario:



Desde allí, se puede ingresar a un buzón de usuario e indicar componer correo. Se puede ingresar a otros buzones y verificar que el correo fue recibido.

Si se presenta un mensaje de error como relaying.denied, es porque hace falta configurar unos filtros de correo que se trataran más adelante.

TEST MAS COMPLETOS

Si se desea mayor información sobre el envío y recepción de correo, o hacer un test con algún servidor se puede utilizar directamente el comando sendmail y ver todo el diálogo de conexión entre los servidores, podemos invocar al sendmail en modo verbose. Aquí partimos de que tenemos un archivo texto llamado prueba con el mensaje a enviar.

Se puede hacer una prueba sencilla de envío de correo (desde el usuario root o de otro que se haya creado) a una cuenta del mismo servidor o de uno externo si ya contamos con el dominio activo , con el comando sendmail -v para trabajar en modo debug y poder observar posibles errores:

En este caso, ya hay un usuario creado llamado webmaster, desde donde enviaremos el correo. Como actualmente estamos trabajando con el usuario root, debemos de cambiar de usuario al webmaster y desde allí se procede a hacer el envío.

```
# su - webmaster
$ pwd
/home/webmaster

$ cat prueba
este es un archivo para envio de correo de prueba desde maquina sts
por favor confirmar que llega el correo

$ /usr/lib/sendmail -v hectorgiltriana@hotmail.com <prueba
hectorgiltriana@hotmail.com... Connecting to mx1.hotmail.com. via esmtp...
```



```

220 mc9-f29.bay6.hotmail.com Microsoft ESMTMP MAIL Service, Version: 5.0.2195.5600 ready
at Sat, 1 Feb 2003 08:01:58 -0800
>>> EHLO www.sts.com.co
250-mc9-f29.bay6.hotmail.com (02.01.00.0007) Hello [200.21.238.196]
250-SIZE 4278190
250-PIPELINING
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VERFY
250-AUTH LOGIN
250-AUTH=LOGIN
250-X-HMAUTH
250 OK
>>> MAIL From:<webmaster@www.sts.com.co> SIZE=124
250 webmaster@www.sts.com.co....Sender OK
>>> RCPT To:<hectorgiltriana@hotmail.com>
250 hectorgiltriana@hotmail.com
>>> DATA
354 Start mail input; end with <CRLF>.<CRLF>
>>> .
250 <200302011601.h11G1vq13069@www.sts.com.co> Queued mail for delivery
hectorgiltriana@hotmail.com... Sent ( <200302011601.h11G1vq13069@www.sts.com.co>
Queued mail for delivery)
Closing connection to mx1.hotmail.com.
>>> QUIT
221 mc9-f29.bay6.hotmail.com Service closing transmission channel
    
```

Se puede observar que el correo fue entregado al servidor destino y almacenado en espera de su recuperación.

Si deseamos probar la recepción de correo , podemos hacer la misma operación de envío hacia nuestro servidor, desde alguna máquina en internet (primero se prueba enviando el correo con la dirección larga que incluye el nombre del servidor y luego probamos enviándolo solo con la cuenta de usuario y nombre del dominio.

```

$ telnet www.sts.com.co
Trying 200.114.1.72...

Connected to 200.114.1.72.

Escape character is '^]'.

Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: root
Password:
Last login: Tue Jan 28 16:44:16 from 200.75.51.66
You have new mail.
# pwd
/root
# hostname
www.sts.com
# cd /
# cat prueba
esta es prueba de correo enviado desde servidor linux www.sts.com , que tambien
esta en red de intercable.

# /usr/lib/sendmail -v webmaster@www.sts.com <prueba
    
```

```

webmaster@www.sts.com.... Connecting to www.sts.com.. via esmtp...
220 www.sts.com.co ESMTP Sendmail 8.11.6/8.11.6; Sat, 1 Feb 2003 11:09:33 -0500
>>> EHLO www.sts.com
250-www.sts.com. Hello [200.75.57.36], pleased to meet you
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250 HELP
>>> MAIL From:<root@www.sts.com> SIZE=109
250 2.1.0 <root@www.sts.com>... Sender ok
>>> RCPT To:<webmaster@www.sts.com.>
250 2.1.5 <webmaster@www.sts.com.>... Recipient ok
>>> DATA
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 h11G9Xn13089 Message accepted for delivery
webmaster@www.sts.com... Sent (h11G9Xn13089 Message accepted for delivery)
Closing connection to www.sts.com..
>>> QUIT
221 2.0.0 www.sts.com. closing connection
    
```

Para poder leer correo desde clientes gráficos, tal como Outlook con windows XP, o kmail de linux, o netscape en ambos ambientes, debemos tener disponible el servicio POP3 o IMAP en el servidor.

3.5.2. ACTIVAR EL SERVICIO POP3 E IMAP

Para poder leer correo desde clientes gráficos, tal como Outlook con windows XP, debemos tener disponible el servicio POP3 o IMAP en el servidor. El IMAP lo usa el interfaz web squirrelmail.

En las versiones Fedora y Redhat enterprise el control de los servicios de POP3, IMAP, ya no lo hace el xinetd.d , sino Dovecot. Para activar los servicios, se edita el archivo de configuración de dovecot y se dejan las líneas:

```

[root@fw ~]# cd /etc
[root@fw etc]# ls dovecot.conf
dovecot.conf
[root@fw etc]#
    
```

editar el archivo y líneas (ya las debe de tener configuradas por defecto)

```

protocols = imap imaps pop3 pop3s
# Support for dynamically loadable modules.
#pop3_use_modules = no
#pop3_modules = /usr/lib/dovecot/pop3
    
```

Se inicia el servicio dovecot y se verifica su estado:

```

[root@condor etc]# service dovecot start
Iniciando Dovecot Imap:                [ OK ]
[root@ etc]# service dovecot status
Se está ejecutando dovecot (pid 2528)...
    
```

```
[root@fw etc]#
```

Se puede comprobar si el pop e imap están escuchando peticiones con el nmap o haciendo telnet al puerto por el que escuchan:

Con nmap:

```
[root@condor etc]# nmap 192.168.19.2

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-01-27 23:53 COT
Interesting ports on condor.uis.edu.co (192.168.19.2):
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
993/tcp   open  imaps
995/tcp   open  pop3s
10000/tcp open  snet-sensor-mgmt

Nmap finished: 1 IP add
```

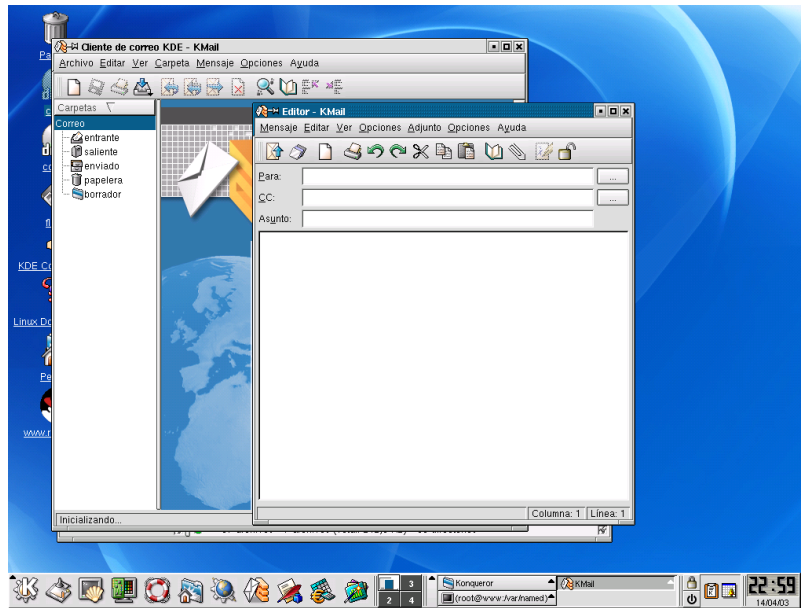
El pop3 escucha por el puerto 110 y para poder comprobar su funcionamiento podemos hacer un telnet al puerto 110 para que nos responda este servicio.

```
[root@condor etc]# mail sts < /etc/hosts
[root@condor etc]# telnet 192.168.19.2 110
Trying 192.168.19.2...
Connected to condor.uis.edu.co (192.168.19.2).
Escape character is '^]'.
+OK dovecot ready.
user sts
+OK
pass sts
+OK Logged in.
list
+OK 1 messages:
1 916
.
quit
+OK Logging out.
Connection closed by foreign host.
```

Ya se ha comprobado que este servicio esta disponible , entonces se puede configurar un interfaz gráfico como outlook para leerlo.

Se comprueba el envío y recepción de correo mediante el outlook de windows.

Esta configuración de la parte cliente de correo , es relativamente sencilla. Linux posee varias interfaz para manejo de correo, como kmail, evolution, y otros.

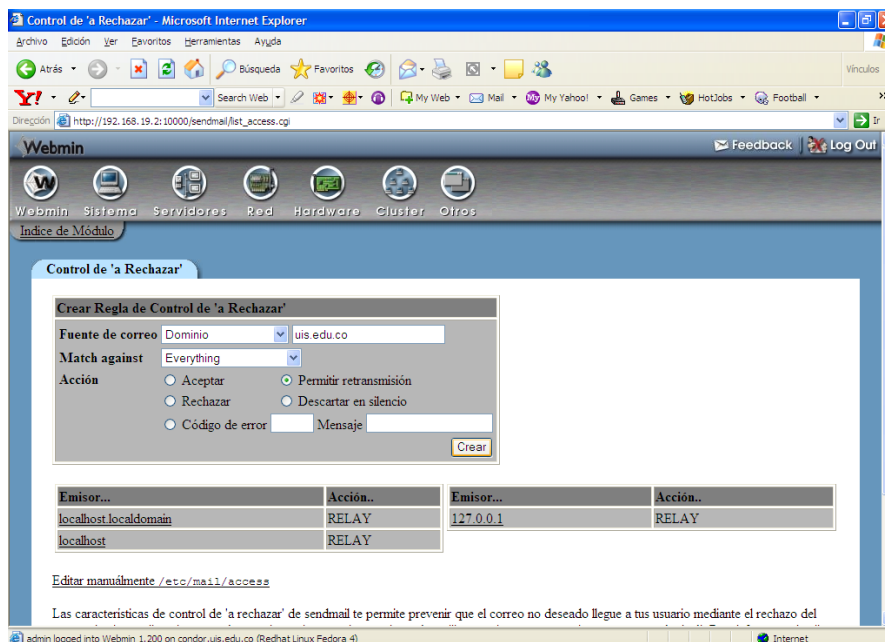


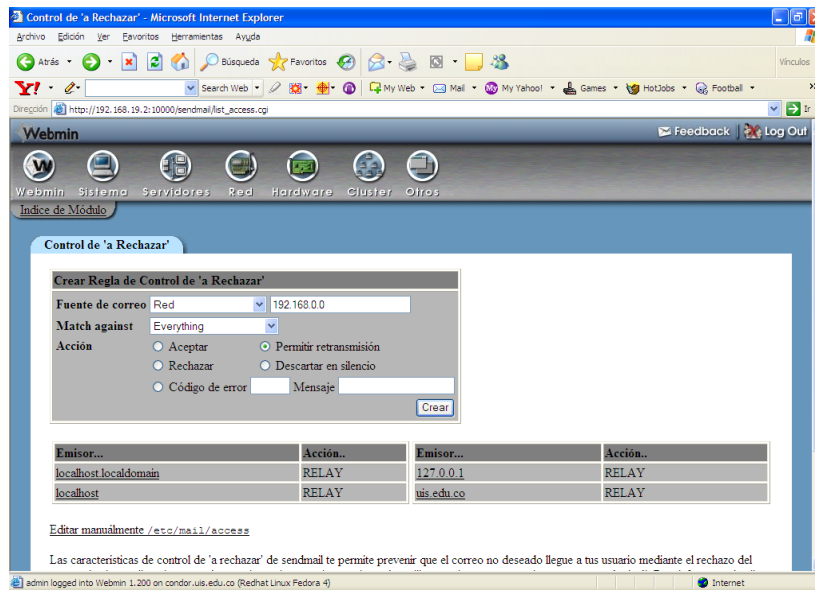
Esta es una imagen del interfaz de correo llamada kmail.

3.5.3. CONTROLES O FILTROS.

Una vez iniciado, el servicio (apagando y activando el servicio sendmail) se puede proceder a colocar filtros para seguridad del mismo. En estos filtros se puede especificar que dominios o que máquinas pueden enviar correo a través de este servidor, a que dominios enviar, etc.

Por sendmail (en servidores) y control a rechazar se va a permitir que los usuarios de la red envíen:





Estos procesos generan una serie de archivos que residen en la carpeta /etc/mail :

```
[root@condor ~]# cd /etc/mail
[root@condor mail]# ls
access      domaintable.db  mailtable      sendmail.cf    submit.cf      virtusertable
access.db   helpfile        mailtable.db  sendmail.mc    submit.mc      virtusertable.db
domaintable local-host-names Makefile      spamassassin  trusted-users
[root@condor mail]# cat access
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain      RELAY
localhost                   RELAY
127.0.0.1                   RELAY

uis.edu.co      RELAY
192.168.0.0    RELAY
[root@condor mail]# cat local-host-names
localhost
localhost.localdomain
uis.edu.co
[root@condor mail]# cat trusted-users
# trusted-users - users that can send mail as others without a warning
# apache, mailman, majordomo, uucp, are good candidates
[root@condor mail]#
```

Hay otro achivo que en algunos servidores es de gran utilidad y es el relay_domains.

Para detener o iniciar el servicio de correo:

```
#service sendmail stop
#service sendmail start
```

o

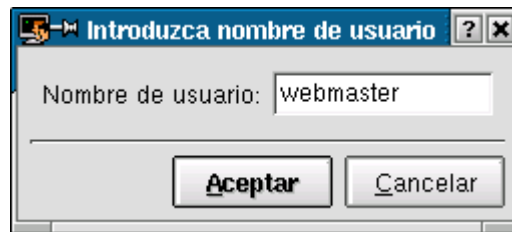
```
#service sendmail restart
```

3.5.4. CREACION DE CUENTAS DE CORREO.

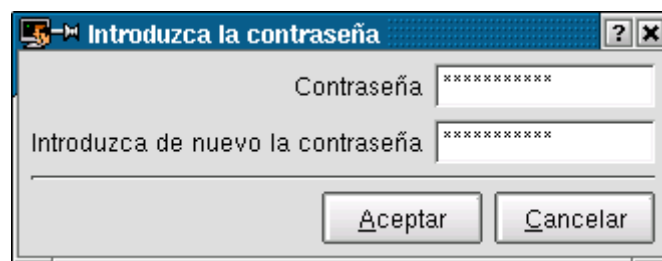
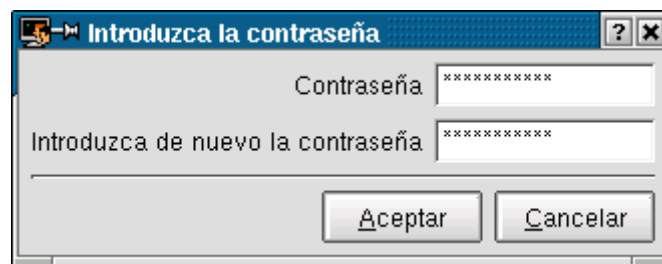
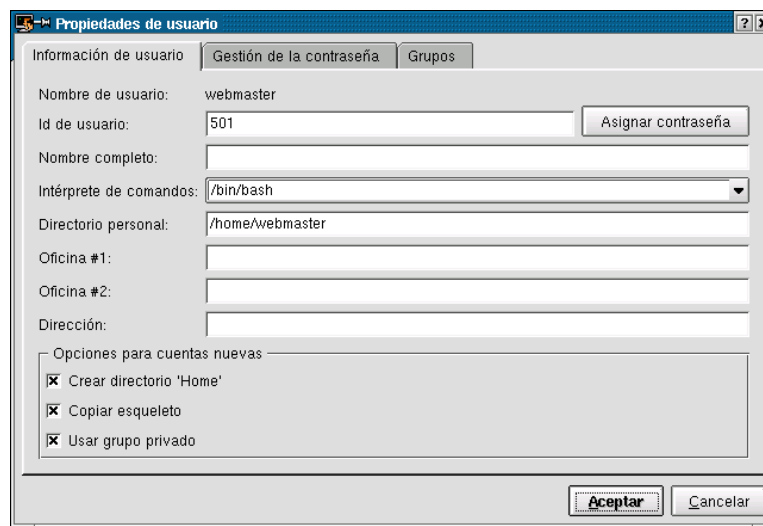
Es un proceso sencillo, ya que es el mismo que crear una cuenta linux para usuario.

Desde el administrador de usuarios, bien sea por sistema o desde ese mismo nivel si se ha invocado últimamente, se procede.

Se escoge el icono superior de add user.



Se digita el nombre del usuario y luego se procede a asignar una contraseña (clave)



Luego en la pestaña superior izquierda de archivo se procede a guardar los cambios. Se pueden reportar algunos mensajes por directorios ya creados o permisos, pero se pueden ignorar.

Para algunas pruebas, se sugiere trabajar alias de correo (o listas básicas). Por ejemplo se desea crear un alias, llamado todos, que hace referencia a cuentas de correo de los diferentes usuarios de la sala. Para esto se edita el archivo /etc/aliases y se incluye una línea:

```
todos: angelica@juan.gama.com.co, sergio@hector.gama.com.co, juan@sergio.gama.com.co,
prueba1@mireya.gama.com.co, miguel@german.gama.com.co, wilson@lucho.gama.com.co,
henry@henry.pirineos.com.co, gftellez@giovanny.pirineos.com.co,
juan1@juan.pirineos.com.co, prueba@guillermo.pirineos.com.co,
gerson@mario.pirineos.com.co, prueba@bell.gama.com.co, korn@pablo.pirineos.com.co
```

La sintaxis de la línea es:

```
Nombrealias: cuentacorreo, cuentacorreo2, cuentacorreo3
```

Luego para enviar un correo a la lista, simplemente se trata como si fuese otro usuario, es decir , se enviaría el correo a la cuenta todos de esa máquina, y hace referencia a las diferentes cuentas de la lista.

3.5.5. MANEJO DE CORREO ENCRIPTADO

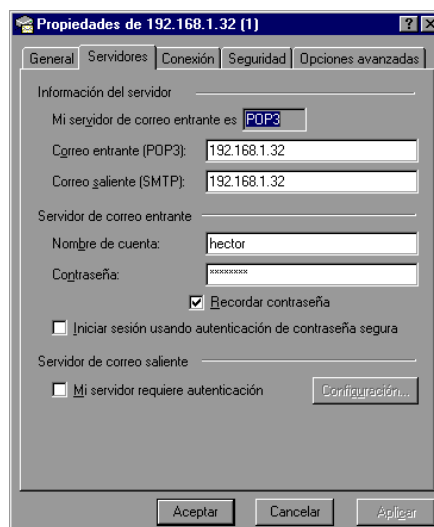
Como se presentó en la utilización de sniffer, el tráfico del correo normal , puede ser visto por cualquier persona dentro de la red con el uso de estas herramientas.

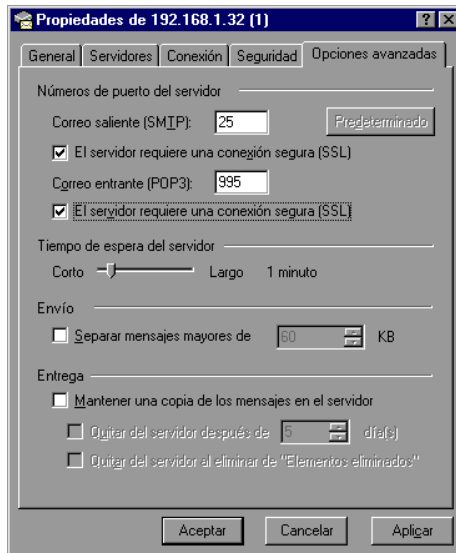
Por tal razón, se debe tratar de utilizar productos que encripten el correo. Se debe activar el servicio POP que trabaja con SSL (secure socket layer) llamado POP3S.

En el caso de esta versión de Linux, hay que recurrir al dovecot para activar este servicio, de forma semejante a la activación del pop3.

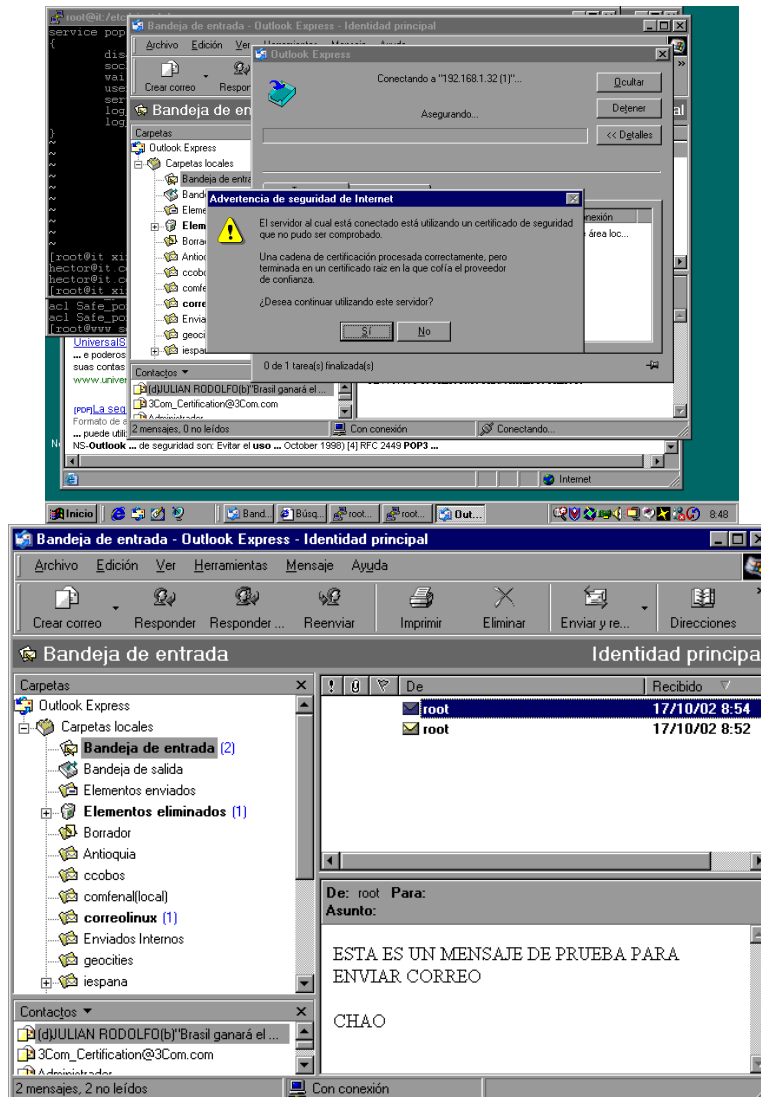
Se debe reiniciar el servicio dovecot (el servicio pop3s escucha por el puerto 995) .

En el producto cliente (outlook) también se debe especificar que se usará un protocolo seguro :

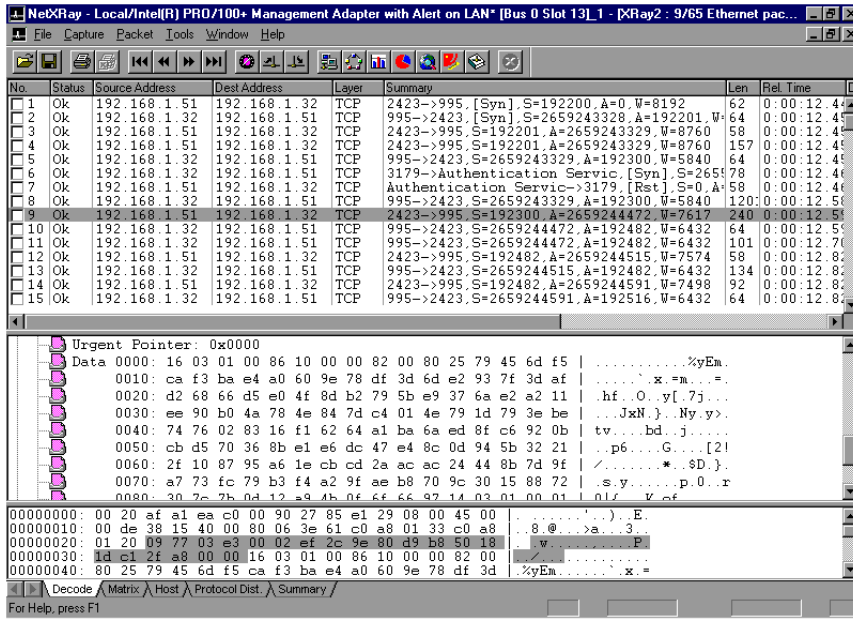




Se procedió a leer correo con el outlook, monitoreando la conexión con el sniffer. Mostró una advertencia en el cliente de correo.



Desde el sniffer se observa que la comunicación esta encriptada y es ilegible.

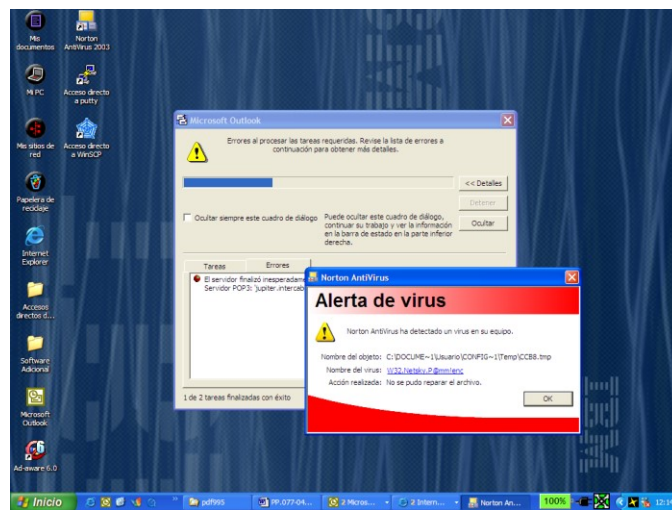


3.5.6. TALLER SERVICIO DE CORREO BASICO

Configurar un servicio de correo con algunas consideraciones de seguridad. Es decir, la comunicación entre el cliente y el servidor debe ser encriptada (mostrarlo) y solo se deben permitir salir correos por el servidor de los equipos clientes de cada fila de trabajo. Se deben crear algunas cuentas de correo con el nombre de los integrantes de los grupos y enviar y recibir correos entre los diferentes servidores dentro de una misma fila. Osea en cada servidor se deben crear cuentas para todos los usuarios clientes de esa fila y todos deben actuar como clientes y servidores alguna vez. Las direcciones de correo deben llevar el nombre de la máquina, pues no hay una máquina predestinada a recibir correo de todo el dominio.

3.5.7. CONTROL DE VIRUS Y SPAM

Un alto porcentaje de los correos que llegan a los usuarios de las empresas, contienen virus, gusanos, programas espías, etc. Si se tiene activado en los equipos clientes un antivirus que revise los correos entrantes o salientes, es frecuente ver mensajes como:

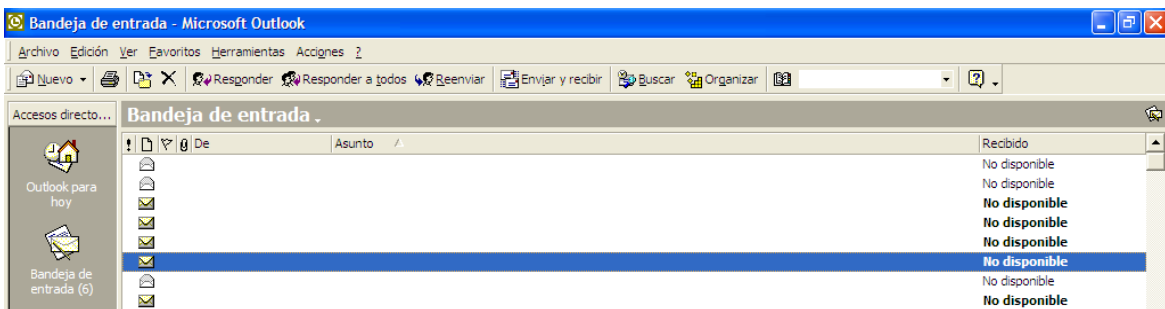
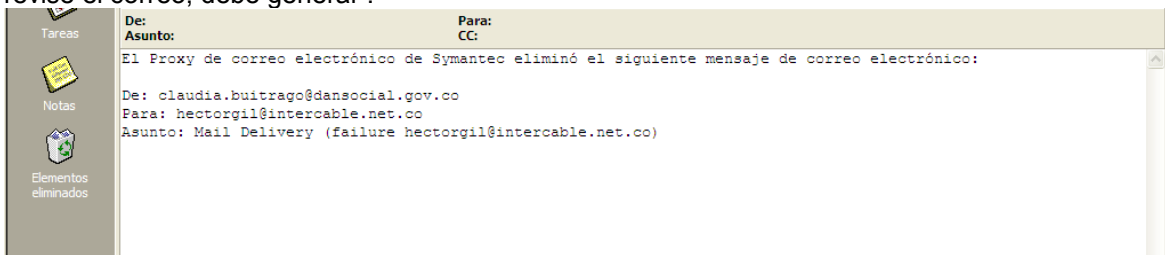


Esta labor de chequeo de virus, se debe delegar en primera instancia Al servidor de correo, para evitar posibles infecciones en los PCs, y además rechazar todos los correos que los contengan.

Dentro de los correos que llegan con frecuencia , observamos mensajes como:



Y si se llega a abrir el archivo anexo, contiene virus. Si hay un software antivirus en el PC que revise el correo, debe generar :



Un alto porcentaje de los correos, son de ese tipo, con asuntos como:

Re,Re:Thanks,
Your pictures
Etc,...

Estas situaciones causan un gran desgaste en administradores, operadores, y usuarios finales. Por tal razón se debe implementar estos controles en el servidor, para minimizar la llegada de estos tipos de correo a los usuarios.

Sendmail es un programa que proporciona el servicio de correo electrónico en sistemas Linux (y Unix.) Entre sus objetivos de diseño destaca un gran poder de configuración - casi ilimitado - capaz de procesar mensajes de email en prácticamente cualquier tipo de red. MTA/Servidor

Sendmail como MTA (Mail Transfer Agent) se encarga de enviar (y reintentar de ser necesario) los mensajes redactados por los usuarios de la organización. Igualmente, recibe los mensajes dirigidos a usuarios de la organización y los coloca en sus respectivos "Buzones de correo" para su posterior lectura.

Sendmail es extremadamente configurable -aunque no necesariamente de un modo sencillo. Para esto posee un archivo de configuración principal que en RedHat es: /etc/mail/sendmail.cf que tiene una sintaxis poco intuitiva, y ha sido diseñado principalmente para que el computador lo lea de un modo eficiente (mas no los humanos). El archivo sendmail.cf define generalmente la ruta de otros archivos de configuración auxiliares que evitan la modificación directa del primero, simplificando la administración de Sendmail.

En las últimas versiones de sendmail (8.12 o superiores) es usual que se configure el servidor para que se ejecute "dividido" en dos programas complementarios a fin de elevar la seguridad del sistema: `/var/spool/clientmqueue` En este caso, el segundo proceso (client queue runner) es controlado mediante otro archivo de configuración: `/etc/mail/submit.cf`

A fin de facilitar la configuración de Sendmail para los usuarios ocasionales y los administradores en general, existe un mecanismo complementario que evita la escritura y modificación directa del archivo "sendmail.cf". Este mecanismo consiste en escribir un archivo relativamente sencillo usando la sintaxis del lenguaje "M4", el cual se proporciona en prácticamente todos los sistemas Unix/Linux (a veces como software opcional.) Mediante este sistema, el usuario creará (o modificará) un archivo relativamente breve, el cual se traducirá en muchas líneas del archivo de configuración.

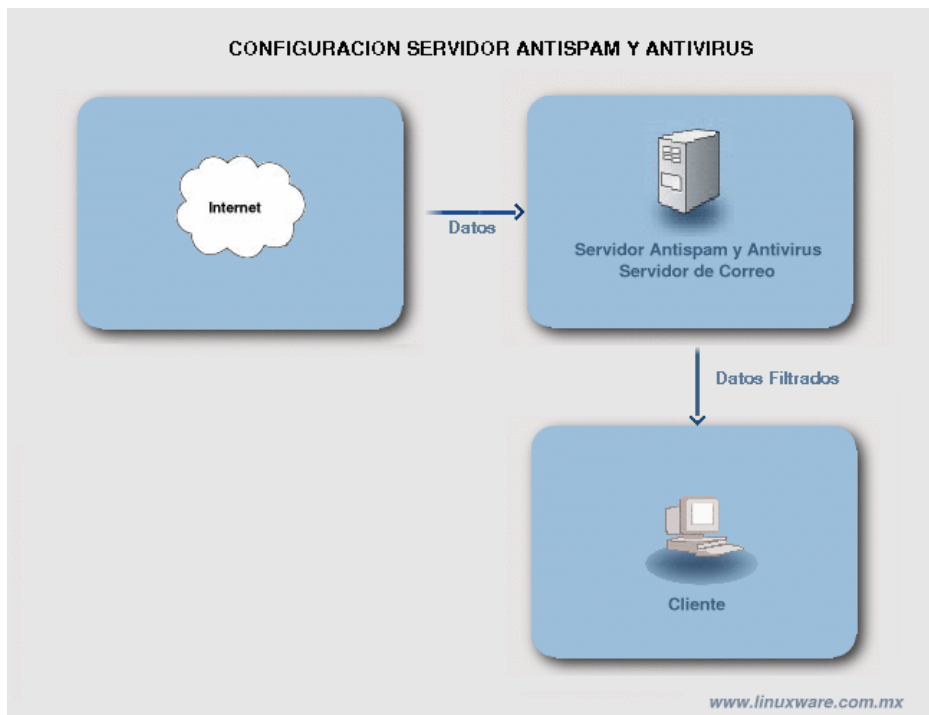
Las soluciones propuestas, traen su propio MTA que reemplaza al sendmail nativo de linux.

En los últimos años, se ha hecho muy común que los virus viajen como archivos adjuntos en mensajes de correo electrónico. Por esta razón los archivos con las extensiones EXE, JS, LNK, PIF, SRC y VBS entre otras han sido considerados peligrosos y no son admitidos por los servidores de correo seguros. De igual forma los correos conocidos como SPAM pueden hacer que los buzones de correo se llenen rápidamente de publicidad e informaciones que no hacen referencia al objetivo principal de la empresa. Debido a esto, surge la necesidad de implementar un mecanismo que se encargue de garantizar el filtro de correo SPAM y la no entrega de archivos infectados con virus a los usuarios finales.

Para esto se cuenta con una herramienta de filtrado MailScanner que garantiza la fiabilidad de los correos que llegan a los buzones de los servidores, inicialmente se plantea un esquema haciendo del MailScanner un muro de fuego para la llegada de estos correos.

Mail Scanner es un spammer y scanner para correo electrónico.

Es capaz de detectar un gran número de tipos de correos electrónicos comerciales o spam.



No solo posibilita el scaneo de virus conocidos sino que también amplía su protección a los no conocidos, chequeando los archivos adjuntos o attachments y rechazando los que contengan

una serie de patrones que MS tiene predeterminados como no aceptados. En los mencionados patrones podemos destacar el de extensión de fichero mediante el cual rechaza mails que contengan una serie de extensiones.

Otra característica destacable es la posible desinfección de adjuntos en los mails (p.e. un macro de Word) es automáticamente desinfectado y a continuación es enviado a su destino original totalmente limpio y listo para que el usuario pueda acceder a este con toda confianza.

Los servidores que utilizan Mailscanner como sistema de protección anti-virus. Todos sus mensajes entrantes y salientes son revisados por este software. En caso de encontrar un mensaje infectado, Mailscanner elimina el virus y envía un reporte tanto al destinatario del mensaje como al remitente.

El reporte llega desde el servidor de correo y la línea de Asunto contiene la frase {VIRUS DETECTADO} al inicio. Este mensaje contiene información sobre el virus que se encontró y las partes del mensaje original que han sido recuperadas.

La detección y limpieza de virus, es realizada por el motor antivirus F-Prot (o clamav o cualquier otro antivirus para linux), este se mantiene actualizado a diario con los últimos dats y registros de virus nuevos. En esta ultima versión, se garantiza que si llega un archivo ZIP a un buzón de usuario, este es desempaquetado para posteriormente revisar el contenido en búsqueda de virus.

El registro de virus se actualiza automáticamente y la efectividad de Mailscanner es reconocida mundialmente, sin embargo, hay mensajes de correo electrónico que no llevan virus adjuntos sino que intentan infectar su computadora al momento de visualizarlos en pantalla, por ello siempre es recomendable que se tenga un software anti-virus instalado en su computadora.

Mailscanner trabaja junto con SpamAssassin, software creado para ayudar a identificar los mensajes de correo electrónico publicitario no solicitado, también conocido como Spam.

SpamAssassin analiza los encabezados y el texto de los mensajes en busca de señales comunes del Spam. Por ejemplo, links para retirarse de la lista, frases de oferta o excusas para justificar el envío del mensaje.

Módulos del Fprot

F-Prot Antivirus Command-Line Scanner

El f-prot es una herramienta para explorar virus en archivos o directorios. Las opciones seleccionadas determinan que métodos se utilizan para la exploración así como la mejor característica de desinfección.

F-Prot Antivirus Daemon Scanner

Es un demonio que explora los archivos individuales, que son sometidos por una petición HTTP. devuelve informes ajustados en formato XML indicando si el archivo explorado fue infectado o no, si la desinfección tuvo éxito, etc. El demonio de exploración toma un solo argumento de la línea de comando, que es la ruta absoluta a la localización de los archivos de la firma y los archivos del mensaje.

F-Prot Antivirus Updater

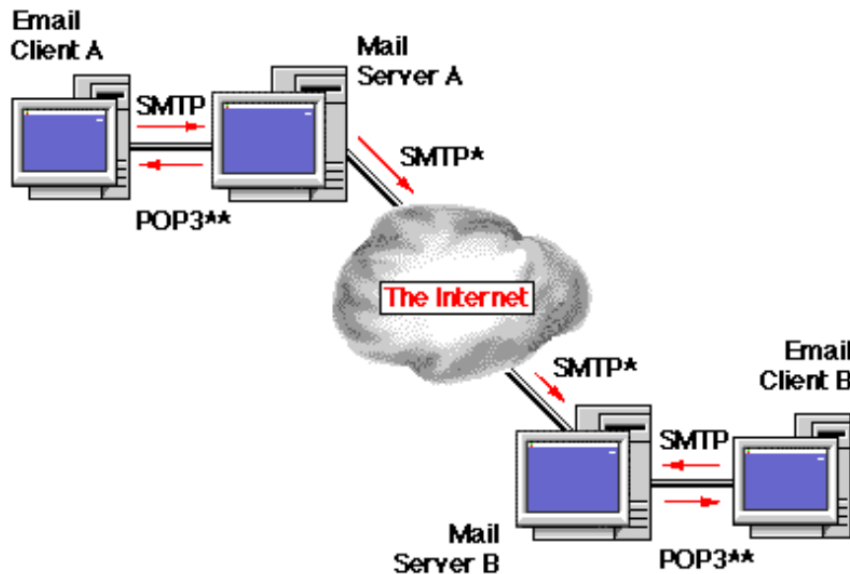
Es un scrip en Perl para la comprobación de actualizaciones de registro de virus en Internet, si hay actualizaciones por registros de nuevos virus, él las descargará e instalará.

F-Prot Antivirus Mail Scanner

Si F-Prot Antivirus detecta una infección en un mensaje o un adjunto, scan-mail.pl intentará neutralizar la amenaza. En caso de suprimir la infección se le indica que adjunte un mensaje de texto.

Vamos a partir de que tenemos un servidor de correo electrónico normal, en un sistema Linux , por ejemplo el sendmail como servidor y clientes outlook en PCs con windows. Primero veamos rápidamente como funciona este sistema (la instalación y configuración se encuentra en el documento de configuración de servicios de internet.pdf.

ESQUEMA GENERAL DEL CORREO TRADICIONAL CON LINUX



Cuando un cliente (por ejemplo con outlook) envía un correo electrónico, este sale de su PC y se almacena en la cola de correo de un servidor predefinido. Recuerden que al configurar una cuenta con outlook, deben definir quién es el servidor de correo saliente y entrante, o sea a quién le entregarán los correos para enviar y de donde leen los correos. Esta comunicación hacia el servidor se hace utilizando el protocolo SMTP (Simple Mail Transfer Protocol). El servidor procesa su cola de correo, hace las traducciones de DNS para encontrar los servidores de correo que atienden los diferentes dominios y si existe la comunicación con estos servidores, entregan el correo al servidor remoto. El correo no llega directamente al cliente o usuario final. Cuando el usuario final se conecta o programa su cliente (por ejemplo outlook) para leer correo de un servidor, en lapsos de tiempo, se autentica con este y descarga a su PC todos los correos que tengan para él, sin verificar su contenido, posibles virus, mensajes no deseados, etc, y todo esto llega al PC. Esta conexión se puede hacer por el protocolo POP3 o IMAP.

Aquí es donde juegan papel importante los filtros de correo para virus y spam. De tal forma que el servidor haga selección y filtrado de los correos que está almacenando, bien sea para enviar o para entregar a los PCs, y rechace, los que tengan virus, o patrones no deseados. De tal forma que cuando el cliente final lea el correo desde el servidor, este sea limpio y que no contenga correos de basura, etc.

3.5.7.1. INSTALACIÓN Y CONFIGURACIÓN DE ANTIVIRUS

Se pueden usar varios antivirus, reconocidos por el MailScanner, como f-prot, clamav.

Si se trabaja con f-prot:

Se copio el instalador que reside en el CD.

```
[root@condor F-prot]# cd /opt
[root@condor opt]# ls -l
total 6992
drwxr-xr-x  2 root root  4096 ene 27 19:38 fedora
-rw-r--r--  1 root root 3566043 jun 24  2005 fp-linux-fs-4[1].5.4.tar.gz
drwx-----  2 root root  16384 ene 27 15:35 lost+found
drwxr-xr-x 108 root bin   4096 abr 10  2005 webmin-1.200
```

Se descomprime el tar.gz

```
tar xvzf fp-linux-fs-4[1].5.4.tar.gz
```

Se descomprimió en /usr/local, pues así lo pide el programa perl.

Desde la carpeta respectiva, se corre el perl de instalación

```
[root@condor f-prot]# perl install-f-prot.pl
(c) FRISK Software International

http://www.f-prot.com/

    F - Prot Antivirus - File Server - for Unix.

#####
# You are starting the configuration part of the:  #
#   F - Prot Antivirus installation.             #
#####

Where do you want a symbolic link for F - Prot Antivirus to be generated?
[/usr/local/bin] :
Where do you want the symbolic links for section 8 manuals to be generated (man8)?
[/usr/share/man/man8/] :
Where do you want the symbolic links for the manuals for executable programs to be generated
(man1)?
[/usr/share/man/man1/] :
Where do you want a symbolic link for the F - Prot Antivirus Daemon Scanner (f-protd) to be
generated?
[/usr/local/sbin/] :

#####
# You are starting the file-check part of the:    #
#   F - Prot Antivirus installation.             #
#####

Checking file: '/usr/local/f-prot/f-prot': OK.
Checking file: '/usr/local/f-prot/man_pages/f-prot.1': OK.
Checking file: '/usr/local/f-prot/man_pages/check-updates.pl.8': OK.
Checking file: '/usr/local/f-prot/f-protd': OK.
Checking file: '/usr/local/f-prot/man_pages/f-protd.8': OK.
Checking file: '/usr/local/f-prot/tools/f-prot.so': OK.
Checking file: '/usr/local/f-prot/man_pages/f-prot.so.8': OK.
Checking file: '/usr/local/f-prot/tools/rc_scripts/f-protd.rc-redhat': OK.
Checking file: '/usr/local/f-prot/tools/rc_scripts/f-protd.rc-debian': OK.
Checking file: '/usr/local/f-prot/tools/rc_scripts/f-protd.rc-suse': OK.
Checking file: '/usr/local/f-prot/tools/rc_scripts/f-protd.rc-mandrake': OK.

#####
# You are starting the installation part of the:  #
```

```
# F - Prot Antivirus installation.          #
#####

Setting up symbolic link: /usr/local/bin/f-prot: OK.
Setting up symbolic link: /usr/share/man/man8/check-updates.pl.8: OK.
Setting up symbolic link: /usr/share/man/man1/f-prot.1: OK.
Setting up symbolic link: /usr/share/man/man8/f-protd.8: OK.
Setting up symbolic link: /usr/local/sbin/f-protd: OK.
Setting up symbolic link: /usr/share/man/man8/f-prot.so.8: OK.
Do you want to activate the F-Prot Antivirus daemon automatically now and
everytime your system is rebooted? (Y/n): y
Starting F-Prot Antivirus Daemon Scanner:      [ OK ]

Changing file permissions:

File permissions: /usr/local/f-prot/f-prot rwxr-x-r-x  OK.
File permissions: /usr/local/f-prot/tools/check-updates.pl rwx-----  OK.
File permissions: /usr/local/f-prot/f-protd rwxr-xr-x  OK.
Checking for new virus signatures:
*****
* F-Prot Antivirus Updater          *
*****

There's a new version of:
"Document/Office/Macro viruses" signatures on the web.
Starting to download...
Download completed.

There's a new version of:
"Application/Script viruses and Trojans" signatures on the web.
Starting to download...
Download completed.

Preparing to install Application/Script viruses and Trojans signatures.
Application/Script viruses and Trojans signatures have successfully been installed.

Preparing to install Document/Office/Macro viruses signatures.
Document/Office/Macro viruses signatures have successfully been installed.

*****
* Update completed successfully. *
*****

#####
# Installation of F - Prot Antivirus is completed. #
#####

[root@condor f-prot]#
```

Se hace una prueba de virus (el virus se simuló copiando un patrón de texto para crear el EICAR virus) con un archivo creado manualmente llamado virus.com:

Contenido del archivo virus.com

[X5O!P%@AP\[4\PZX54\(P^\)7CC\)7}\\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\\$H+H*](#)

```
[root@fw opt]# f-prot /opt/prueba.virus
```

```
Virus scanning report - 22 December 2005 @ 11:56
```

```
F-PROT ANTIVIRUS
```

```
Program version: 4.6.3
```

```
Engine version: 3.16.10
```

```
VIRUS SIGNATURE FILES
```

```
SIGN.DEF created 24 November 2005
```

```
SIGN2.DEF created 24 November 2005
```

```
MACRO.DEF created 20 November 2005
```

```
Search: /opt/prueba.virus
```

```
Action: Report only
```

```
Files: "Dumb" scan of all files
```

```
Switches: -ARCHIVE -PACKED -SERVER
```

```
/opt/prueba.virus Infection: EICAR_Test_File
```

```
Results of virus scanning:
```

```
Files: 1
```

```
MBRs: 0
```

```
Boot sectors: 0
```

```
Objects scanned: 1
```

```
Infected: 1
```

```
Suspicious: 0
```

```
Disinfected: 0
```

```
Deleted: 0
```

```
Renamed: 0
```

```
Time: 0:00
```

```
[root@fw opt]#
```

Al probar las actualizaciones automáticas debe asegurarse de que el servidor puede conectarse a internet identificándose con una IP pública, pues puede ocurrir lo siguiente:

```
[root@fw tools]# /usr/local/f-prot/tools/check-updates.pl
```

```
Unable to connect retrieve update info from server.
```

```
Error: Argumento inválido
```

```
Exiting...
```

```
[root@fw tools]#
```

Falla porque el equipo no puede conectarse a internet mediante una dirección IP pública. Esto se puede solucionar de dos formas:

- Que el equipo este conectado a internet directamente con una tarjeta a la cual se le asigna una dirección IP Pública.
- Que el equipo si esta dentro de una red con una IP privada, pueda recurrir a un dispositivo que le haga NAT (ejm: Firewall).

Por webmin, se revisa que este bien definido el default gateway (pues la va a hacer NAT). También se puede hacer por edición del archivo.

```
[root@demos network-scripts]# pwd
```

```
/etc/sysconfig/network-scripts
```

```
[root@demos network-scripts]# cat ifcfg-eth0
```

```
GATEWAY=192.168.19.1
```

```
BOOTPROTO=none
```

```
PEERDNS=yes
```

```
IPV6INIT=no
```

```
TYPE=Ethernet
```



```
HWADDR= Aquí va la MAC
DEVICE=eth0
NETMASK=255.255.255.0
BROADCAST=192.168.19.255
IPADDR=192.168.19.2
NETWORK=192.168.19.0
USERCTL=no
ONBOOT=yes
```

Se volvió a correr el proceso de las actualizaciones automaticas:

```
[root@fw ~]# cd /usr/local/f-prot/
[root@fw f-prot]# ls
CHANGES  etc      install-f-prot.pl  LICENSES-others  README  tmp
doc_ws    f-prot  LICENSE           MACRO.DEF        SIGN2.DEF  tools
ENGLISH.TX0  f-prot.sh  LICENSE-FPAV      man_pages        SIGN.DEF
[root@fw f-prot]# cd tools
[root@fw tools]# ls
check-updates.pl
[root@fw tools]# ./check-updates.pl
*****
* F-Prot Antivirus Updater          *
*****

There's a new version of:
"Document/Office/Macro viruses" signatures on the web.
Starting to download...
Download completed.

There's a new version of:
"Application/Script viruses and Trojans" signatures on the web.
Starting to download...
```

Se programo una tarea para que esta actualización la realice todos los días.
Se hizo editando el archivo de programación del cron para el usuario root, pero se puede hacer por el módulo del webmin. El contenido del archivo del root donde se programan las tareas del cron es:

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.12947 installed on Tue Oct 18 18:37:44 2005)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
5 2 * * * /usr/local/f-prot/tools/check-updates.pl -cron -quiet
# 5 2 * * 1-5 /opt/verifica.sh
0 1 * * * /opt/limpiatrash.sh
0 3,13 * * * /opt/restauraDerechos.sh
```

Este archivo reside en /var/spool/cron y se llama root. En este caso se observa que hay otras tareas programadas.

3.5.7.2. INSTALACIÓN, CONFIGURACIÓN MAILSCANNER E INTEGRACIÓN

Instalación del producto MailScanner e integración con el antivirus f-prot:

Desde /opt se descomprimió el instalador del MailScanner (el instalador se incluyó en el CD, pues es un producto de terceros).

```
[root@fw opt]# tar xvzf MailScanner-4.47.4-2.rpm.tar.gz
MailScanner-4.47.4-2/
MailScanner-4.47.4-2/perl-Archive-Zip-1.14-1.src.rpm
```

```

MailScanner-4.47.4-2/perl-Compress-Zlib-1.34-1.src.rpm
MailScanner-4.47.4-2/perl-Convert-BinHex-1.119-2.src.rpm
MailScanner-4.47.4-2/perl-Convert-TNEF-0.17-1.src.rpm
MailScanner-4.47.4-2/perl-ExtUtils-MakeMaker-6.30-1.src.rpm
MailScanner-4.47.4-2/perl-File-Spec-0.82-1.src.rpm
MailScanner-4.47.4-2/perl-File-Temp-0.16-1.src.rpm
MailScanner-4.47.4-2/perl-HTML-Parser-3.45-1.src.rpm
MailScanner-4.47.4-2/perl-HTML-Tagset-3.03-1.src.rpm
MailScanner-4.47.4-2/perl-IO-stringy-2.108-1.src.rpm
MailScanner-4.47.4-2/perl-MailTools-1.50-1.src.rpm
MailScanner-4.47.4-2/perl-MIME-tools-5.417-1.src.rpm
MailScanner-4.47.4-2/perl-Net-CIDR-0.10-1.src.rpm
MailScanner-4.47.4-2/perl-TimeDate-1.1301-3.src.rpm
MailScanner-4.47.4-2/MailScanner-perl-MIME-Base64-3.05-5.src.rpm
MailScanner-4.47.4-2/CheckModuleVersion
MailScanner-4.47.4-2/install.sh
MailScanner-4.47.4-2/README
MailScanner-4.47.4-2/ExtUtils-MakeMaker-6.30.tar.gz
MailScanner-4.47.4-2/tnef-1.2.3.1-1.i386.rpm
MailScanner-4.47.4-2/QuickInstall.txt
MailScanner-4.47.4-2/mailscanner-4.47.4-2.noarch.rpm
[root@fw opt]#
    
```

Se corre el install.sh , que verifica dependencias , e instala los módulos que hacen falta. Muestra una serie de mensajes y advierte que no nos preocupemos si hay muchos errores, etc y va instalando lo que considere que hace falta. Al final muestra algo como:

```

.....
.....
The important ones are HTML-Parser and MIME-tools.

Preparing... ##### [100%]
 1:perl-Convert-TNEF ##### [100%]

Oh good, module Compress::Zlib version 1.34 is already installed.

Oh good, module Archive::Zip version 1.14 is already installed.

Installing tnef decoder

Preparing... ##### [100%]
 1:tnef ##### [100%]

Now to install MailScanner itself.

NOTE: If you get lots of errors here, run the install.sh script
NOTE: again with the command "./install.sh nodeps"

Preparing... ##### [100%]
 1:mailscanner ##### [100%]

To activate MailScanner run the following commands:

service sendmail stop
chkconfig sendmail off
chkconfig --level 2345 MailScanner on
service MailScanner start
    
```

For technical support, please read the MAQ at www.mailscanner.biz/maq/
and buy the book at www.mailscanner.info/store

Please buy the MailScanner book from www.mailscanner.info/
It is a very useful administration guide and introduction
to MailScanner. All the proceeds go directly to making
MailScanner a better supported package than it is today.

```
[root@fw MailScanner-4.47.4-2]#
```

Se recomiendan los pasos para dejar activo el MailScanner:

```
[root@fw MailScanner-4.47.4-2]# service sendmail stop
Apagando sendmail: [ OK ]
Desactivaci3n de sm-client: [ OK ]
[root@fw MailScanner-4.47.4-2]# chkconfig sendmail off
[root@fw MailScanner-4.47.4-2]# chkconfig --level 2345 MailScanner on
[root@fw MailScanner-4.47.4-2]# service MailScanner start
Starting MailScanner daemons:
  incoming sendmail: [ OK ]
  outgoing sendmail: [ OK ]
  MailScanner: [ OK ]
[root@fw MailScanner-4.47.4-2]#
```

Se verifica el estado del MailScanner:

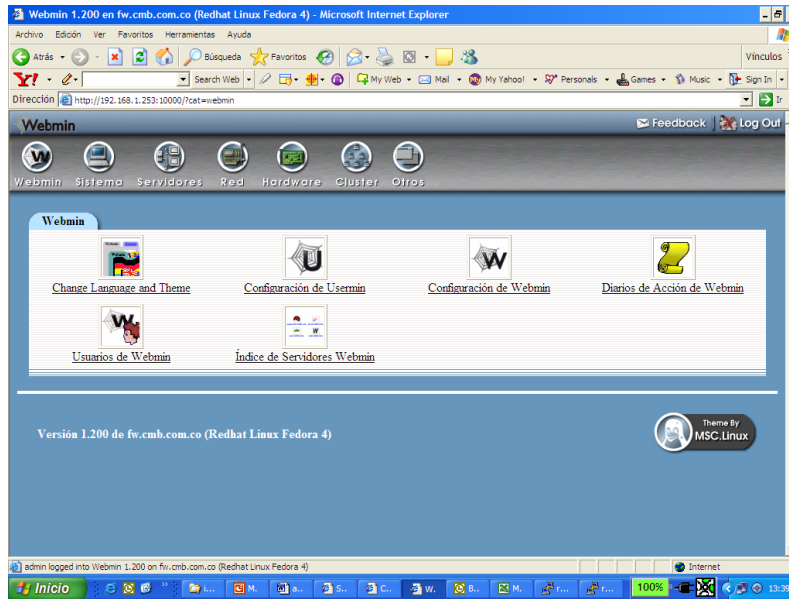
```
[root@fw MailScanner-4.47.4-2]# service MailScanner status
Checking MailScanner daemons:
  MailScanner: [ OK ]
  incoming sendmail: [ OK ]
  outgoing sendmail: [ OK ]
[root@fw MailScanner-4.47.4-2]#
```

Observemos que hay un proceso de recepci3n de correo (incoming), uno de envi3 (outgoing) y el MailScanner como tal. Estos reemplazan al sendmail en si (si se desea volver al servicio de sendmail anterior se debe recurrir a la copia que se recomend3 hacer).

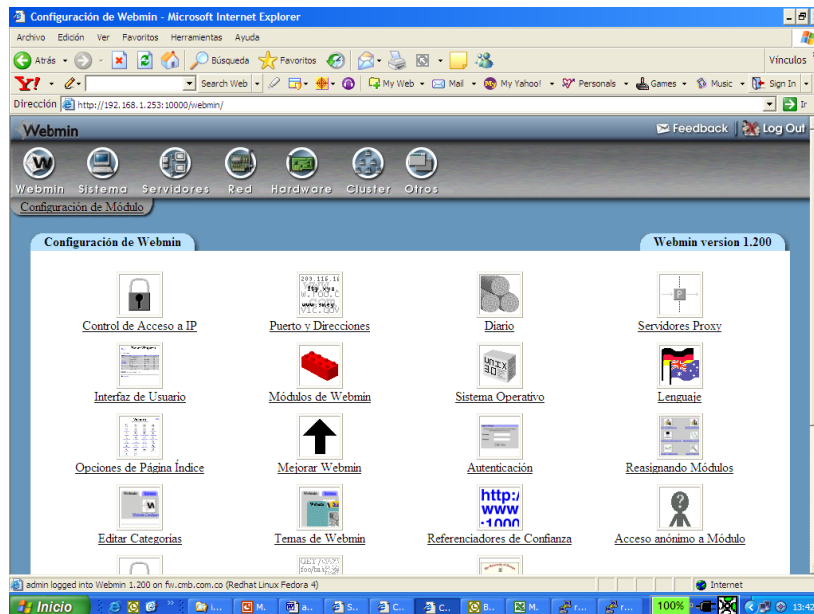
La configuraci3n del MailScanner, se puede hacer por edici3n del archivo de configuraci3n o por medio de un interfaz gr3fico (como el webmin, si se tiene el m3dulo respectivo).

- Configuraci3n por medio del webmin

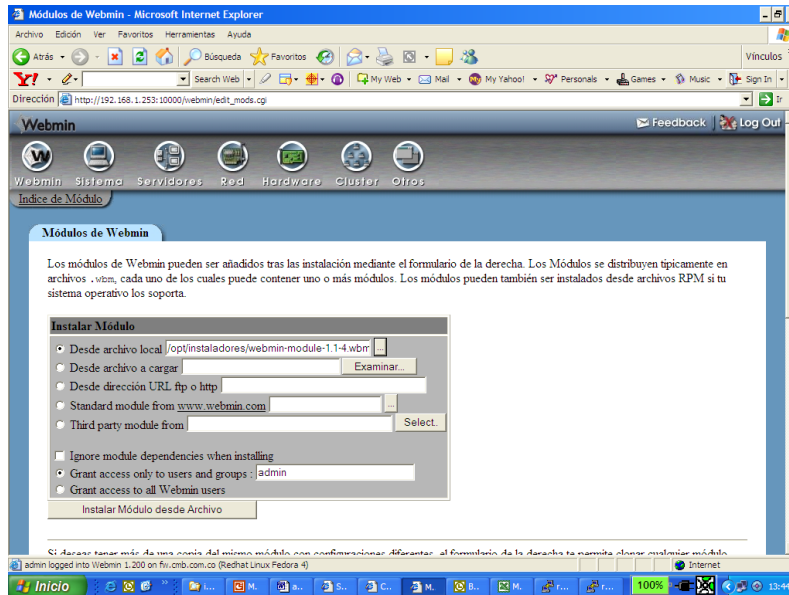
Se va a instalar el m3dulo del webmin para administrar MailScanner por webmin, para no tener que recurrir a la configuraci3n por manipulaci3n del archivo. El m3dulo del webmin se descarg3 por internet. Luego desde configuraci3n del webmin:



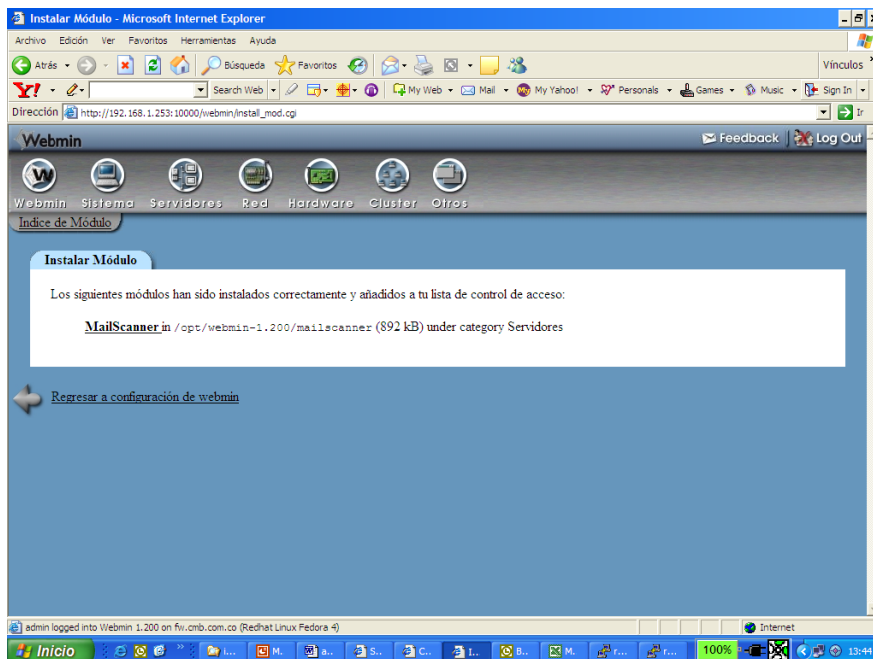
Por módulos:



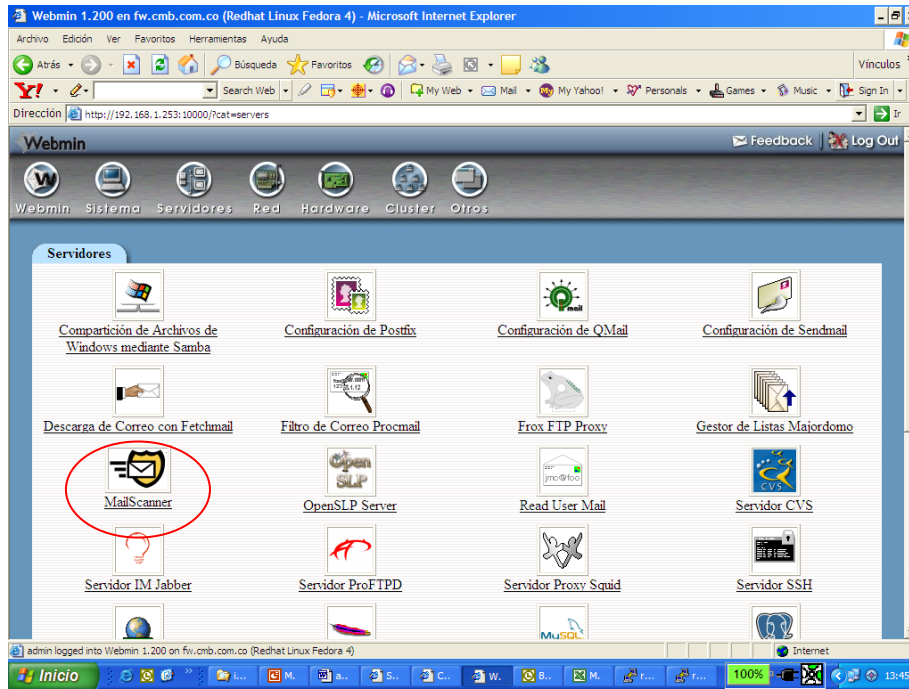
Se le indica la ruta del archivo con el módulo:



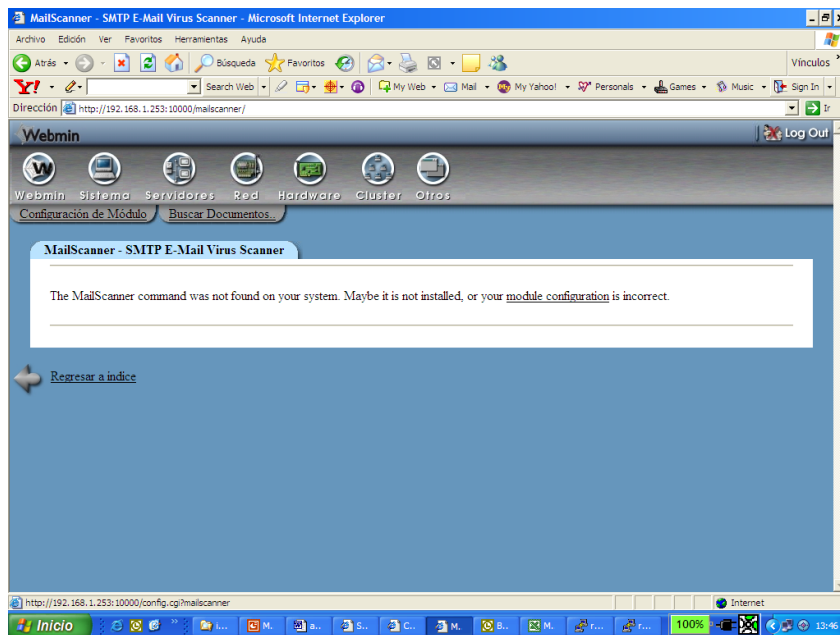
Y se adiciona:

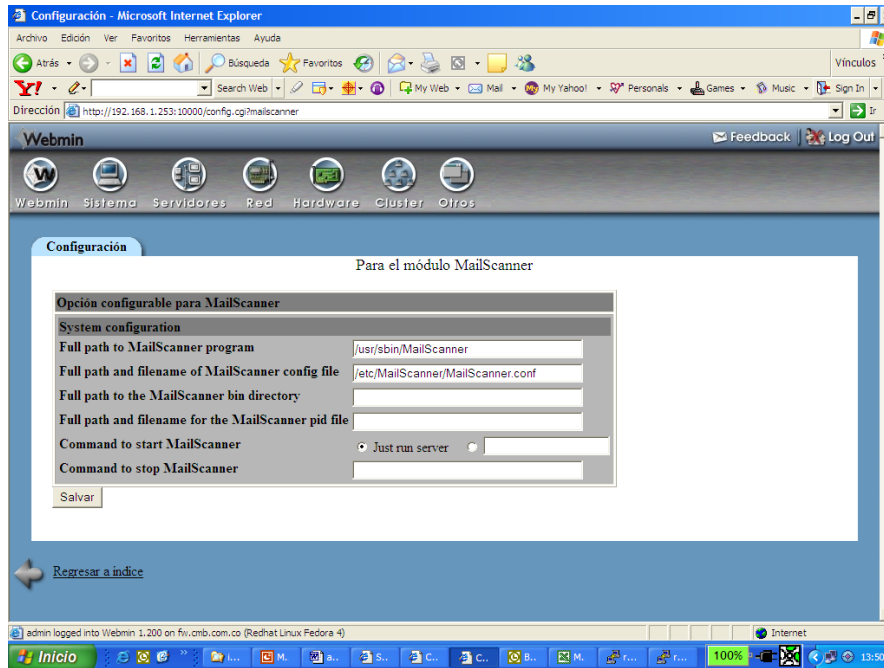


Se verifica por servidores que ya aparezca :

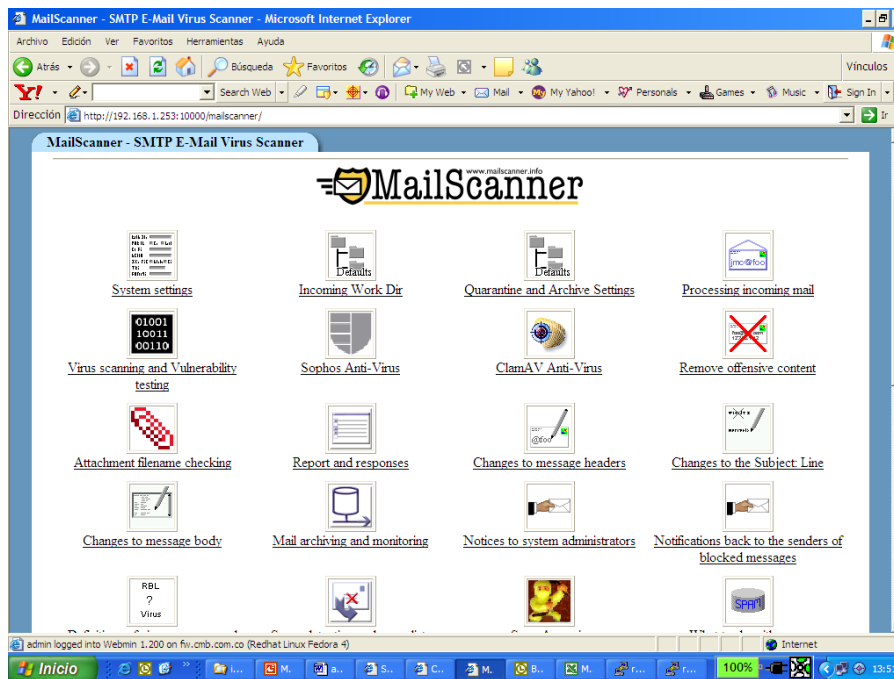


La primera vez que se ingresa, hay que suministrar cierta información sobre este:

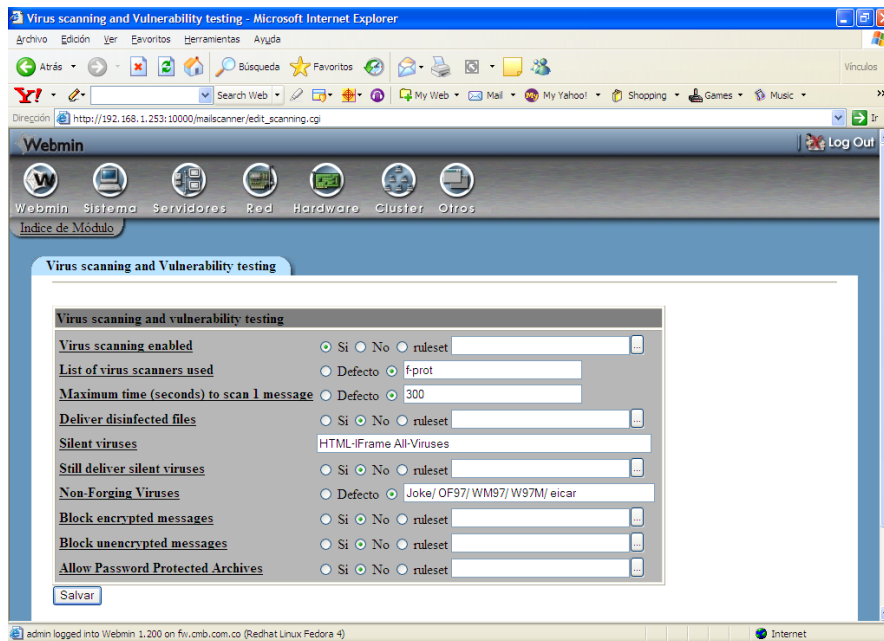




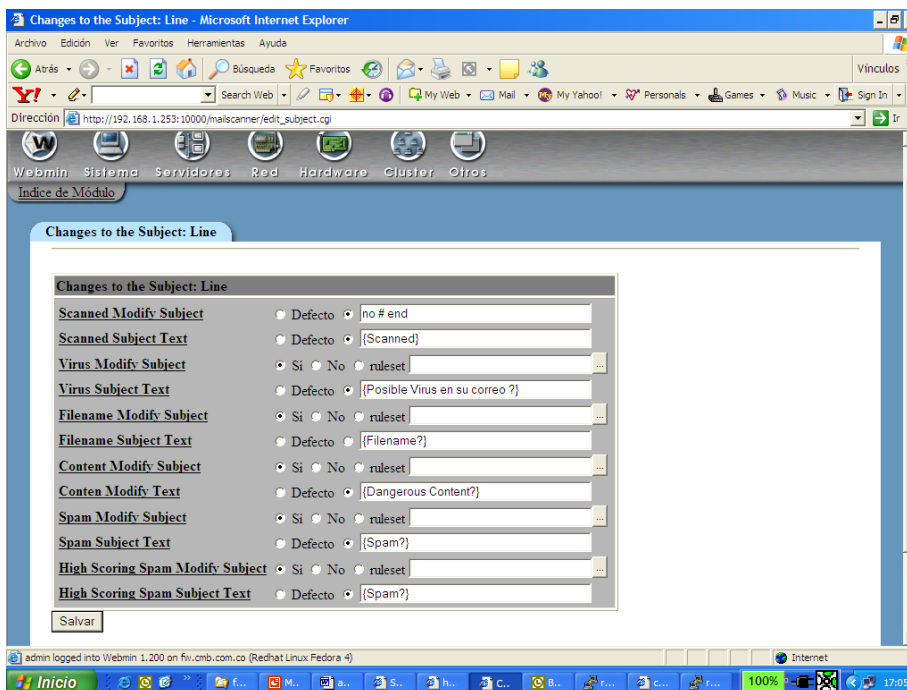
Se salva y se puede ya ingresar a las opciones



Ya se puede hacer la configuración desde aquí, por ejemplo definir con que antivirus se integrará (en este caso el clamav):



Se pueden configurar otras opciones como:



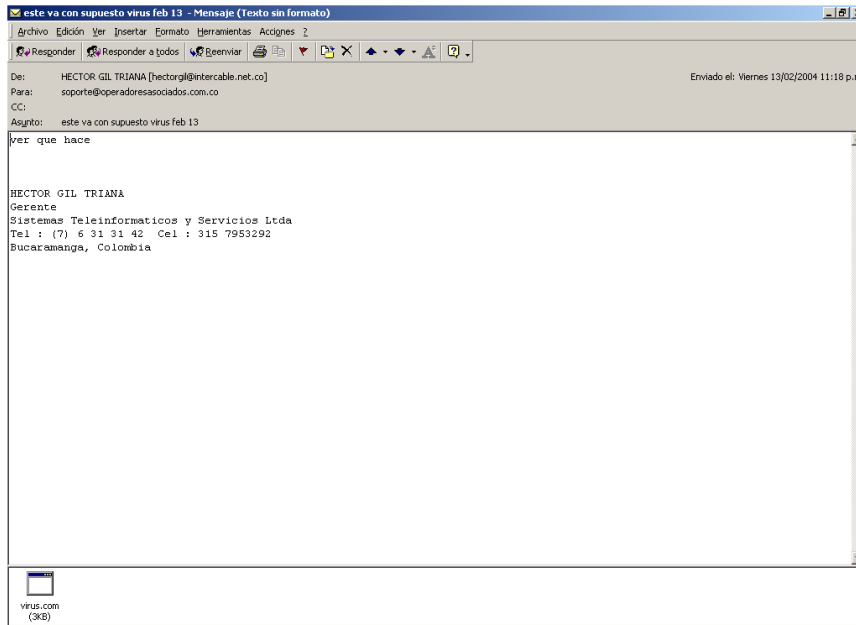
Cuando se hacen cambios al MailScanner, este se debe reiniciar:

```
[root@fw MailScanner]# service MailScanner stop
Shutting down MailScanner daemons:
  MailScanner:          [ OK ]
  incoming sendmail:    [ OK ]
  outgoing sendmail:    [ OK ]
[root@fw MailScanner]# service MailScanner start
Starting MailScanner daemons:
  incoming sendmail:    [ OK ]
  outgoing sendmail:    [ OK ]
  MailScanner:          [ OK ]
```

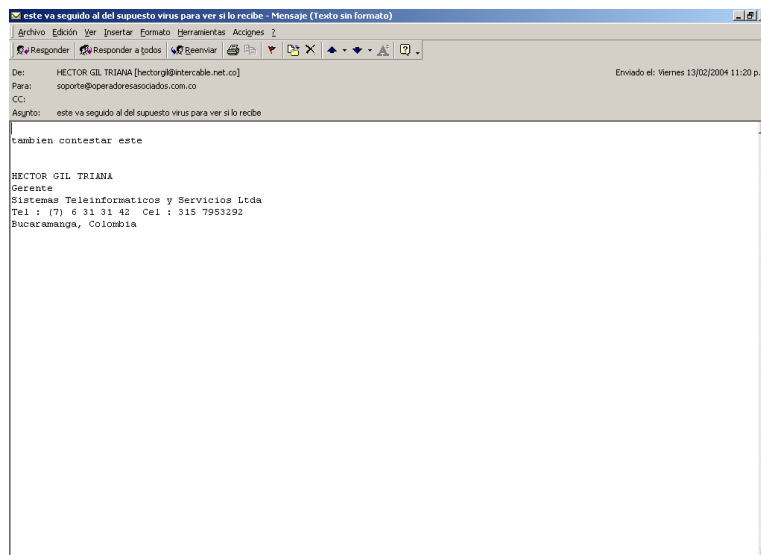

Se procede a hacer pruebas de envío de correo externo , con posibles virus para ver como se comporta. Para esto, se utilizó el servidor de correo de nuestra empresa.

Desde outlook, a través se envió un correo con el supuesto virus creado por nosotros en un archivo, para ver como reacciona el mail scan.

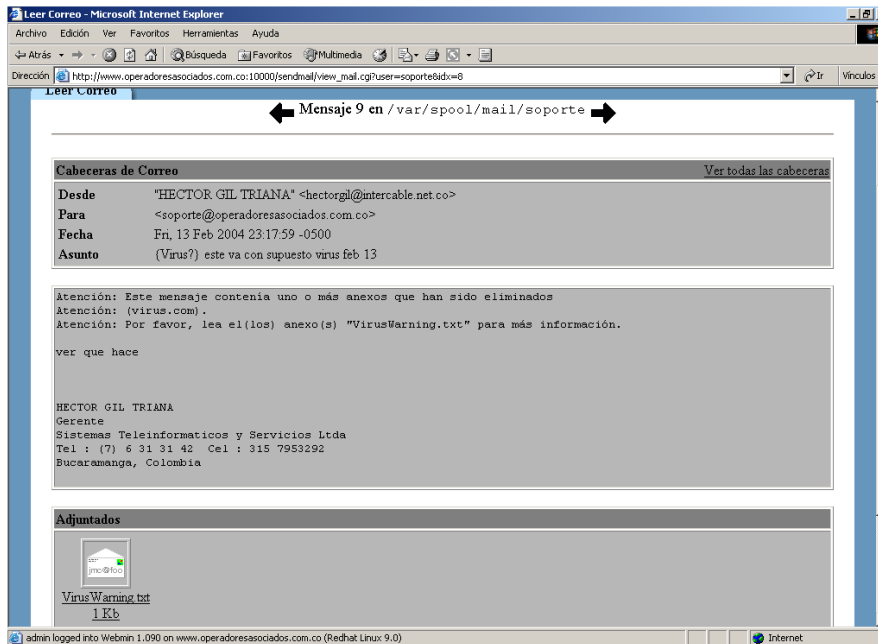
En la máquina de la empresa , active que se notifique a los usuarios de esto y que use también un filtro de SPAM (se puede usar el módulo MCP del MailScanner o spamassasin). Se comprueba enviando correo con supuesto virus. La pantalla de enviar desde outlook mostraba:



Luego se envia otro a continuación sin archivo anexo, sin virus

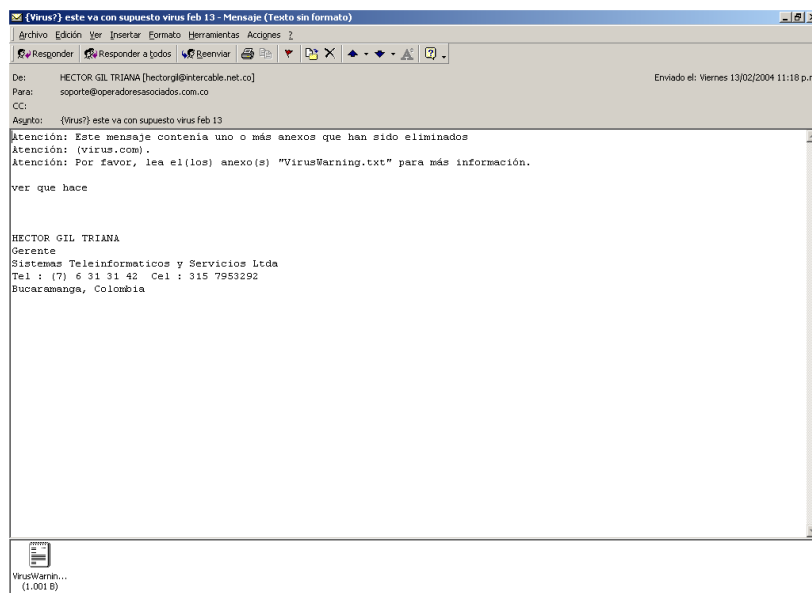


Luego se ingresa por webmin a ver el correo de la maquina de la empresa , para el usuario soporte y se ve que recibió el correo, pero notifica que lo limpio y quito archivos anexos por virus.

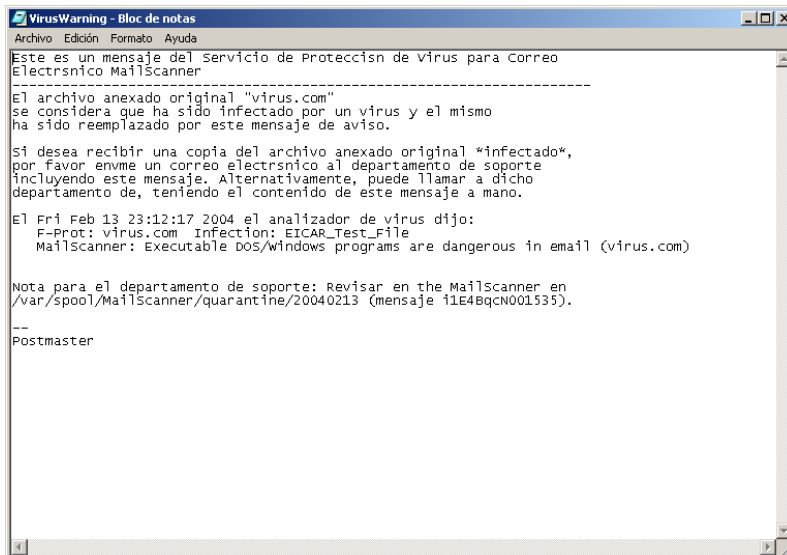


El siguiente mensaje que envié sin virus si llego bien.

Si el correo se lee en la empresa con outlook, por ejemplo, llega así:



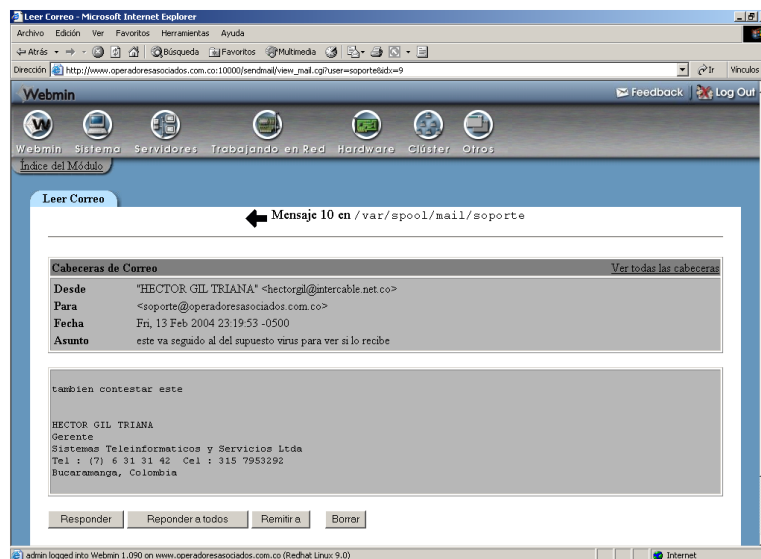
Y si se ve el mensaje de texto que reemplazo el attachment, encontramos



Si se verifica que el archivo esta en cuarentena (allí aparece con el número citado en el correo):

```
[root@www root]# cd /var/spool/
[root@www spool]# cd MailScanner/quarantine/
[root@www quarantine]# ls
20040211 20040213 20040214 20040215 20040216
[root@www quarantine]# ls -l
total 20
drwx----- 80 root root 4096 feb 11 15:09 20040211
drwx----- 3 root root 4096 feb 13 23:12 20040213
drwx----- 4 root root 4096 feb 14 16:32 20040214
drwx----- 4 root root 4096 feb 15 12:46 20040215
drwx----- 5 root root 4096 feb 16 17:50 20040216
[root@www quarantine]# cd 20040213
[root@www 20040213]# ls
i1E4BqcN001535
[root@www 20040213]#
```

El otro correo que si estaba bien, llego completo.



Con esto se comprueba que el MailScanner esta filtrando bien, la parte de virus.

3.5.7.3. PARA COMPLEMENTAR

Se desea poder filtrar correo no deseado, con textos en el encabezado (subject) y en el cuerpo del correo (body). Esto se puede hacer con reglas implementadas por el spamassassin (que viene con el sistema operativo) , o con el módulo del MCP del MailScanner. Cuaquiera de los dos que se use, se le debe indicar al MailScanner que se integre con ellos. Investigar que labores se debe adelantar para lograr esto y hacer las pruebas pertinentes.

3.5.8. TALLER SERVICIO DE CORREO CON FILTRADO DE VIRUS Y SPAM

Al finalizar el módulo, en las máquinas Linux de la sala , montar varios servidores de correo, que haga el filtrado de virus y correo no deseado (por palabras en el asunto y en el cuerpo del correo). Recuerden que para esto se debe tener un servidor DNS corriendo en la sala, que resuelva los nombres del dominio y de los servidores a implementar.

Las personas de cada fila, deben configurar también los equipos clientes (con webmin y otros con outlook) para leer y enviar los correos y hacer las pruebas pertinentes.

3.5.9. CONFIGURACION DE INTERFAZ WEB PARA CORREO

Procedemos con la configuración del squirrelmail, para manejo gráfico (web) del correo.

Se recurrirá al producto squirrelmail. Con el sistema esta instalado:

```
[root@fw instaladores]# rpm -a -q | grep squirrel
squirrelmail-1.4.4-2
```

Si no esta instalado, se debe obtener el paquete rpm (archivo instalador) y se procede con la instalación:

```
[root@hector rpm]# rpm -ivh squirrelmail-1.4.8-4.el5.noarch.rpm
advertencia:squirrelmail-1.4.8-4.el5.noarch.rpm: CabeceraV3 DSA signature: NOKEY, key ID
82fd17b2
Preparando... ##### [100%]
 1:squirrelmail ##### [100%]
[root@hector rpm]#
```

Los archivo residen en :

```
[root@fw squirrelmail]# pwd
/usr/share/squirrelmail
[root@fw squirrelmail]# ls
class config functions help images include index.php locale plugins src themes
[root@fw squirrelmail]#
```

Desde la carpeta de config se corre el archivo perl de configuracion:

```
[root@fw config]# pwd
/usr/share/squirrelmail/config
[root@fw config]# ls
config_default.php config_local.php config.php conf.pl index.php
[root@fw config]#
```

La ruta completa de la carpeta es: /usr/share/squirrelmail/config

Se corre el conf.pl con perl:

```
# perl conf.pl
```

Y se escogen las diferentes opciones del menu:

Primero las preferencias:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
```

```
Main Menu --
```

1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

```
D. Set pre-defined settings for specific IMAP servers
```

- C Turn color off
- S Save data
- Q Quit

```
Command >> 1
```

Allí se puede cambiar el logo, y otras cosas, pero deben tener ya listos algunos archivos. Para un logo, por opción 2 (tener cuidado la ruta donde esta la imagen, pues si no se escribe completo asume que es la carpeta config:

```
Organization Preferences
```

1. Organization Name : HECTOR ESPECIALIZACION
2. Organization Logo : logo-correo.png
3. Org. Logo Width/Height : (308/111)
4. Organization Title : HECTOR CORREO VERSION 1
5. Signout Page :
6. Top Frame : _top
7. Provider link : <http://www.squirrelmail.org/>
8. Provider name : SquirrelMail

- R Return to Main Menu
- C Turn color off
- S Save data
- Q Quit

Para cambiar idioma, desde principal con opción 10 y luego opción 1

```
Language preferences
```

1. Default Language : es_ES
2. Default Charset : iso-8859-1
3. Enable lossy encoding : false

- R Return to Main Menu
- C Turn color off
- S Save data
- Q Quit

```
Command >>
```

Por la parte (2) de Server Settings, se configura:

```

Server Settings

General
-----
1. Domain           : localhost
2. Invert Time      : false
3. Sendmail or SMTP : Sendmail

A. Update IMAP Settings : localhost:143 (uw)
B. Change Sendmail Config : /usr/sbin/sendmail

R Return to Main Menu
C Turn color off
S Save data
Q Quit

Command >>
    
```

Dominio al que pertenece, dirección IP del servidor de correo, puerto IMAP (143), y otros.

```

Server Settings

General
-----
1. Domain           : espec.edu.co
2. Invert Time      : false
3. Sendmail or SMTP : Sendmail

IMAP Settings
-----
4. IMAP Server      : hector.espec.edu.co
5. IMAP Port        : 143
6. Authentication type : login
7. Secure IMAP (TLS) : false
8. Server software   : uw
9. Delimiter        : /

B. Change Sendmail Config : /usr/sbin/sendmail
H. Hide IMAP Server Settings

R Return to Main Menu
C Turn color off
S Save data
Q Quit
    
```

Se salvo la información, y se procedió a configurar el servidor web para que maneje un alias llamado /mail que apunte al directorio donde esta el squirrelmail:

Se incluye la línea:

```
Alias /mail "/usr/share/squirrelmail"
```

Y se reinicia el servicio web:

```

[root@fw squirrelmail]# service httpd stop
Parando httpd: [FALLÃ]
[root@fw squirrelmail]# service httpd start
    
```

```
Iniciando httpd: [ OK ]
[root@fw squirrelmail]#
```

Aquí mostro FALLA porque el servicio estaba apagado.

3.5.9.1. CONFIGURACIÓN DE PLUGGIN PARA EL CORREO WEB

En la carpeta de plugins hay unos básicos como:

```
[root@demos squirrelmail]# ls plugins/
abook_take  calendar      fortune  listcommands  newmail      squirrelspell
administrator  delete_move_next  index.php  mail_fetch    sent_subfolders  translate
bug_report  filters       info     message_details  spamcop
[root@demos squirrelmail]#
```

Por la opción 3 del menu principal, se definen los nombres de las carpetas donde se almacenaran los archivos manipulados por el interfaz web para cada usuario dentro de su directorio de trabajo. Pueden quedar:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-----
Folder Defaults
1. Default Folder Prefix      : mail/
2. Show Folder Prefix Option  : true
3. Trash Folder               : INBOX.Trash
4. Sent Folder                : INBOX.Sent
5. Drafts Folder              : INBOX.Drafts
6. By default, move to trash  : true
7. By default, move to sent   : true
8. By default, save as draft  : true
9. List Special Folders First : true
10. Show Special Folders Color : true
11. Auto Expunge              : true
12. Default Sub. of INBOX     : false
13. Show 'Contain Sub.' Option : true
14. Default Unseen Notify     : 2
15. Default Unseen Type       : 1
16. Auto Create Special Folders : true
17. Folder Delete Bypasses Trash : false
18. Enable /NoSelect folder fix : false
```

```
R Return to Main Menu
C Turn color off
S Save data
Q Quit
```

```
Command >>
```

Según esto, dentro del directorio de trabajo de cada usuario se tienen elementos como:

```
Mail ( directorio donde residen los correos manipulados por el interfaz gráfico)
INBOX.Sent ( Residen los archivos enviados por el interfaz web)
INBOX.Trash ( Residen los archivos borrados por el interfaz web)
INBOX. Drafts( Residen los archivos en borrador por el interfaz web)
```

Hay que tener cuidado pues estas estructuras pueden ocupar mucho espacio en disco y se debe de estar limpiando o configurar desde las opciones del interfaz web para que no se usen.

Por la opción 7 del menu principal se puede definir un mensaje que aparezca a los usuarios cuando ingresen, puede ser:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-----  
Message of the Day (MOTD)
```

```
BIENVENIDO AL SISTEMA DE CORREO DE ST&S . HOY A LAS 10PM SE SUSPENDERA EL  
SERVICIO
```

```
1 Edit the MOTD
```

```
R Return to Main Menu
```

```
C Turn color off
```

```
S Save data
```

```
Q Quit
```

```
Command >>
```

Por la opción 10 del menú principal definimos el idioma, y puede quedar:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-----  
Language preferences
```

```
1. Default Language : es_ES
```

```
2. Default Charset : iso-8859-1
```

```
3. Enable lossy encoding : false
```

```
R Return to Main Menu
```

```
C Turn color off
```

```
S Save data
```

```
Q Quit
```

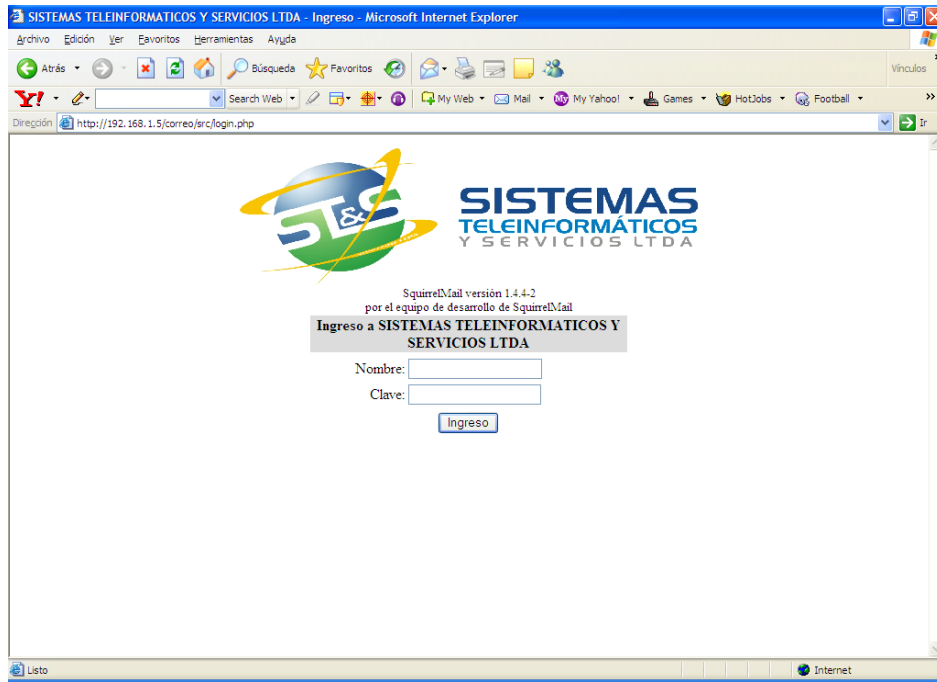
```
Command >>
```

Por la opción 9, se manejan los pluggins que enriqueceran el interfaz web, pero primero comprobaremos como esta hasta ahora el sitio web.

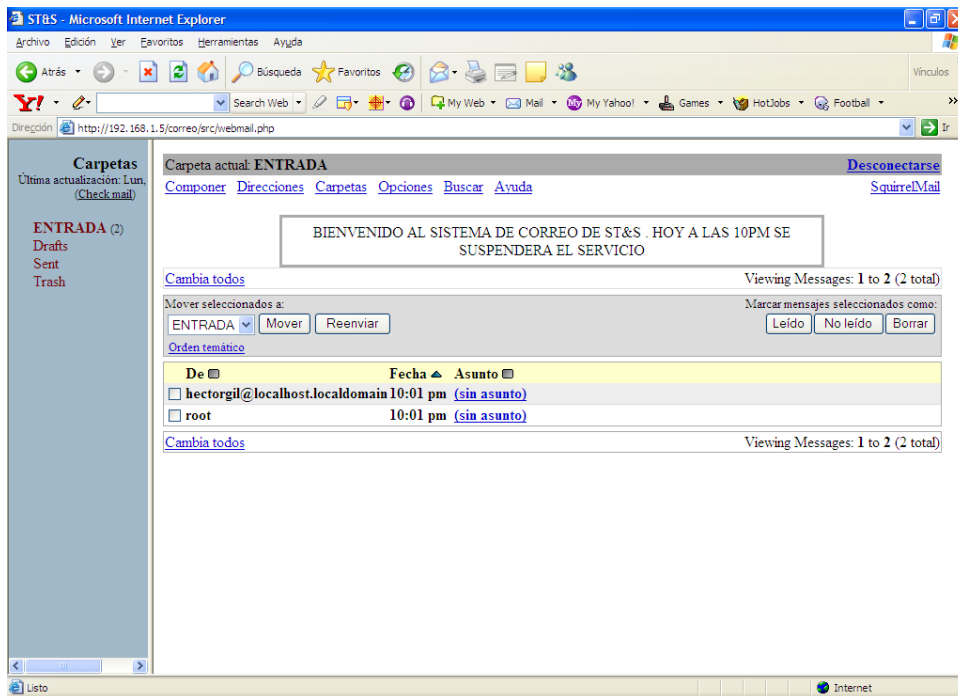
Para poder verlo desde el sitio web, debemos configurar en el apache, un alias que apunte a la carpeta donde reside el squirrelmail. Esto se hace modificando el archivo de configuración del apache (/etc/httpd/conf/httpd.conf) e incluyendo la siguiente línea:

```
Alias /correo "/usr/share/squirrelmail"
```

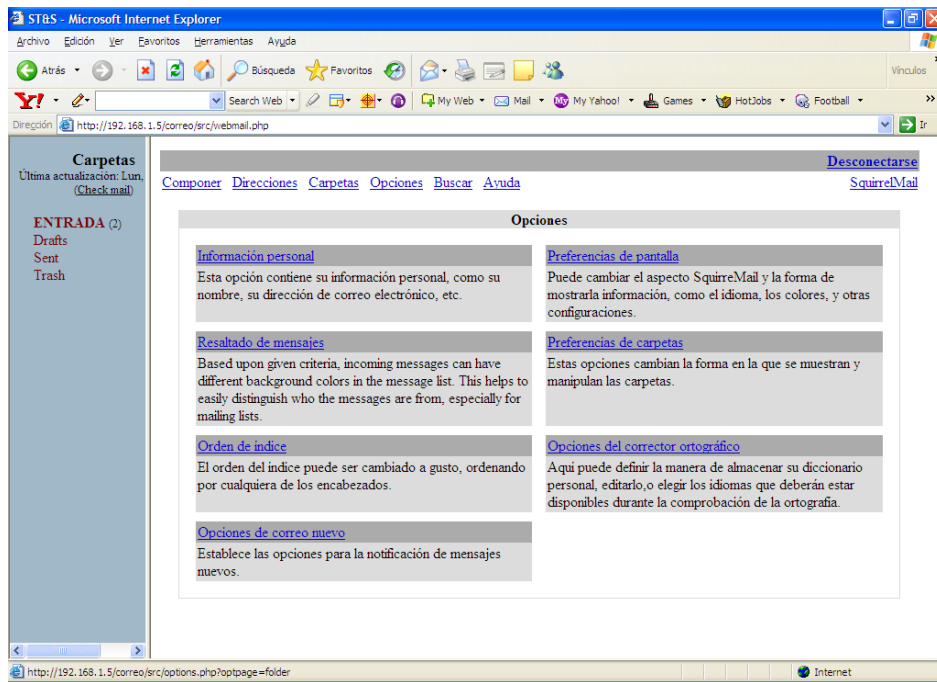
Se reinicia el servidor apache y se comprueba ingresando por el navegador con: (para este caso <http://192.168.1.5/correo>) y debe aparecer:



Al ingresar con el usuario (para este caso sts), se observa en la parte superior el mensaje de bienvenida especificado:



Por opciones solo se observa:



Y allí es donde vamos a incluir un plugin para permitir el cambio de clave del usuario desde el interfaz web.

Los plugins se ubicaron en /opt/pluggins y de allí se pasarán a la respectiva carpeta del squirrelmail:

```
[root@demos instaladores]# pwd
/opt/instaladores
[root@demos instaladores]# cd pluggins\ squirrelmail/
[root@demos pluggins squirrelmail]# ls
[root@demos pluggins squirrelmail]# ls
addgraphics-2.3-1.0.3.tar.gz  compatibility-2.0.4.tar.tar  saconf.1.0-1.2.7.tar.tar
calendar.0.2-1.2.3.tar.gz  disk_quota-3.1.1.tar.gz    show_user_and_ip-3.1-1.2.2.tar.gz
change_passwd-4.0-1.2.8.tar.gz  folder_sizes.1.4-1.4.tar.gz  user_logo_1_1.tar.gz
check_quota-1.1-1.2.7.tar.gz  global_sql_addressbook-0.5.tar.gz  username-2.3-1.0.0.tar.gz
check_quota-1.2-1.2.7.tar.gz  motd.1.2-1.0.3.tar.gz
compatibility-1.3.tar.gz  notify_1_3.tar.tar
[root@demos pluggins squirrelmail]#
```

Iniciaremos con el de compatibilidad , cambio de clave, notificación de nuevos correos.

Se copiaron los archivos a la carpeta del squirrelmail:

```
[root@demos pluggins squirrelmail]#
cp compatibility-1.3.tar.gz change_passwd-4.0-1.2.8.tar.gz /usr/share/squirrelmail/plugins/
[root@demos pluggins squirrelmail]#
```

- Compatibilidad

Se descomprimió el archivo (se trabajo con el de versión 1.3):

```
tar xvzf compatibility-1.3.tar.gz
```

Dentro de la carpeta respectiva se revisó el INSTALL, y se observa que solo se debe activar desde el menu de plugins.

Corriendo el perl conf.pl se adiciona el plugin de compatibility (por la opción 8)

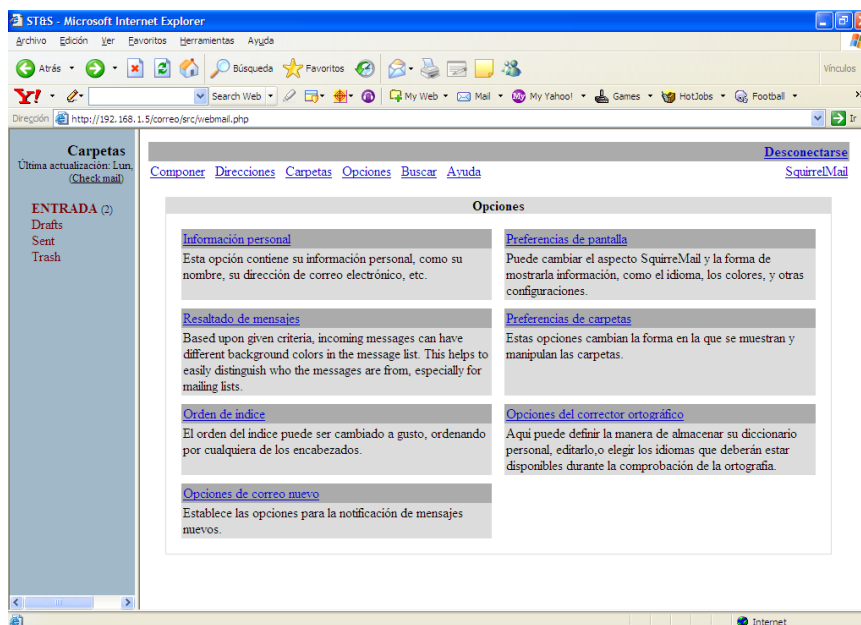
```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Plugins
Installed Plugins
 1. delete_move_next
 2. squirrelspell
 3. newmail
 4. compatibility

Available Plugins:
 5. translate
 6. fortune
 7. listcommands
 8. message_details
 9. info
10. spamcop
11. abook_take
12. bug_report
13. calendar
14. administrator
15. filters
16. mail_fetch
17. sent_subfolders

R Return to Main Menu
C Turn color off
S Save data
Q Quit

Command >>
```

Se verifica que el interfaz web , continua trabando y mostrando las opciones.



- Cambio de clave
- Desde la carpeta de plugins donde se había copiado previamente, se descomprime el archivo:

```
tar xvzf change_passwd-4.0-1.2.8.tar.gz
```

Desde la carpeta respectiva:

```
[root@demos plugins]# cd change_passwd
[root@demos change_passwd]# ls
chpasswd  config.php.sample  exec_test.php  getpot  INSTALL  options.php  setup.php
chpasswd.c  COPYING  functions.php  index.php  locale  README  version
[root@demos change_passwd]#
```

Se realizan los siguientes pasos:

```
$ cp config.php.sample config.php
$ vi config.php ( si es necesario cambiar algún parámetro de tiempo de vida de la clave, etc)
```

Se cambian los permisos:

```
[root@demos change_passwd]# chown root:apache chpasswd
[root@demos change_passwd]# chmod 4750 chpasswd
[root@demos change_passwd]# ls -l chpasswd
-rwsr-x--- 1 root apache 17917 abr 25 2004 chpasswd
[root@demos change_passwd]#
```

Ahora desde la carpeta conf, se corre el perl para adicionar el plugin y debe quedar.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

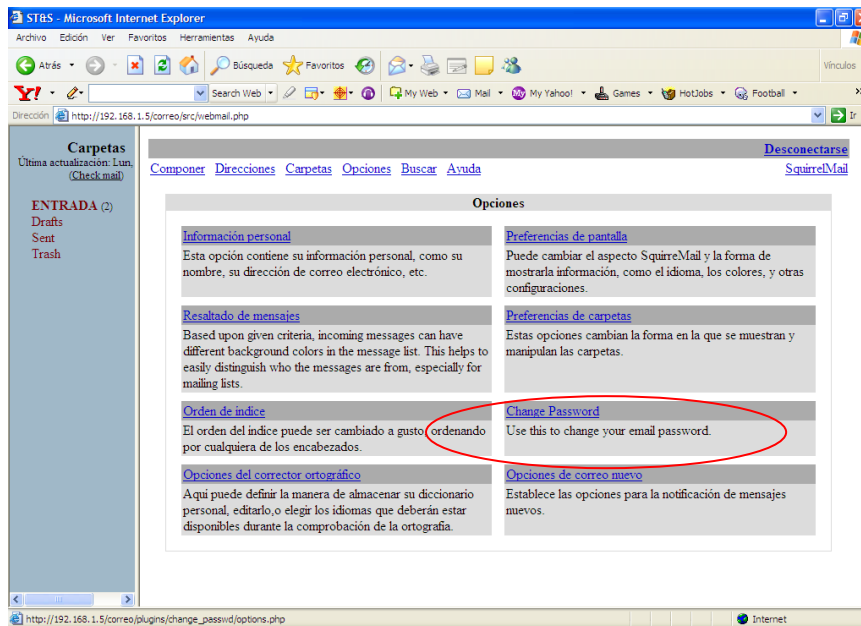
```
-----
Plugins
Installed Plugins
 1. delete_move_next
 2. squirrelspell
 3. newmail
 4. compatibility
 5. change_passwd

Available Plugins:
 6. translate
 7. fortune
 8. listcommands
 9. message_details
10. info
11. spamcop
12. abook_take
13. bug_report
14. calendar
15. administrator
16. filters
17. mail_fetch
18. sent_subfolders

R Return to Main Menu
C Turn color off
S Save data
Q Quit

Command >>
```

Al probar, se debe ver en opciones el permitir cambio de clave



Aparece en inglés pero lo vamos a cambiar para español:

En la carpeta del plugin respectivo, se editó el archivo functions.php, y se cambio la línea:

```
[root@demos change_passwd]# pwd
/usr/share/squirrelmail/plugins/change_passwd
```

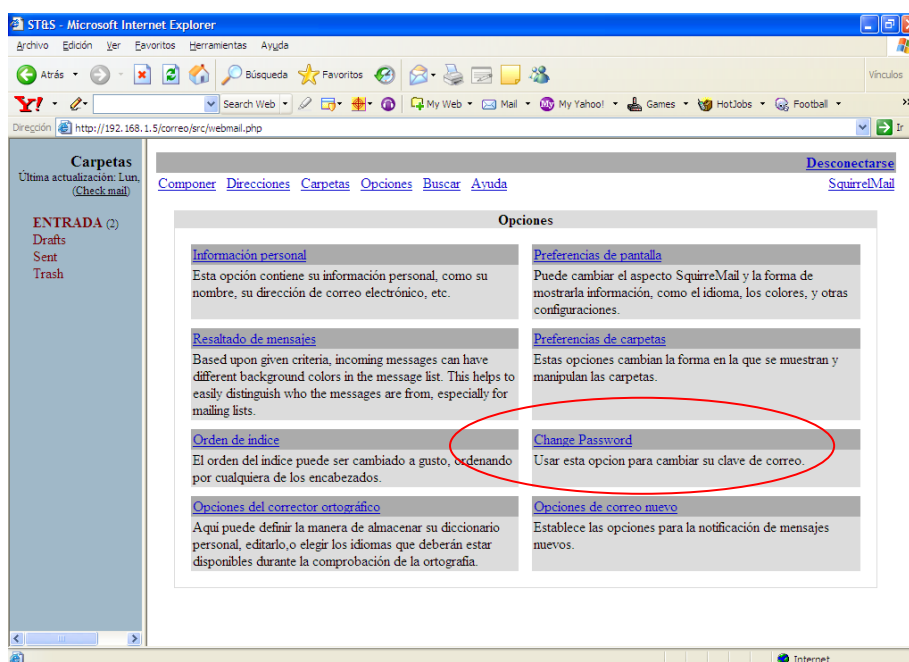
Estaba:

```
'desc' => _("Use this to change your email password."),
```

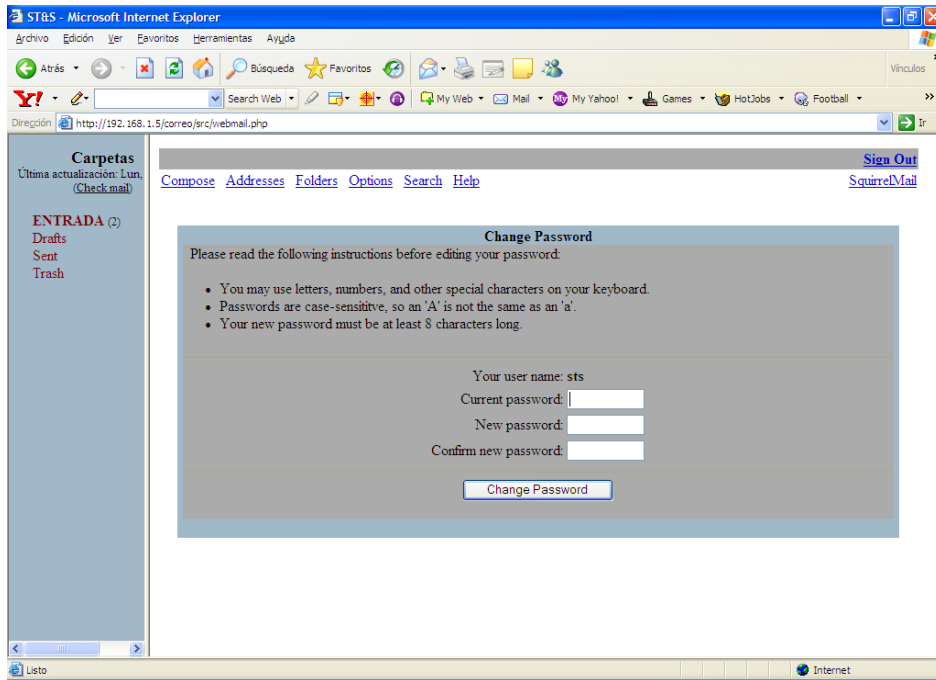
Se cambió por:

```
'desc' => _("Usar esta opcion para cambiar su clave de correo."),
```

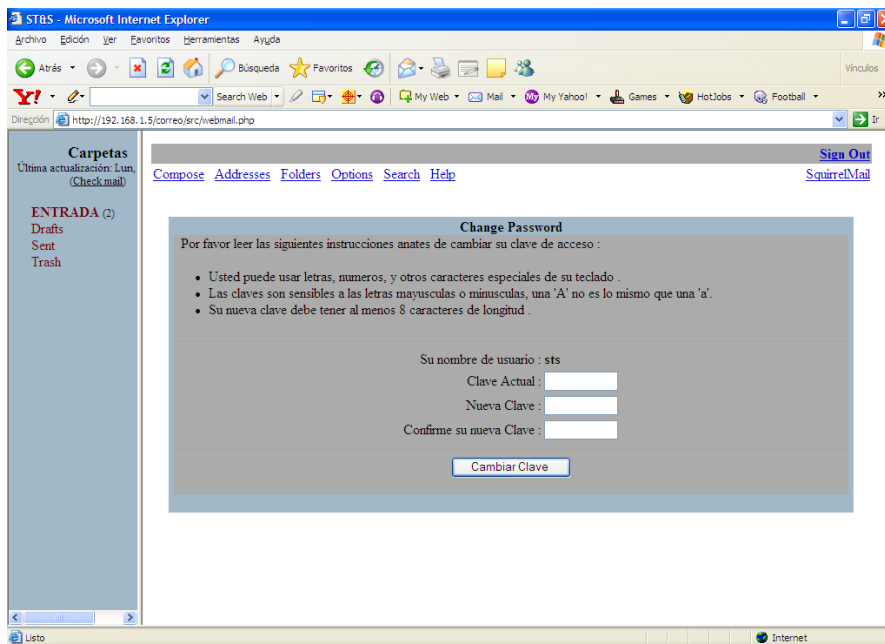
Ahora aparece:



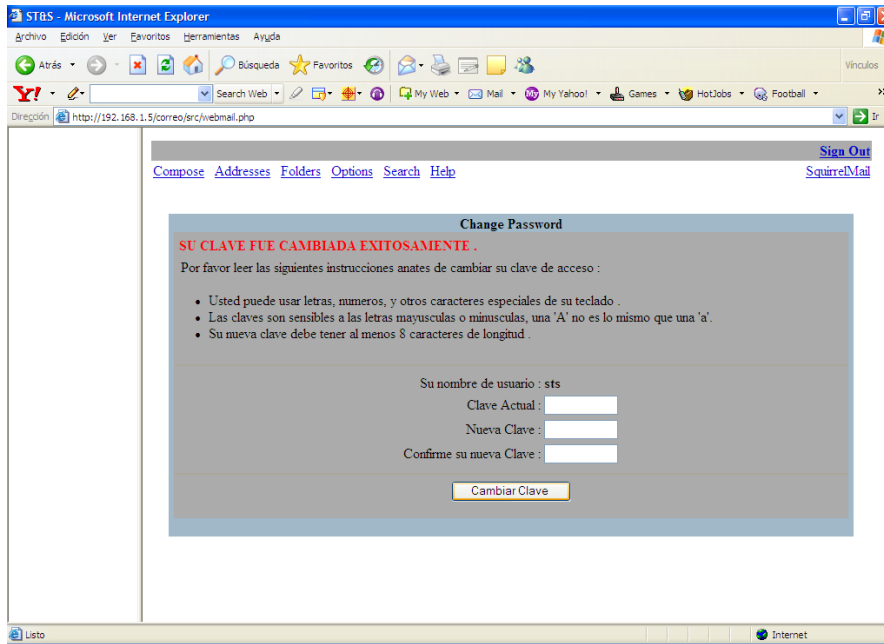
Al ingresar por la opción, los textos también están en inglés:



Editando el archivo options.php, se convirtió el texto al español y ahora queda:



Si la clave fue cambiada con éxito, muestra:



Todos estos mensajes los cambiamos con el editor de texto.

- Mostrar el nombre del usuario y la dirección IP

```
tar xvzf show_user_and_ip-3.1-1.2.2.tar.gz
```

```
[root@demos plugins]# cd show_user_and_ip
```

```
[root@demos show_user_and_ip]# ls
```

```
CHANGELOG config.php.sample functions.php index.php INSTALL LICENSE locale  
setup.php version
```

```
[root@demos show_user_and_ip]#
```

```
cp config.php.sample config.php
```

Al incorporar el pluggin debe aparecer:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-----  
Plugins
```

```
Installed Plugins
```

1. delete_move_next
2. squirreldspell
3. newmail
4. compatibility
5. change_passwd
6. [show_user_and_ip](#)

```
Available Plugins:
```

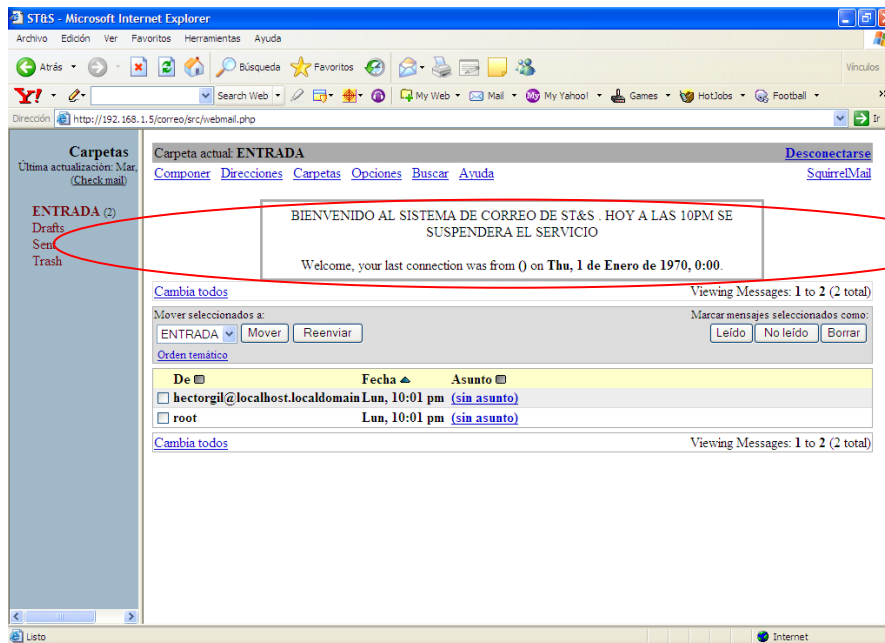
7. translate
8. fortune
9. listcommands
10. message_details
11. info
12. spamcop
13. abook_take
14. bug_report
15. saconf
16. calendar

- 17. administrator
- 18. filters
- 19. mail_fetch
- 20. sent_subfolders

- R Return to Main Menu
- C Turn color off
- S Save data
- Q Quit

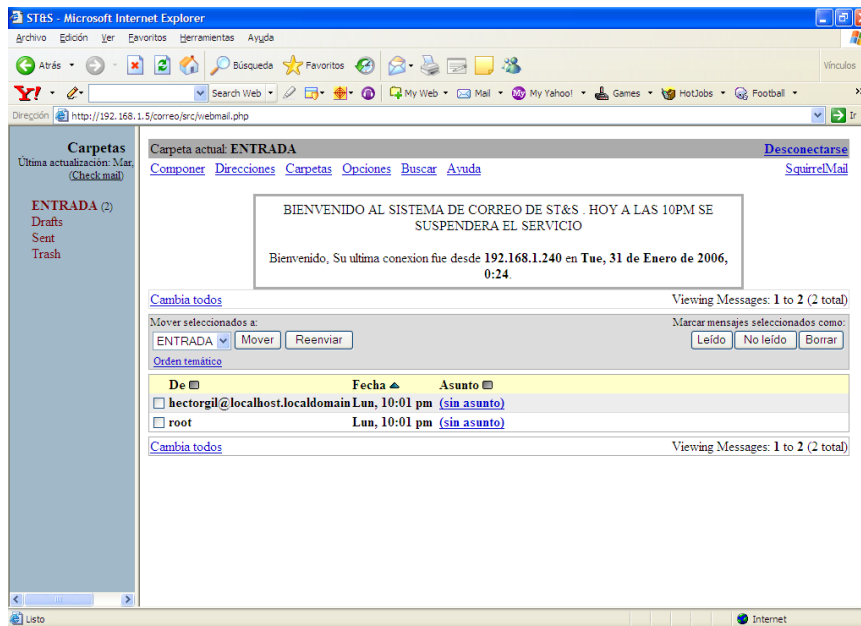
Command >>

Al comprobar , el mensaje aparece en inglés.



Se va a cambiar a español:

Se editó el archivo `functions.php` y se cambió el texto, pero falta cambiar mas. Por ahora al ingresar el usuario muestra:



3.5.10. MANEJO DE QUOTAS DE DISCO

Cuando un usuario tiene asignado un directorio dentro de una partición de disco, este puede escribir en ella hasta que la partición se llene, perjudicando a los demás usuarios y procesos que residen en esa partición. Es conveniente en algunas circunstancias asignar limites de consumo de espacio en disco dentro de una partición a un usuario y esto es llamado cuota de disco. Para el caso del correo electrónico, nos permite controlar el espacio que un usuario tiene para almacenar sus correos (tamaño de buzón), o el tamaño de los archivos manipulados por el interfaz web.

El proceso para asignar una cuota de disco a un usuario es:

Se debe activar el uso de cuota en la partición deseada, editando el archivo fstab y adicionando la opción de usrquota ,como se observa a continuación:

```
[root@servcorreo etc]# cat /etc/fstab
LABEL=/          /          ext3 defaults 1 1
none             /dev/pts   devpts gid=5,mode=620 0 0
LABEL=/home      /home      ext3 defaults,usrquota 1 2
LABEL=/opt       /opt       ext3 defaults 1 2
none            /proc      proc defaults 0 0
none            /dev/shm   tmpfs defaults 0 0
LABEL=/tmp       /tmp       ext3 defaults 1 2
LABEL=/usr       /usr       ext3 defaults 1 2
LABEL=/var       /var       ext3 defaults 1 2
/dev/sda7        swap       swap defaults 0 0
/dev/cdrom       /mnt/cdrom udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0         /mnt/floppy auto noauto,owner,kudzu 0 0
[root@servcorreo etc]#
```

En la partición deseada se debe crear un archivo llamado aquota.user con unos permisos 600 y cuyo dueño y grupo sea root, para almacenar información de las cuotas sobre esa partición. Si el archivo no existe, se puede forzar su creación con una utilidad propia del sistema operativo, como se menciona más adelante.

Se hace un reboot del sistema y al reinicia se corre un comando para verificar si ya están disponibles. Este comando chequea que el archivo aquota.user existe en la partición que se desea las cuotas y si no existe lo crea.

```
[root@servcorreo root]# quotacheck -vagumf
quotacheck: Scanning /dev/sda8 [/home] done
quotacheck: Checked 73 directories and 114 files
quotacheck: Old file not found.
[root@servcorreo root]# ls -l /home
total 40
-rw----- 1 root  root    7168 ene 28 11:55 aquota.user
drwx----- 4 clamav clamav  4096 ene 20 16:26 clamav
drwxrwx--- 4 correo1 apache  4096 ene 13 17:16 correo1
drwx----- 4 hectorgil apache  4096 ene 28 11:47 hectorgil
drwx----- 2 root  root   16384 ene 12 11:09 lost+found
drwxrwx--- 12 prueba  apache  4096 ene 28 11:49 prueba
[root@servcorreo root]#
```

- Verificar si la cuota esta activa en la partición. Usando el comando repquota:

```
# repquota /home
*** Report for user quotas on device /dev/sda8
Block grace time: 7days; Inode grace time: 7days

                Block limits          File limits
User           used  soft  hard  grace  used soft hard  grace
-----
root  --   32   0   0        2  0  0
postfix --    4   0   0        1  0  0
prueba --  840   0   0       194  0  0
correo1 --   92   0   0        22  0  0
clamav  --   76   0   0        18  0  0
hectorgil --  96   0   0        22  0  0
```

Podemos observar que el usuario hectorgil no tiene cuota asignada (valores de soft y hard en cero) y que ha utilizado 96 blocks de espacio en /home.

3.5.10.1. ASIGNACION DE QUOTAS A LOS USUARIOS

Se puede hacer por línea de comandos, o por medio del interfaz web webmin.

Por comandos se hace de la forma:

Definir cuota para un usuario con el comando edquota. Por defecto los usuarios no tienen cuota activa, y el valor de "0", así lo define (como se puede observar debajo de la columna soft, y hard en el ejemplo anterior. Cuando se invoca el comando edquota, se llama al editor vi y se debe de modificar la línea presentada:

```
# edquota hectorgil
```

```
Disk quotas for user hectorgil (uid 505):
Filesystem          blocks  soft  hard  inodes  soft  hard
/dev/sda8           96     300  500   22     0    0
```

Aquí se esta definiendo quota para la partición sda8 (/home). La quota se puede definir de acuerdo a los bloques de disco que un usuario puede usar en una partición (bloques de 1K), o por la cantidad de inodos. Se define el valor de soft (primer límite de la cantidad de espacio que puede usar) y hard (último límite al que se puede llegar). En el ejemplo 300 bloques (300 Kb) en los cuales el usuario ya es avisado de que esta superando la quota, pero aún puede llegar al último límite que es el hard (500 Kb).

Para verificar la quota de un usuario se puede invocar el comando quota nombreusuario:

```
[root@servcorreo hectorgil]# quota hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8   96  300  500      22   0   0
[root@servcorreo hectorgil]#
```

Si es el caso, se pueden definir quotas para otros usuarios tomando como modelo la quota asignada a anterior. Se usa la opción -p y el nombre del usuario que se tomará como base. Si el usuario anterior es hectorgil , podemos definir la quota para los otros usuarios (en este caso correo1) tomando como base a hectorgil:

```
[root@servcorreo hectorgil]# edquota -f /home -p hectorgil correo1
```

Se verifica:

```
[root@servcorreo hectorgil]# quota correo1
Disk quotas for user correo1 (uid 501):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8   92  300  500      22   0   0
```

La quota es asignada sin invocar al editor. Esto puede se muy útil para asignar masivamente quota a varios usuarios, como es el caso de servidores de correo donde a un grupo de usuarios le asignaran 10 Mb y a otros 5 Mb. Se requiere separar la lista de usuarios y correr un shell que realice esto, de forma automática leyendo de un archivo con los nombres de los usuarios, una vez estos estén creados, como se verá en el proceso de migración de cuentas.

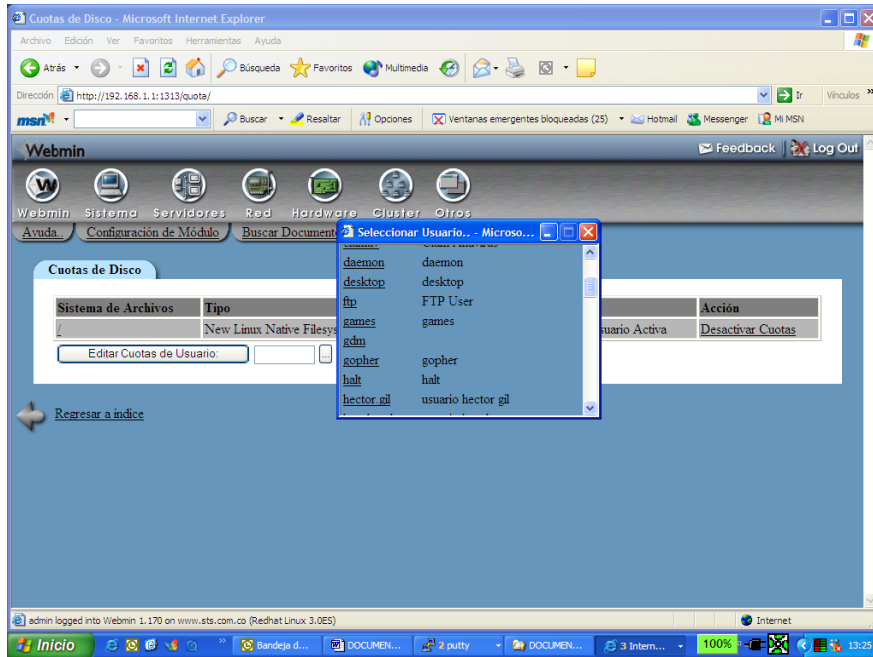
Si se va a asignar la quota por medio del interfaz gráfico webmin, se hace así:

Entrando por el icono de sistema, de la parte superior, podemos observar un icono para manejo de quotas del sistema operativo:

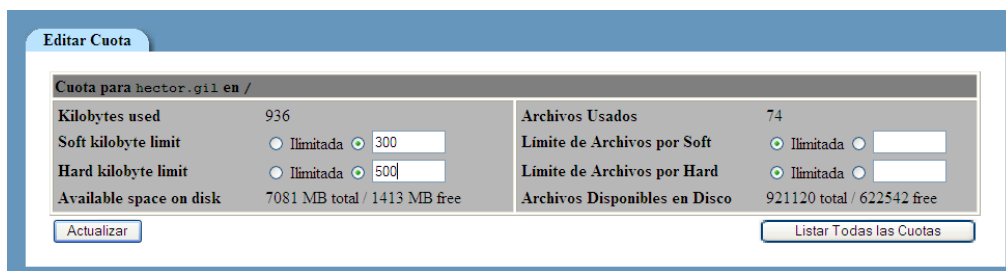


Allí podemos manejar las quotas de los usuarios, por ejemplo:

Nos ubicamos al final y buscamos el usuario al cual le vamos a cambiar sus parámetros. Luego indicamos que editar quota



Como pueden existir varias particiones en las cuales se defina cuota, aparece una lista de ellas y se debe escoger en cual partición se requiere editar estos valores y aparece:



Y se cambian los valores deseados y se indica actualizar.

3.5.10.2. PRUEBAS DEL CONTROL POR QUOTAS

Como la cuenta hectorgil es una cuenta de correo electrónico, y su buzón reside en la partición cuya cuota esta controlada, enviaremos unos correos con archivos anexos a la cuenta hectorgil que le definimos quota, por modo comandos y se irá monitoreando la cuota desde comandos:

```
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  196  5000  5000      31  0  0
[root@servinternet1 instaladores]# mail hectorgil@comultrasan.com.co < imap-2002d-2.i386.rpm
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  916  5000  5000      32  0  0
[root@servinternet1 instaladores]# mail hectorgil@comultrasan.com.co < imap-2002d-2.i386.rpm
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  1636  5000  5000      33  0  0
```

```
[root@servinternet1 instaladores]# mail hectorgil@comultrasan.com.co < imap-2002d-2.i386.rpm
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  2356 5000 5000      34  0  0
[root@servinternet1 instaladores]# mail hectorgil@comultrasan.com.co < imap-2002d-2.i386.rpm
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  3076 5000 5000      35  0  0
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  3076 5000 5000      35  0  0
[root@servinternet1 instaladores]#
```

Seguí enviando hasta que llene la cuota y trate de enviar uno más grande de los 450 K que le quedaban:

```
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  4520 5000 5000      38  0  0
[root@servinternet1 instaladores]# mail hectorgil@comultrasan.com.co < imap-2002d-2.i386.rpm
[root@servinternet1 instaladores]# quota -v hectorgil
Disk quotas for user hectorgil (uid 505):
  Filesystem blocks quota limit grace files quota limit grace
  /dev/sda8  4520 5000 5000      38  0  0
[root@servinternet1 instaladores]#
```

Los correos no le llegan , y si vemos la cola del servidor , pues desde allí mismo le estamos enviando los correos , se observa que estan represados por error en una rutina (es por la cuota llena):

```
[root@servinternet1 instaladores]# mailq
[root@hector mail]# mailq
  /var/spool/mqueue (1 request)
-----Q-ID----- --Size-- -----Q-Time----- -----Sender/Recipient-----
q14E8MV4005533 2170138 Sat Feb 4 09:08 <root@hector.espec.edu.co>
  (Deferred: local mailer (/usr/bin/procmail) exited with EX_TE)
  <prueba@hector.espec.edu.co>
Total requests: 1
```

Se debe liberar la cuenta para que le puedan llegar mas correos.

3.5.11. PARA COMPLEMENTAR

Se desea incorporar pluggins en el interfaz web del correo, que mejoren su presentación y que nos permitan:

- Visualizar la cuota de correo de los usuarios, para que estén atentos a la limpieza de sus áreas de trabajo y buzones.
- Notificar cuando un nuevo correo llega.

Y hacer las pruebas respetivas.

3.6. SERVICIO NFS (NETWORK FILE SYSTEM)

NFS es un servicio de red que permite a los usuarios de sistemas unix acceder los sistemas de archivos y directorios de otros equipos en la red. Los Hosts pueden ser de diferente marca y sistema operacional, desde que soporten este servicio. En general se usa entre máquinas Unix.

Se debe tener en cuenta los siguientes conceptos, pues de esto dependen las labores que se adelantarán en las respectivas máquinas.

Servidor: El hosts que permite el acceso a sus sistemas de archivos o directorios locales (este debe exportar sus recursos).

Cliente : El hosts que solicita el acceso a sistemas de archivos o directorios de otras máquinas (este debe montar los recursos exportados por otras máquinas).

3.6.1. CONFIGURANDO EL SERVIDOR NFS

Si se hace esta labor desde comandos unix, hay que editar el archivo donde el servidor exporta los recursos. El archivo **/etc/exports** permite poner a disposición de otros host, sus sistemas de archivos o directorios locales. Luego se procede con el comando **exportfs** .

Este comando arranca leyendo el archivo **/etc/exports**. Si el archivo exports es modificado, se debe volver a correr comando exportfs para actualizar.

Opciones Básicas del comando exportfs:

- a Exporta todos los recursos listados en /etc/exports.
- u Termina el export del recurso escrito a continuación.
- v Muestra mensajes de salida durante el proceso.

Cada línea del archivo exports es un recurso que se exportará o se va a prestar a otras máquinas, y tiene algunas opciones.

Por ejemplo, con este archivo export:

```
# cat /etc/exports
/a
/ccial
/sts -anon=0
/usr -anon=0
```

Se va a exportar la carpeta /a, /ccial y las dos últimas tienen unas opciones, para que le de mas derechos a root:

Para procesar este archivo se usa el comando exportfs:

```
# exportfs -va
re-exported /a
re-exported /ccial
exported /sts
exported /usr
```

En la máquina cliente (donde se utilizarán las carpetas) se crearon los puntos de montaje y se montaron los directorios (estas son las labores que debe realizar el equip cliente y que se mencionaran más adelante):

```
# mkdir usr2
```

```
# mkdir sts2

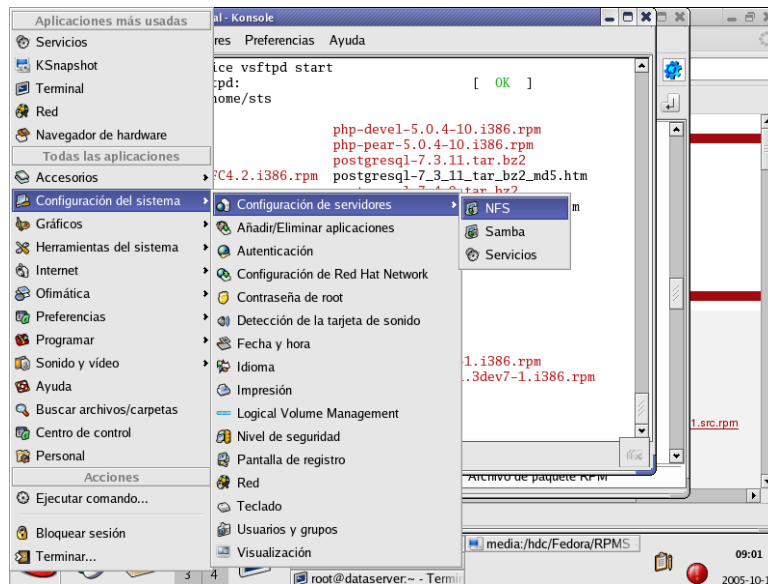
# mount 192.168.36.50:/sts /sts2
# mount 192.168.36.50:/usr /usr2
# df -k
/      (/dev/root      ): 56729641 blocks 17203102 i-nodes
/stand (/dev/boot     ): 19894 blocks  7664 i-nodes
/sts2  (192.168.36.50:/sts): 282078 blocks   0 i-nodes
/usr2  (192.168.36.50:/usr): 282078 blocks   0 i-nodes
```

Con el comando `df -k`, se verifican las particiones que tienen montadas en el sistema. Se observa que `sts2` y `usr2` ahora son particiones de la máquina (que realmente son directorios de la otra máquina).

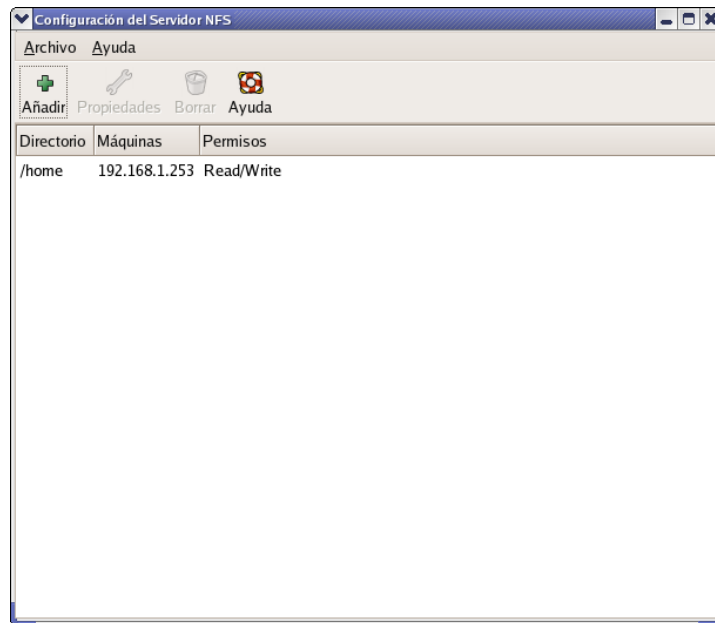
Exportando archivos y directorios mediante interfaz gráfico

Se puede hacer desde el escritorio KDE o desde el Webmin.

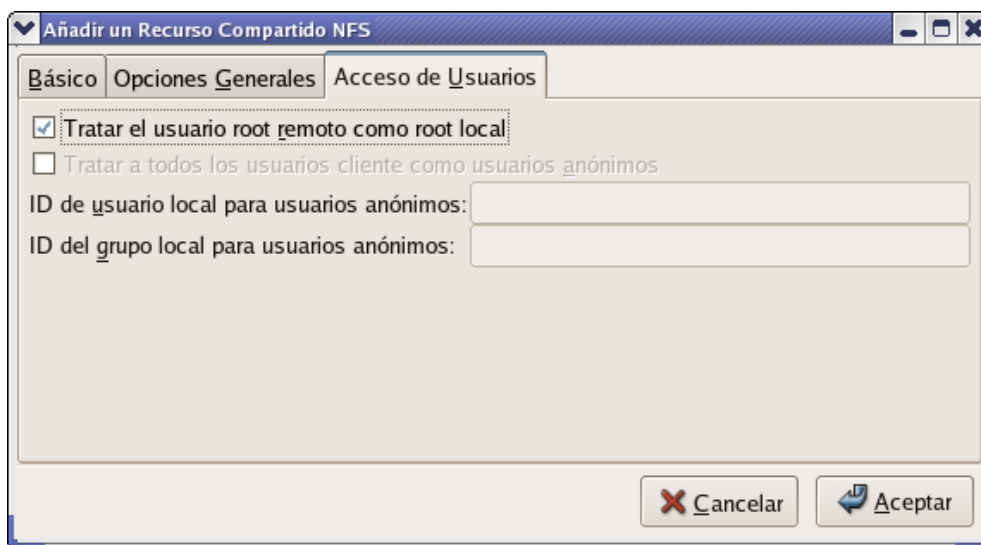
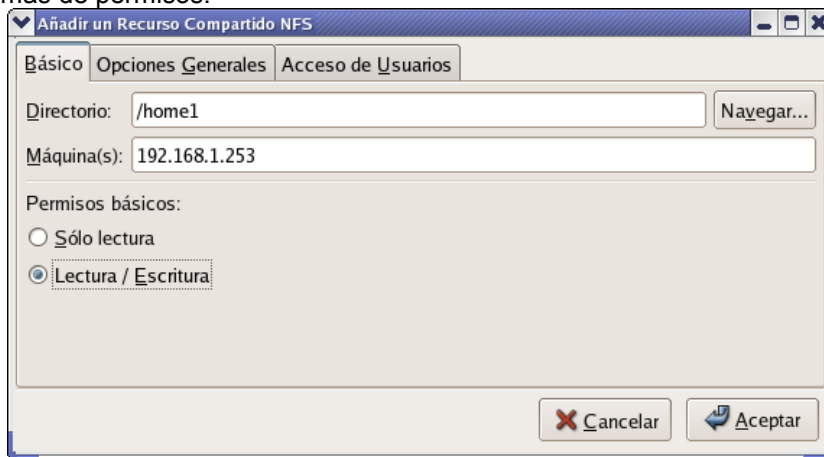
Si es por el escritorio KDE, para acceder a la configuración de NFS Server, por inicio, configuración del sistema, configuración de servidores, y NFS:

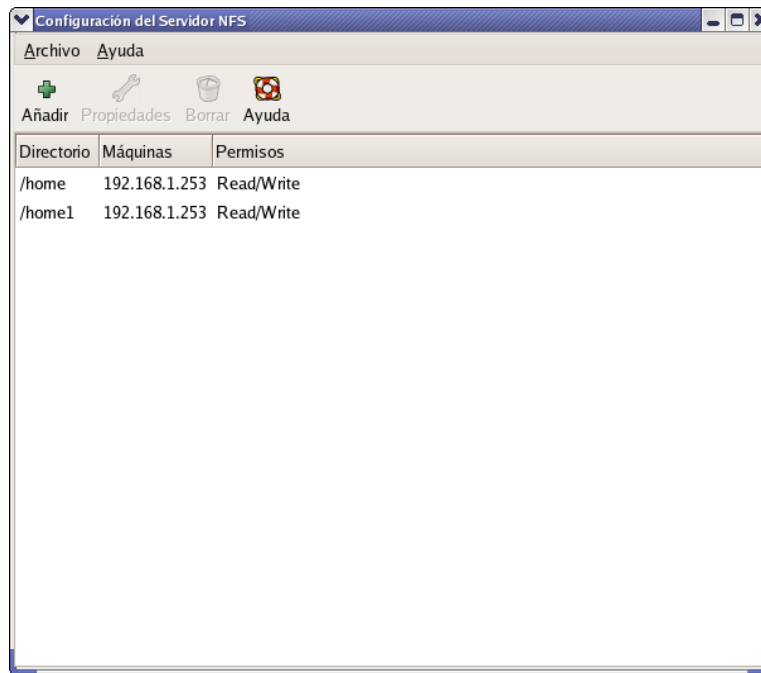


Allí se deben declarar las carpetas que se van a exportar, a que máquinas y algunos permisos (por ejemplo ya se exporto /home):



Vamos a exportar /home1, para que la pueda acceder la máquina 192.168.1.253, en modo lectura/escritura, y el usuario root de una máquina debe ser equivalente al root de la otra para evitar problemas de permisos.





Esto se ve reflejado en el archivo /etc/exports:

```
[root@dataserver RPMS]# cat /etc/exports
/home          192.168.1.253(rw,sync,nohide,no_root_squash)
/home1        192.168.1.253(rw,sync,no_root_squash)
[root@dataserver RPMS]#
```

Se puede verificar que los directorios exportados ya están disponibles , o si no están, que los exporte con el comando exportfs :

```
[root@dataserver RPMS]# exportfs -va
exporting dataserver1.cmb.com.co:/home1
exporting dataserver1.cmb.com.co:/home
[root@dataserver RPMS]#
```

Habilitando el servidor NFS

El servicio de NFS se habilita desde configuración del sistema, y servicios, para que siempre inicie con el sistema. O se puede iniciar manualmente con:

```
[root@www root]# service nfs start
Inicio de los servicios NFS:           [ OK ]
Starting NFS quotas:                  [ OK ]
Inicialización del demonio NFS:       [ OK ]
Inicialización de NFS mountd:         [ OK ]
[root@www root]#
```

3.6.2.CONFIGURANDO EL CLIENTE

En la máquina cliente, se deben montar los recursos que el servidor exporto y que el cliente desea. Esto se logra con el comando mount, previamente creando el directorio donde se montará el recurso o desde el interfaz gráfico webmin.

Por comandos el proceso sería:

Crear las carpetas donde se van a montar los recursos que exporto la máquina servidora y luego se montan los directorios sobre las carpetas creadas.

```
# mkdir /home1n
# mkdir /homen
# mount -t nfs 192.168.1.254:/home /homen
# mount -t nfs 192.168.1.254:/home1 /home1n
```

Si observamos las particiones del sistema vemos, que aparecen los dos montajes remotos que se realizaron. Los usuarios finales ven estas particiones como directorios locales:

```
root@dataserver home]# df -k
S.ficheros      1K-blocks   Used Available Use% Montado en
/dev/sda6       2016016    314048 1599556 17% /
/dev/sda1        15554     13388   1363 91% /boot
/dev/sda8       7091968   4447340 2284372 67% /home
none            192348      0    192348 0% /dev/shm
/dev/sda2       4538156   3914104 393520 91% /usr
/dev/sda5       3020140   203912 2662812 8% /var
/dev/sdb6       295564    107999 172305 39% /root1
/dev/sdb7       2008108   1423856 482244 75% /usr1
/dev/sdb8       6151076   4647316 1191300 80% /home1
192.168.1.254:/home 13887800 4983652 8187292 38% /homen
192.168.1.254:/home1 8054344 5864140 1774456 77% /home1n
```

Después de utilizados, se deben desmontar; para lo cual existen los comandos mount y umount respectivamente. Las opciones básicas de estos son:

- t Define el tipo a ser montado (Debe ser **nfs**).
- a Intenta montar todas las entradas listadas en el archivo /etc/fstab, o desmontar las encontradas en el archivo /etc/mntab.
- o Lee las opciones desde la línea de comando y no desde el archivo.

Si se desea que los recursos montados en el cliente, permanezcan cada vez que se inicie el sistema, se debe editar el archivo /etc/fstab para indicárselo.

```
# cat fstab
LABEL=/          /          ext3 defaults 1 1
none             /dev/pts   devpts gid=5,mode=620 0 0
none             /proc      proc defaults 0 0
none             /dev/shm   tmpfs defaults 0 0
/dev/hda3        swap       swap defaults 0 0
/dev/cdrom       /mnt/cdrom iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0         /mnt/floppy auto noauto,owner,kudzu 0 0
192.168.1.254:/home /homen    nfs noexec,dev,suid,rw 1 1
```

3.6.3. TALLER DE SERVICIO NFS

Configurar el servicio de NFS de los equipos de la sala, para exportar el directorio /var/log , pero solo pueden tener acceso a este , los equipos de la misma fila de su equipo. De igual forma comprobar que pueden acceder el directorio que su vecino exporto (var/log) y montarlo sobre el directorio /prestado, previamente creado.

3.7. SERVIDOR PROXY

Linux viene con un servicio de proxy llamado SQUID. Este servicio nos permitirá controlar quienes pueden acceder el servicio de internet , restringir algunos sitios a donde no pueden salir y prestar el servicio de caché en disco para no saturar el canal. Se trabajó directamente en el archivo de configuración del squid , llamado squid.conf ubicado en el directorio /etc/squid

Este archivo es demasiado extenso y no lo incluiremos en este informe, solo haremos referencia a las líneas de código involucradas para lograr nuestros objetivos. El archivo completo se anexa en el CD bajo archivos/etc/squid.

Segmento de Archivo /etc/squid/squid.conf

```

acl red src "/etc/squid/lista-ip-validas"
acl negados url_regex "/etc/squid/sitios-negados"
#acl red src 192.168.1.0/255.255.255.0
# TAG: http_access
#     Allowing or Denying access based on defined access lists
#
#     Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
#     NOTE on default values:
#
#     If there are no "access" lines present, the default is to deny
#     the request.
#
#     If none of the "access" lines cause a match, the default is the
#     opposite of the last line in the list.  If the last line was
#     deny, then the default is allow.  Conversely, if the last line
#     is allow, the default will be deny.  For these reasons, it is a
#     good idea to have an "deny all" or "allow all" entry at the end
#     of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
http_access deny negados
http_access allow localhost
http_access allow red
http_access deny all
#
    
```

En la parte inferior de este segmento de texto podemos observar que se aplican luego los permisos sobre los elementos creados llamados red y negados. A red se le conceden los permisos y a negados se le rechazan (cierran). Al resto se le niegan los accesos.

Se personalizo la página que muestra el mensaje de rechazar una conexión a un sitio negado y se explica como hacerlo para los otros mensajes por ejemplo de persona o IP no autorizada para navegar o de no encontrar una dirección IP correspondiente a un nombre.

Esto se logra editando el archivo relacionado con el error que se encuentra en la carpeta errors , bajo el directorio /etc/squid.

Hay un link que se debe cambiar para que los mensajes sean en español:

```

[root@fw ~]# cd /etc/squid
[root@fw squid]# ls -l
total 340
-rw-r----- 1 root squid  367 may 16  2005 cachemgr.conf
lrwxrwxrwx  1 root root   31 dic  1 18:38 errors -> /usr/share/squid/errors/English
lrwxrwxrwx  1 root root   22 dic  1 18:38 icons -> /usr/share/squid/icons
-rw-r--r--  1 root root 26104 may 16  2005 mib.txt
-rw-r--r--  1 root root 11651 may 16  2005 mime.conf
-rw-r--r--  1 root root 11651 may 16  2005 mime.conf.default
-rw-r--r--  1 root root  421 may 16  2005 msntauth.conf
-rw-r--r--  1 root root  421 may 16  2005 msntauth.conf.default
-rw-r----- 1 root squid 118415 dic  2 13:39 squid.conf
    
```

```
-rw-r--r-- 1 root root 118251 may 16 2005 squid.conf.default
[root@fw squid]#
[root@fw squid]# unlink errors
[root@fw squid]# ln -s /usr/share/squid/errors/Spanish errors
[root@fw squid]# ls -l
total 336
-rw-r----- 1 root squid 367 may 16 2005 cachemgr.conf
lrwxrwxrwx 1 root root 31 dic 2 14:19 errors -> /usr/share/squid/errors/Spanish
lrwxrwxrwx 1 root root 22 dic 1 18:38 icons -> /usr/share/squid/icons
-rw-r--r-- 1 root root 26104 may 16 2005 mib.txt
-rw-r--r-- 1 root root 11651 may 16 2005 mime.conf
-rw-r--r-- 1 root root 11651 may 16 2005 mime.conf.default
-rw-r--r-- 1 root root 421 may 16 2005 msntauth.conf
-rw-r--r-- 1 root root 421 may 16 2005 msntauth.conf.default
-rw-r----- 1 root squid 118415 dic 2 13:39 squid.conf
-rw-r--r-- 1 root root 118251 may 16 2005 squid.conf.default
[root@fw squid]#
```

Listado de directorio /etc/squid/errors

```
[root@www squid]# cd errors
[root@www errors]# ls
ERR_ACCESS_DENIED      ERR_FTP_NOT_FOUND      ERR_READ_ERROR
ERR_FTP_PUT_CREATED    ERR_READ_TIMEOUT
ERR_CACHE_ACCESS_DENIED ERR_FTP_PUT_ERROR      ERR_SHUTTING_DOWN
ERR_CACHE_MGR_ACCESS_DENIED ERR_FTP_PUT_MODIFIED
ERR_SOCKET_FAILURE
ERR_CANNOT_FORWARD     ERR_FTP_UNAVAILABLE   ERR_TOO_BIG
ERR_CONNECT_FAIL       ERR_INVALID_REQ        ERR_UNSUP_REQ
ERR_DNS_FAIL           ERR_INVALID_URL        ERR_URN_RESOLVE
ERR_FORWARDING_DENIED  ERR_LIFETIME_EXP       ERR_WRITE_ERROR
ERR_FTP_DISABLED       ERR_NO_RELAY            ERR_ZERO_SIZE_OBJECT
ERR_FTP_FAILURE        ERR_ONLY_IF_CACHED_MISS generic
ERR_FTP_FORBIDDEN      errors                  README
```

Por ejemplo para los sitios negados que están en la lista de sitios no permitidos el archivo es : ERR_ACCESS_DENIED. Se puede editar y personalizar el mensaje :

```
ERROR
LA ADMINISTRACION DE LA EMPRESA INFORMA QUE ESTOS SITIOS WEB TIENEN
ACCESO RESTRINGIDO

-----
DIRECCION DEL SITIO RESTRINGIDO: %U
MENSAJE DE ERROR
Access Denied.

Las politicas de acceso a internet tienen restringido este sitio Si es de acceso vital, por favor
contacte al Administrador de la red
Para contactar a su administrador, enviar a: %w.
```

De igual forma para el archivo que muestra que una dirección o URL esta mal.

Archivo : ERR_INVALID_URL

```
ERROR
EL SITIO WEB SOLICADO NO FUE ENCONTRADO

-----
DIRECCION DEL SITIO SOLICITADO: %U
```

Mensaje de Error:

Sitio web invalido (URL no encontrado)

El nombre del sitio no fue encontrado. Posibles problemas:

Incorrecto protocolo de acceso o no se escribió (Debe ser de la forma `http://` o similar)

No se escribió el nombre de la máquina o del dominio

Incluyeron espacios en blanco en la dirección escrita

Dirección del sitio web mal escrita o con caracteres invalidos

Su administrador de la red %w.

O Archivo ERR_DNS_FAIL:

El Sitio Web Solicitado no puede ser encontrado

DIRECCION SOLICITADA: %U

MENSAJE DE ERROR:

No se puede encontrar la direccion IP para el sitio solicitado %H

El Servidor DNS responde:

%z

Esto significa que :

El servidor Proxy (cache) no es capaz de traducir el nombre solicitado en la dirección IP .

Por favor chequee que la dirección esta bien escrita .

Su administrador de la red es: %w.

El archivo donde se controlan los sitios-negados es: /etc/squid/sitios-negados , y su contenido es:

```
[root@www squid]# cat sitios-negados
```

```
www.sitioporno.com
www.otrositioporno.com
www.playboy.com
www.chicas.com
napster
sex
porn
mp3
xxx
adult
astalavista
```

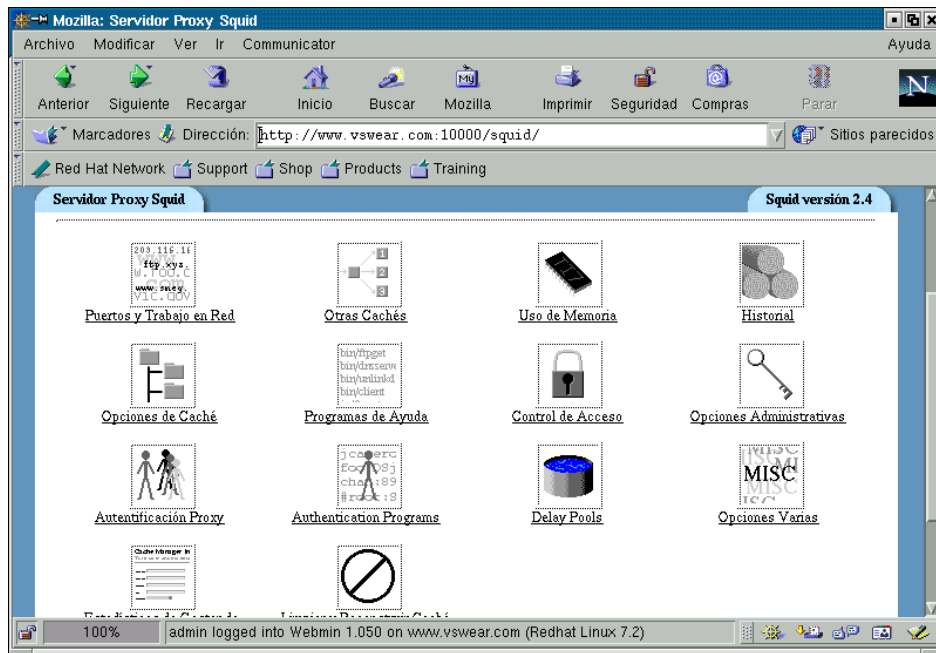
Este archivo se puede editar con cualquier editor , e incluirle los sitios o palabras que no desee puedan figurar en el URL o dirección digitada por el usuario desde el navegador.

En el archivo squid.conf se declaro un elemento llamado red que apunta a un archivo llamado "lista-ip-validas " con las direcciones IP de las máquinas que pueden navegar en internet para las personas autorizadas para usar este servicio . Allí se incluyeron las direcciones IP de algunas máquinas de la empresa.

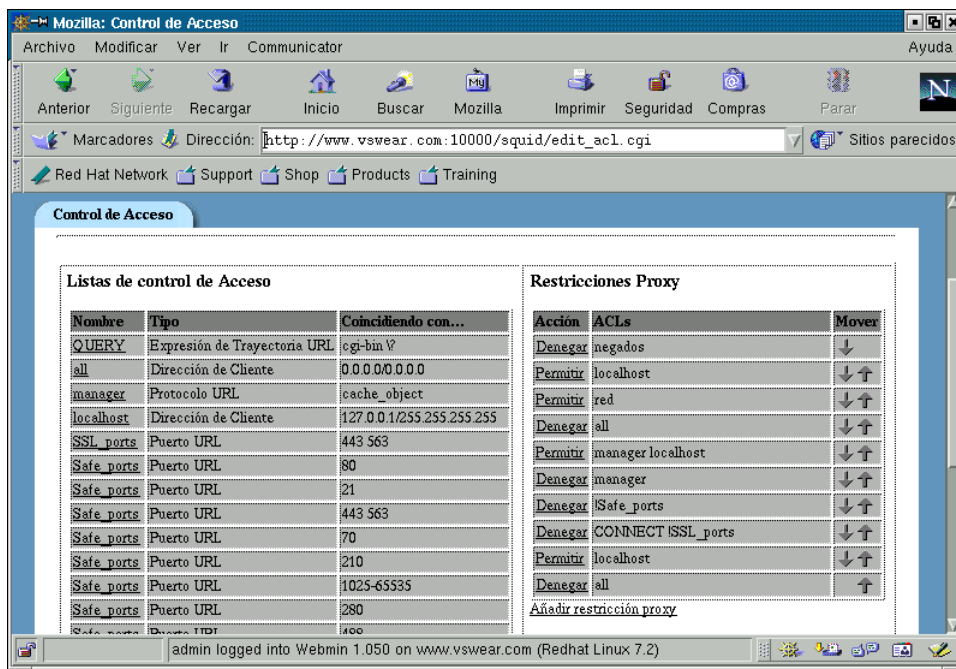
Este archivo se puede manipular con cualquier editor e incluir la dirección IP de cada máquina , una por línea o dar rangos, etc.

También se puede manipular desde el interfaz gráfica llamada webmin, que permite configurar y administrar la mayoría de los servicios linux (entrar por servidores y escoger squid)

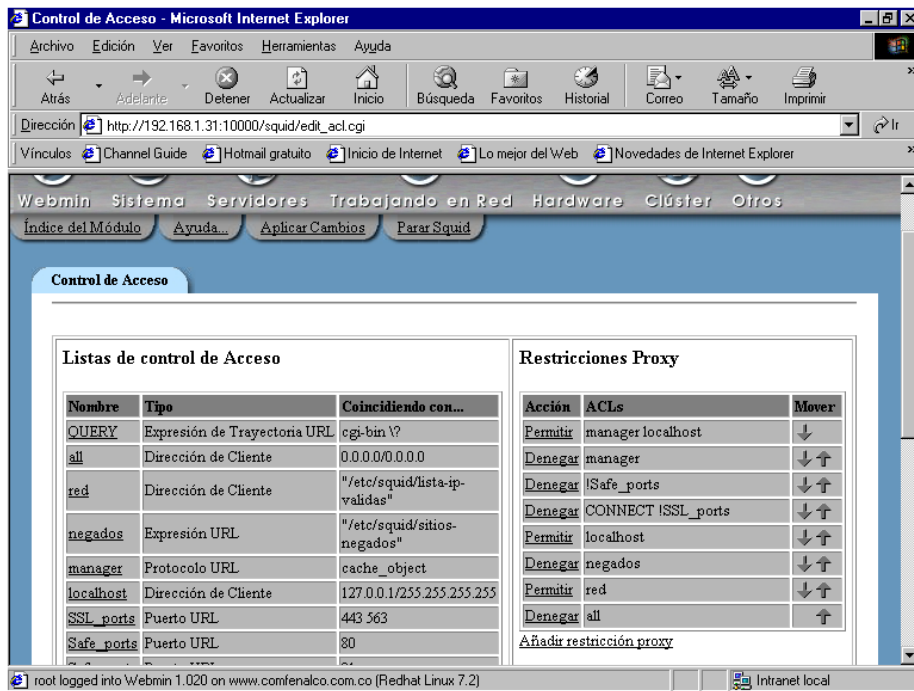
Debe aparecer una pantalla como :



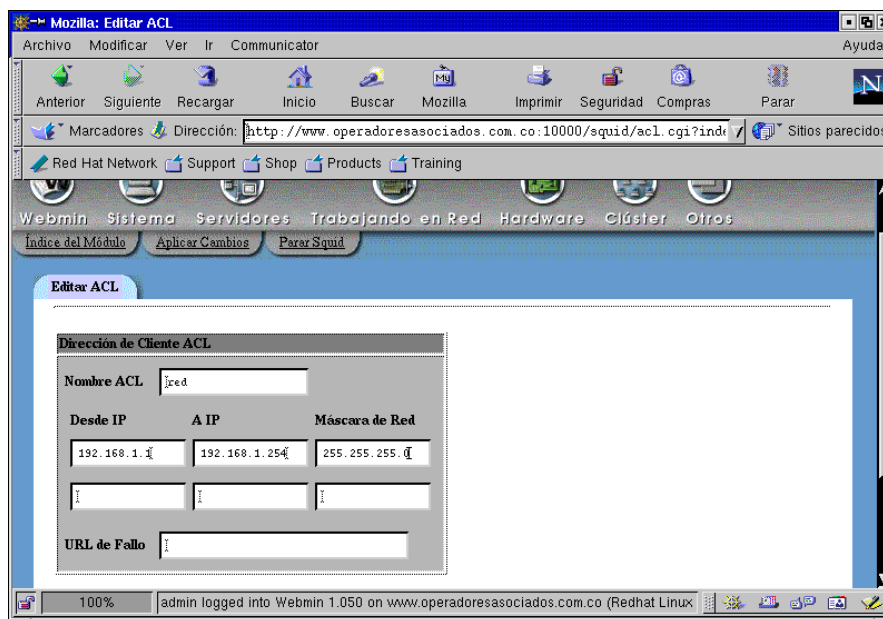
Si entramos por control de acceso podemos ver las lista de acceso mencionadas en el archivo squid.conf, tales como sitios-negados, lista para elemento llamado red, etc.



Escogemos el elemento red al lado izquierdo de la pantalla (en columna de listas de control de acceso)

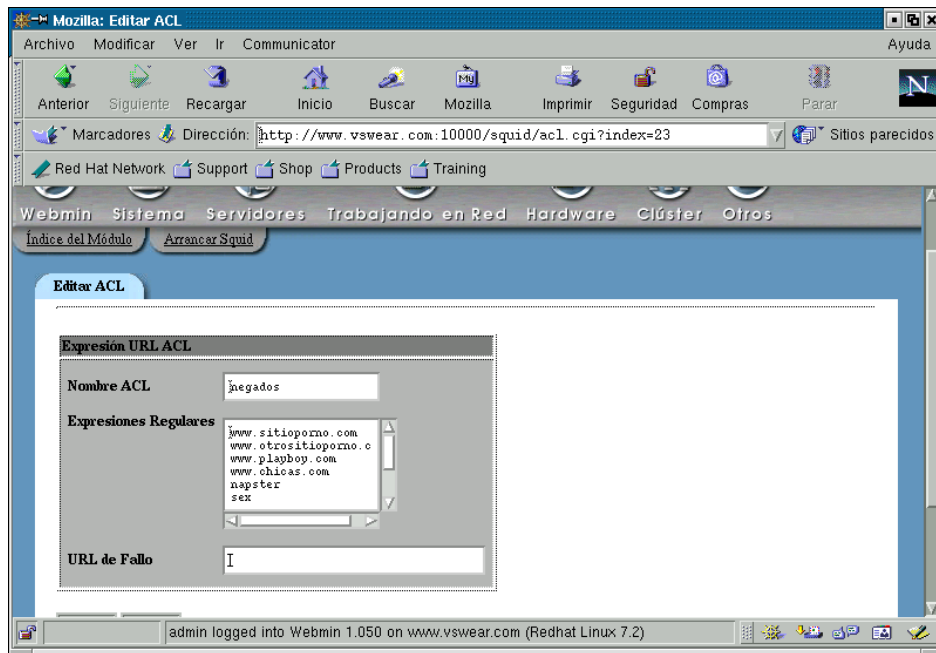


Y se abre la lista de equipos asociados.



Allí podemos eliminar o insertar nuevas direcciones IP , para suspender o permitir el uso de internet.

De igual forma se puede escoger la lista de sitios negados y modificarlos.



Luego se debe proceder a reiniciar el servicio de proxy (squid) desde una ventana de comandos linux:

```
# service squid stop
Parando squid: 2003/01/13 10:53:58
| aclParseIpData: WARNING: Netmask masks away part of the specified IP in '10.0.0.2-
10.0.0.250/255.0.0.0'
..... [ OK ]
# service squid start
Iniciando squid:
[ OK ]
```

La labor que se debe adelantar en los clientes del proxy (navegadores) es mínima. Se debe indicar la dirección o nombre del servidor proxy y el puerto por el cual escucha o atiende a los clientes.

3.7.2. MANTENIMIENTO DE LOS LOG DE EVENTOS

Si en el archivo squid.conf, se activaron los log de eventos, de accesos, etc, estos archivos pueden crecer y llenar las particiones. Por lo tanto se debe hacer un mantenimiento o limpieza de los archivos con cierta frecuencia.

Los archivos se encuentra en las carpetas:

/var/log/squid
/var/spool/squid

3.7.3. TALLER DE PROXY

Configurar el squid para filtrar algunos sitios en internet, por contenidos en el URL, por dirección IP de los equipos clientes, personalizando los mensajes de error presentados.

Ejemplo usar el URL de fallo para IP:

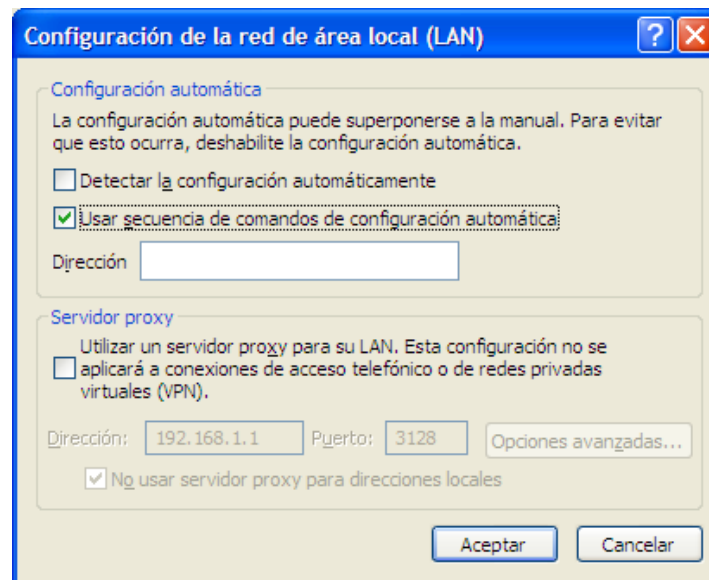
<http://192.168.57.168/squid/porip.html>

Y en el servidor web se debe tener esa página disponible con el mensaje deseado.

3.7.3.1. PARA COMPLEMENTAR

Se deben configurar el squid para hacer unos filtrados especiales, por horario, por tipo de archivo (ejm: .exe, .avi), y presentar estadísticas sobre el uso del squid.

En los navegadores, se puede configurar que se use una secuencia de comandos para determinar el proxy. En el campo de dirección se digita un URL de donde cargar la secuencia de comandos y generalmente es un archivo con extensión .pac.



Estos archivos nos permiten la toma de decisiones sobre que proxy usar, dependiendo del origen, el destino, etc, en empresas donde existan varios y también desarrollar otras tareas. Investigar sobre este tipo de archivos de comandos, y plantear algunos ejemplos.

3.7.4.PROXY TRANSPARENTE³

En condiciones normales , a todos los clientes se les debe especificar en el navegador quien es elservidor proxy (se debe dar la dirección IP o nombre de la máquina proxy y el puerto por el cual escucha las peticiones). Si una red tiene demasiados clientes este trabajo puede ser dispendioso.

Se puede hacer una configuración especial para implementar un proxy , sin que los usuarios deban enterarse de que en la red hay este servicio de proxy.

Se deseará simular que cada paquete que pase por su máquina Linux esté destinado a un programa en la propia máquina. Esto se utiliza para hacer proxies transparentes: un proxy es un programa que filtrando las comunicaciones entre la red y el mundo real , permite control de accesos a internet, caché, control de sitios visitados, etc. . La parte transparente se debe a que su red nunca tendrá por qué enterarse de que está comunicándose con un proxy, a menos, claro, que el proxy no funciones.

Se debe recurrir al uso de IPTABLES.

Que es IPTABLES ?

Iptables, se usa para configurar, mantener e inspeccionar las reglas de cortafuegos IP del núcleo Linux. Es un descendiente directo de ipchains (que vino de ipfwadm, que vino del ipfw IIRC de BSD), con extensibilidad. Los módulos del kernel pueden registrar una tabla nueva, e indicarle a un paquete

³ Iptables y el servicio de Traducción de Direcciones de Redes (NAT), Por Haller Javier Bracho Hernández, hbracho@linux.org.ve

que atravesase una tabla dada. Este método de selección de paquetes se utiliza para el filtrado de paquetes, para la **Traducción de Direcciones de Red (NAT)** y para la manipulación general de paquetes antes del enrutamiento. Una de las ventajas de iptables sobre ipchains es que es pequeño y rápido.

Anexo a este CD un documento PDF con una buena explicación del servicio de iptables y configuración de NAT y proxy transparente.

Para realizar esto se parte de que existe una máquina linux que filtra todo el tráfico saliente y entrante de la red y que los usuarios la tienen definida como su default gateway. Se debe incluir una regla con iptable de la siguiente forma:

```
# Envía el tráfico que llega a la máquina que filtra el tráfico ( o firewall) y que va dirigido al puerto 80 (web) a nuestro proxy squid instalado en el mismo servidor (transparente)
```

```
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Estas reglas se pueden digitar desde línea de comandos, pero al reiniciar la máquina se perderían. Es aconsejable ubicarlas en un archivo que se procese al inicio del sistema. Más adelante veremos que se puede ubicar , junto con las reglas de firewall del sistema.

3.8. SERVICIO DHCP

DHCP es Dynamic Host Configuration Protocol. Es usado para control de parametros de los clientes vitales en las redes. ES decir para que los clientes carguen de forma automática una serie de parámetros de su configuración de la red.

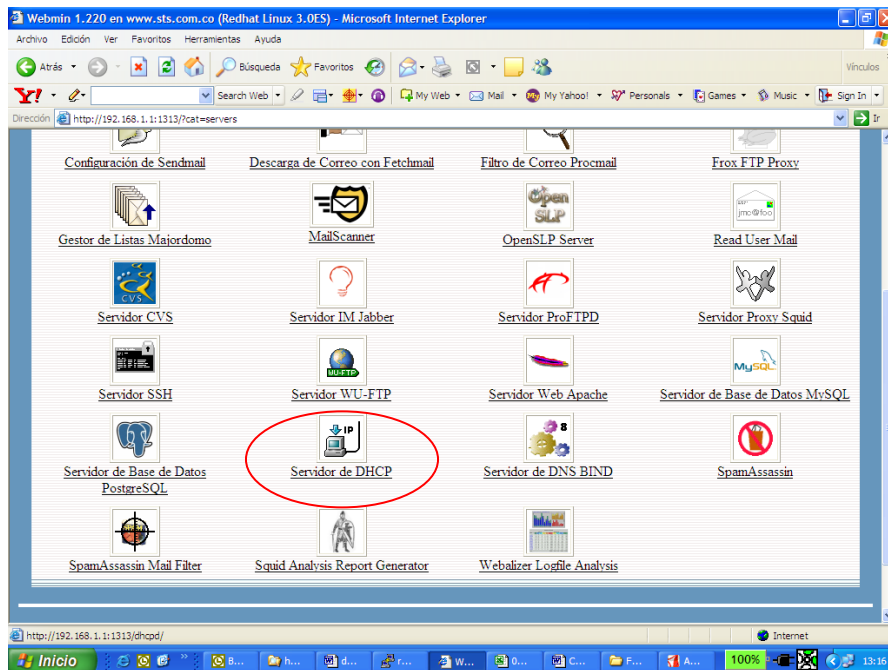
El DHCPD es un demonio que permite configurar las maquinas de una red dandoles:

- IP
- Mascara
- DNS
- Puerta de Enlace
- Nombre DNS

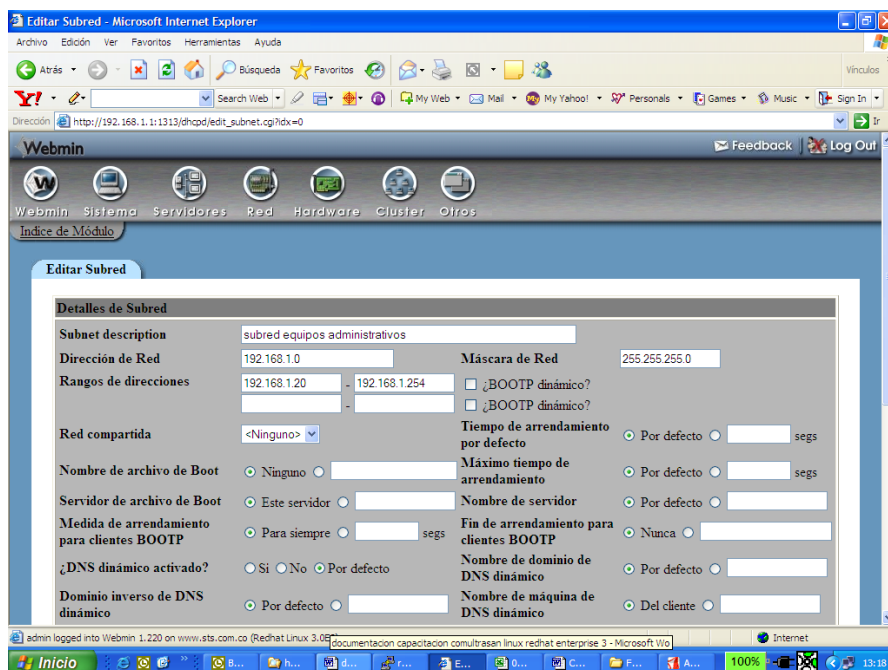
Para acceder la configuración del servidor, se puede hacer por el webmin.

3.8.1. CONFIGURACIÓN DEL SERVIDOR DHCP

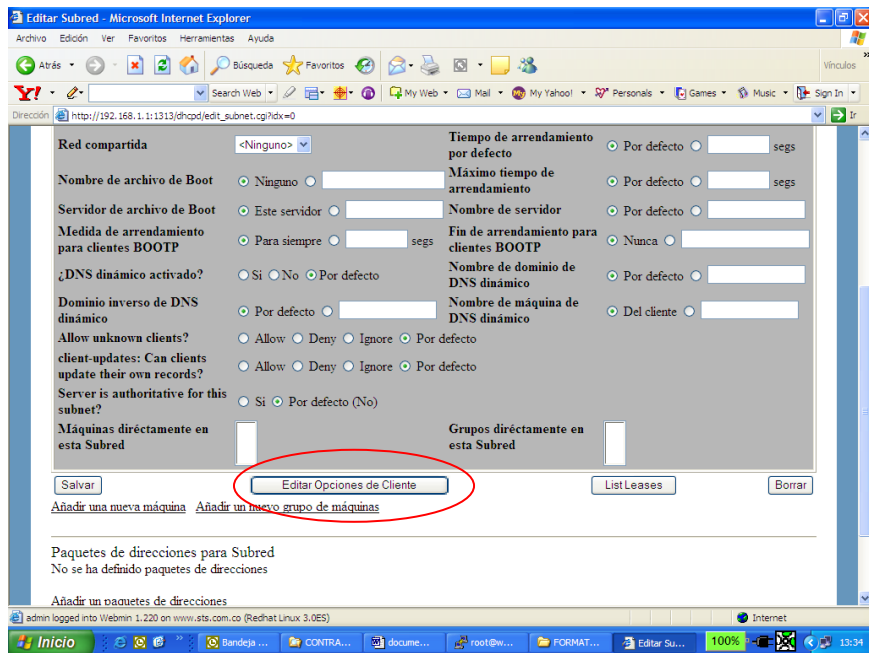
Para acceder la configuración del servidor,por webmin, simplemente entrando por servidores y DHCP:



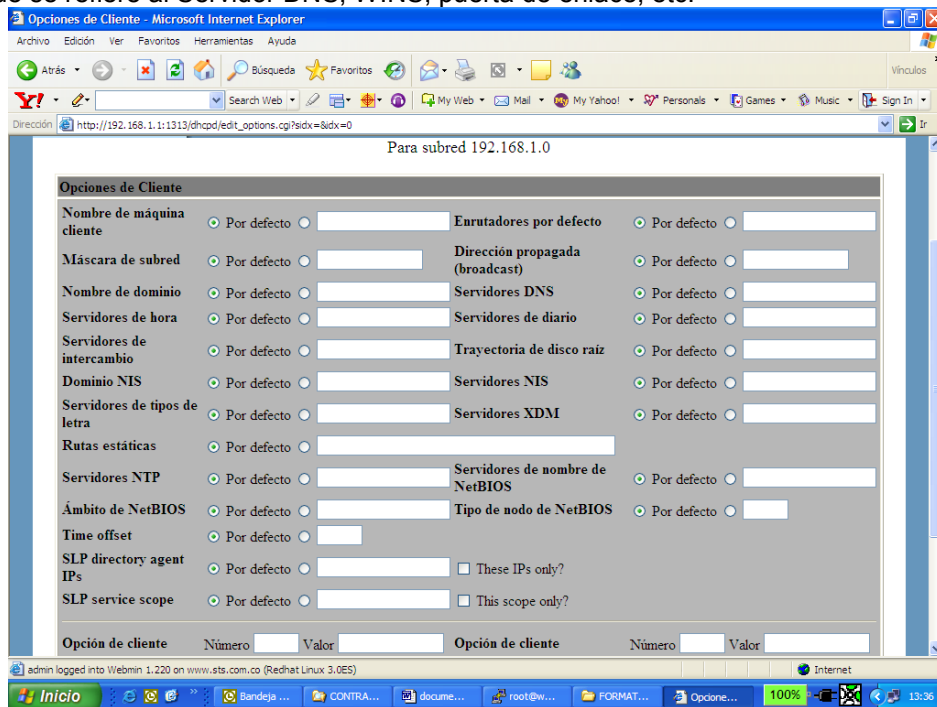
Se escoge luego añadir una subred y se procede con:



Dentro de la subred a manejar, se puede especificar el rango de direcciones que el servidor va a entregar a los equipos clientes y otras opciones. En la parte inferior, de esa pantalla de diálogo, se pueden especificar los valores que debe cargar el cliente:

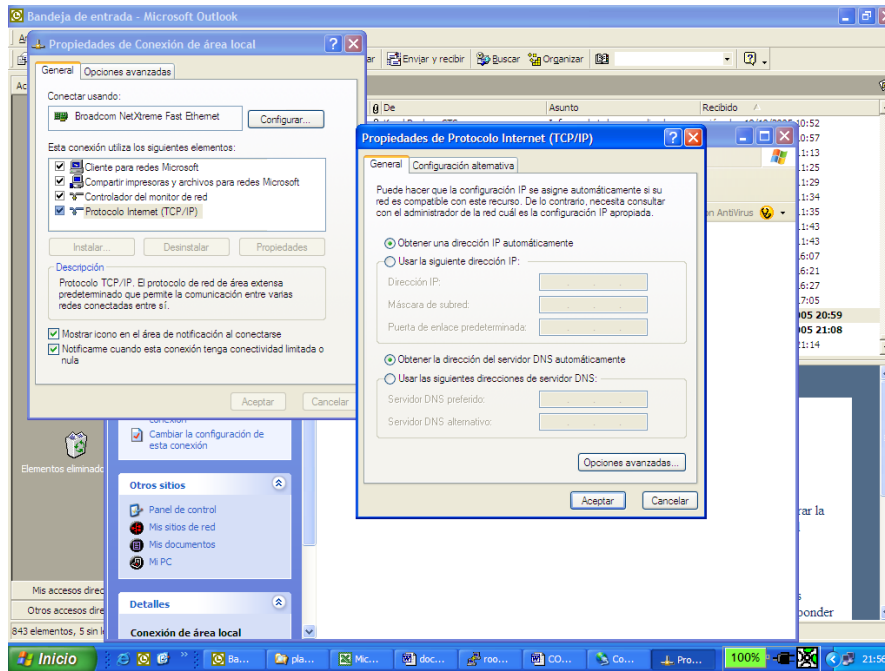


En lo que se refiere al Servidor DNS, WINS, puerta de enlace, etc.



3.8.2. CONFIGURANDO EL CLIENTE

Si es una máquina windows, en los parámetros de dirección IP, se deja : obtener una dirección:



La asignación de ips puede ser dinamica, donde los clientes toman una IP de un rango especificado y esta cambia en el cliente cada vez que se arranque.

NOTA: Si al arrancar el servicio dhcp, muestra error, por global ddns-update-style; (ver el messages).

Se debe incluir una instrucción ddns, como muestra:

El archivo de configuracion debe quedar, por ejemplo:

```
[root@hector log]# cat /etc/dhcpd.conf
ddns-update-style none;
option domain-name-servers 192.168.45.43;
# sala especializacion
subnet 192.168.45.0 netmask 255.255.255.0 {
    range 192.168.45.200 192.168.45.215;
}
```

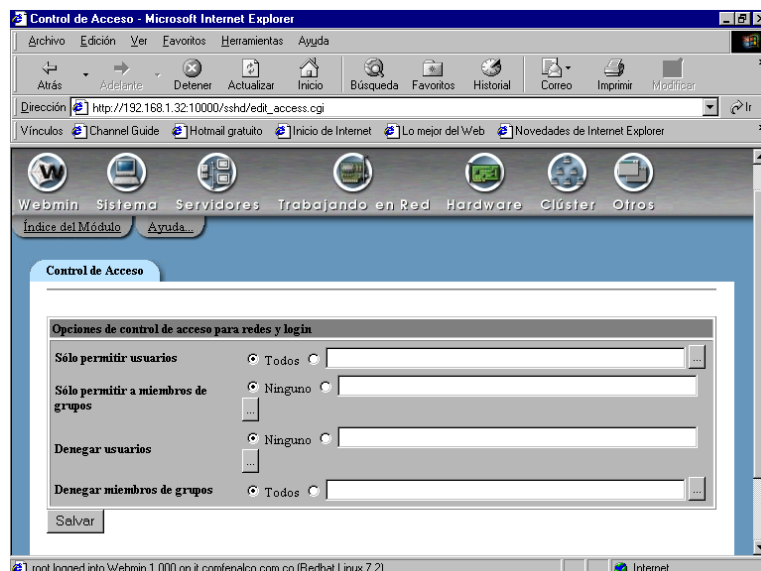
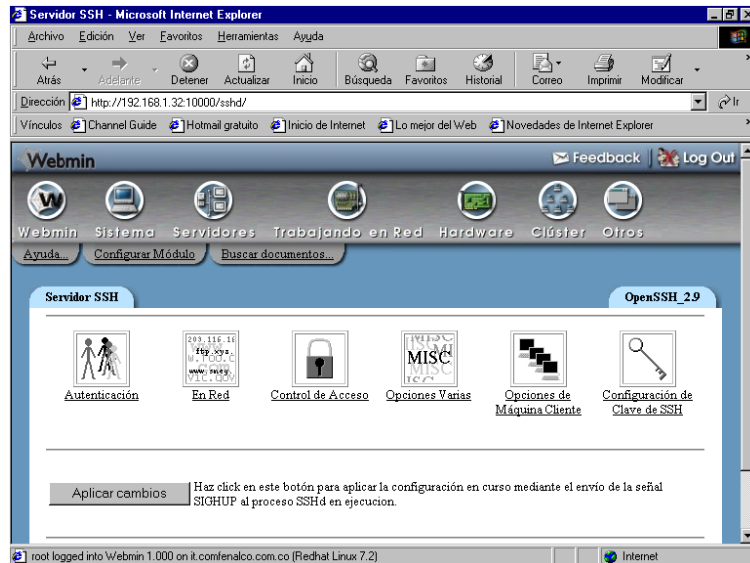
3.8.3. TALLER DE DHCP

Se debe definir un servidor DHCP por cada fila , donde se especifique los rangos de IP a repartir, la dirección del gateway y DNS a utilizar. Se activa el servicio y se modifican los clientes (equipos restantes de la fila) para que lo usen. Bootear los clientes y ver que parámetros tomaron.

3.9. SERVICIO SSH (SHELL SEGURO)

Para evitar que las comunicaciones con este servidor sean vistas en la red , por productos como sniffer, se deben manejar comunicaciones seguras (encriptadas) tanto en el cliente , como en el servidor.

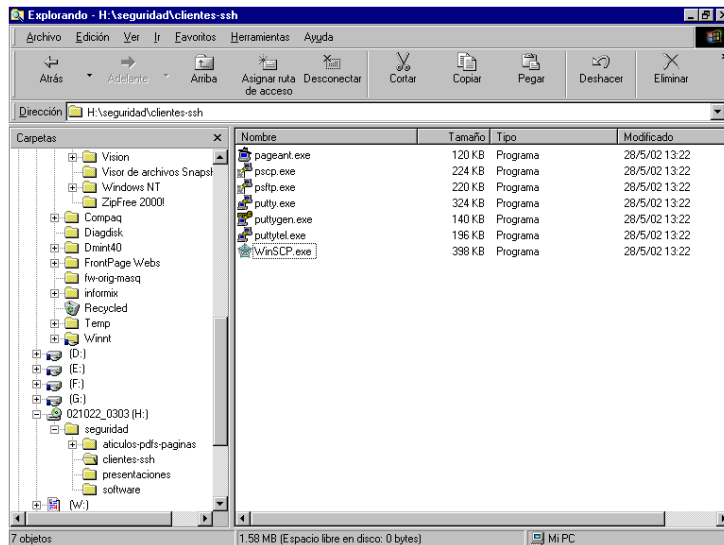
Para activar el servicio SSH , se debe garantizar que el servicio arranque con el sistema y luego se puede invocar desde el webmin para hacer configuraciones especiales. Por ejemplo especificar que usuarios o desde que máquinas se pueden conectar usando este servicio.



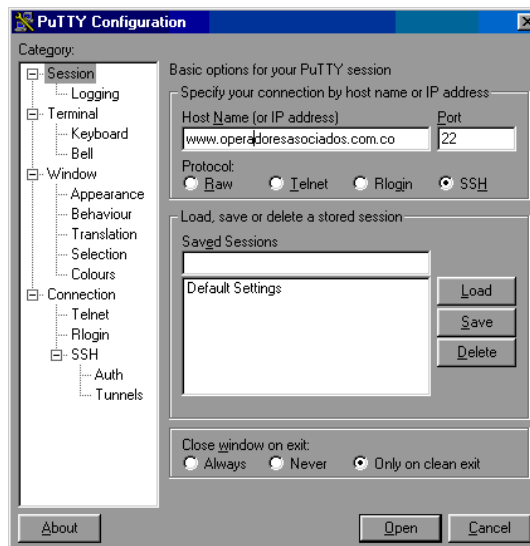
Es recomendable que no se use comandos como telnet, ftp, correo, rlogin, rcp, etc, ya que viajan de forma transparente por la red. En su lugar, por ejemplo para el telnet, ftp, rlogin, rcp, se debe usar el SSH. Si requiere conectarse por la red interna con el servidor desde un cliente (windows), es recomendable que use este servicio, ya que el telnet normal esta deshabilitado por seguridad.

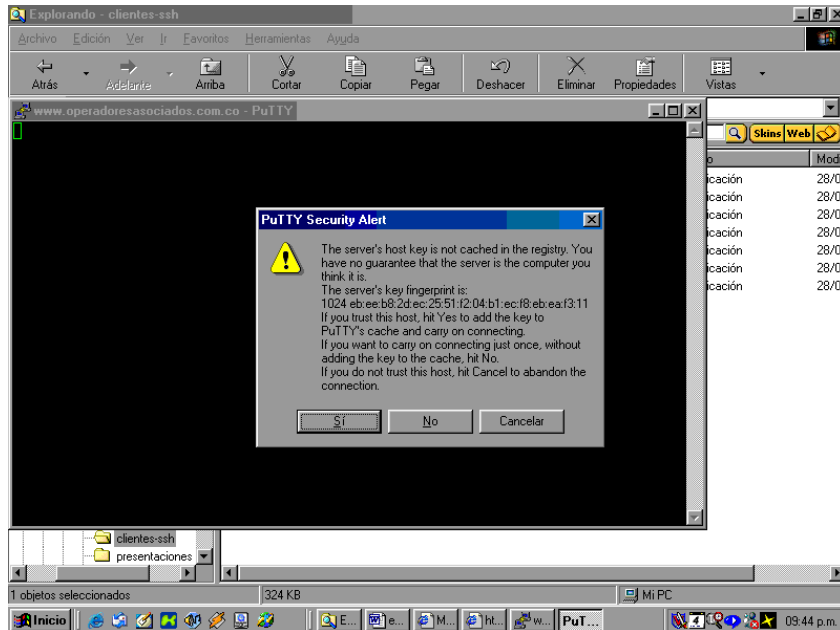
Una vez que este servicio este funcionando, las conexiones desde los clientes se deben hacer con los respectivos productos encriptados.

Se anexa una carpeta en el CD de documentación con una serie de productos libres para trabajar como productos clientes SSH en windows y conectarse al servidor de forma confiable.

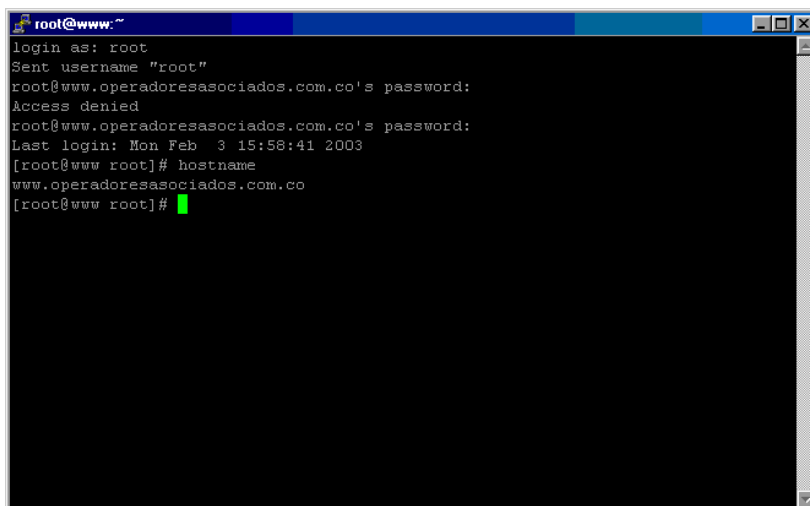


Por ejemplo, si se desea hacer una conexión o emulación de una terminal remota desde un equipo externo a la red (o inclusive interno) se puede usar el comando putty, de la siguiente forma:

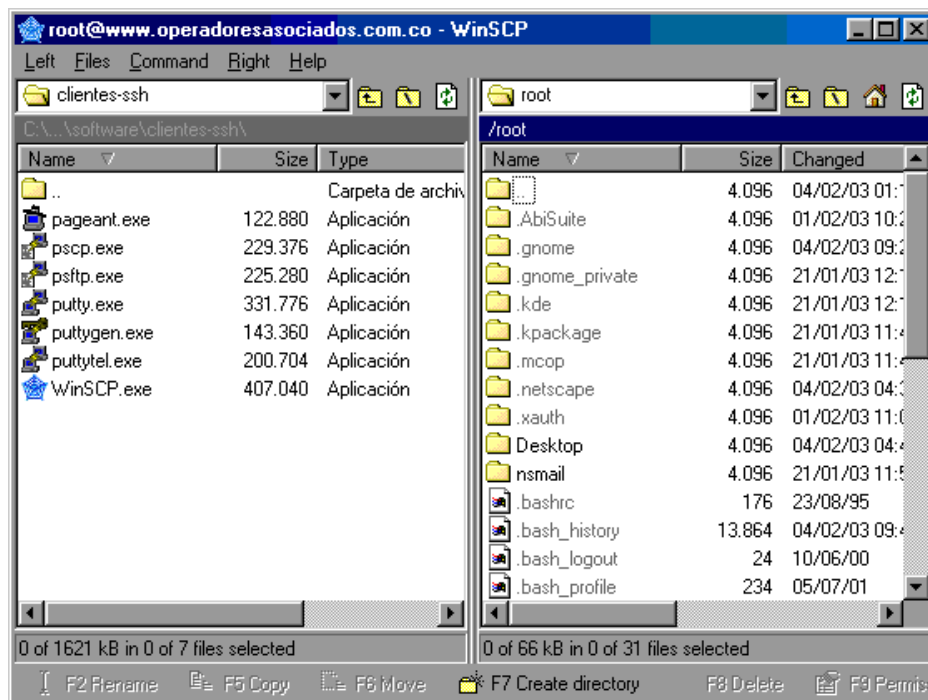
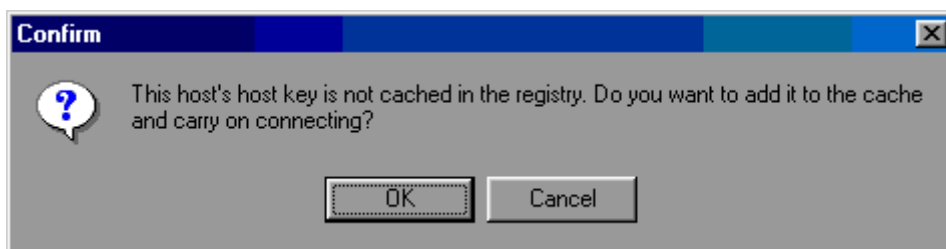




Se presenta una ventana o terminal, desde la cual podemos ingresar con un usuario y password como si fuese local.



De forma semejante, si deseamos hacer una transferencia de archivos (antes ftp), podemos utilizar la herramienta WinSC que realiza la mismas funciones con un interfaz gráfico bastante amigable, que me permite enviar o recibir archivos de una forma encriptada.



La ventana de la izquierda es la máquina local (PC desde donde nos conectamos) y la ventana de la derecha es el servidor.

3.9.1. TALLER SSH

Activar el servicio de SSH en los servidores Linux y entrar desde algunos clientes linux y windows para realizar sesiones remotas y transferencias de archivos de forma encriptada. Como comprueban esto? , demostrarlo.

3.10. SERVICIO FTP

FTP (File Transfer Protocol)

File Transfer protocol. Permite a los usuarios acceder y transmitir archivos en servidores localizados sobre internet. Estos servidores se pueden acceder a través de un browser (ejm: <ftp://ftp.microsoft.com>) o por línea de comandos (ejm: ftp <ftp.microsoft.com>) . En el primer caso toda la interacción se hace con el mouse y de esta forma se puede hacer el download de archivos. En el segundo caso es necesario conocer la sintaxis de los comandos FTP.

Cuando un usuario entra a un servidor FTP con una cuenta normal, puede desplazarse por todo el árbol de unix donde tenga permisos de lectura (la mayoría) y pone en riesgo la confidencialidad de la información del sistema. Es aconsejable no habilitar este servicio cuando la máquina esta conectada a internet y en caso de ser vital, mejor e configura el servicio ftp anonymous.

3.10.1.CONFIGURACIÓN DE FTP SERVER (ACCESO ANONYMOUS)

Se debe verificare que existe un servicio FTP activo. Esta versión incluye el servicio vsftpd, para la parte servidor y gftp para la parte grafica del cliente.

Este sistema viene con un servidor ftp llamado vsftpd, que puede iniciarse siempre al inicio (por configuración del sistema, servidores, servicios), o manualmente con:

```
[root@www root]# service vsftpd start
Iniciando vsftpd para vsftpd:          [ OK ]
[root@www root]#
```

La configuración de este servicio se realiza desde el archivo de configuración ubicado en /etc/vsftpd y que se llama vsftpd.conf:

```
[root@www root]# cd /etc/vsftpd
[root@www vsftpd]# ls -l
total 8
-rw----- 1 root  root   4138 sep 22 13:45 vsftpd.conf
[root@www vsftpd]#
```

El usuario Anónimo (Anonymous) : es el más usual en internet, donde un usuario con ese nombre llega a un servidor y puede entrar con cualquier password, pero cae en un directorio público, de donde generalmente sólo puede leer los archivos que están permitidos.

Para solo permitir este tipo de usuario y no ls usuarios reales del sistema se manipulan las siguientes líneas del archivo de configuración:

```
anonymous_enable=YES
#local_enable=Yes
```

Manipulando otras líneas, se puede permitir o no que los usuarios escriban sobre el servidor, cambiar el mensaje de bienvenida, etc.

Generalmente, los servidores FTP que pemiten entrada al usuario anonymous, lo controlan a satisfacción. Se le indica que directorios puede ver, simulando la raíz de unix, que comandos puede ejecutar, cuantos usuarios pueden estar en el sistema, para que no afecten el rendimiento de mi máquina, etc. Los usuarios llegan a /var/ftp y allí se les simula la raíz del sistema, creando otras carpetas si se desea.

```
[root@www vsftpd]# cd /var/ftp
[root@www ftp]# ls
pub
[root@www ftp]#
```

Se le puede indicar al sistema que registre los accesos (entradas y salidas de transferencias de archivos) ,con la línea:

```
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
```

y se puede pedir que sean redirigidas al syslog de la máquina.
Si se desea cambiar la carpeta que el toma como raíz (por defecto /var/ftp):

```
anon_root=/publico
```

Donde /publico es la nueva carpeta.

En el servidor existe un archivo donde se puede indicar, a que usuarios no se les permite el acceso a la máquina por FTP. Este archivo se llama /etc/vsftpd.ftpusers. Por defecto el usuario root esta incluido allí, pues por seguridad no se le permite entrar con FTP por la red , ya que este servicio no esta encriptado y fácilmente podrían obtener su clave de acceso.

3.10.1. TALLER FTP

Habilitar el servicio FTP en las máquinas linux. Entrar con un usuario normal y ver que pueden hacer. Tratar de recorrer el árbol de directorios linux y llevarse archivos del sistema. Hacerlo desde línea de comandos, y desde interfaz gráfico.

Configurar el usuario anonymous , definiendo en /opt/ftp la raíz ficticia. Crear si no la tiene una estructura similar a unix allí. En una carpeta llamada publico colocar los archivos que se desean publicar. No dar permisos de que escriban allí , ni borren. La clave del usuario anonymous puede ser cualquier cosa.

Configurar el servidor para que solo permita el acceso a ftp con la cuenta anonymous. No permitir ningún usuario diferente así este creado en la máquina.

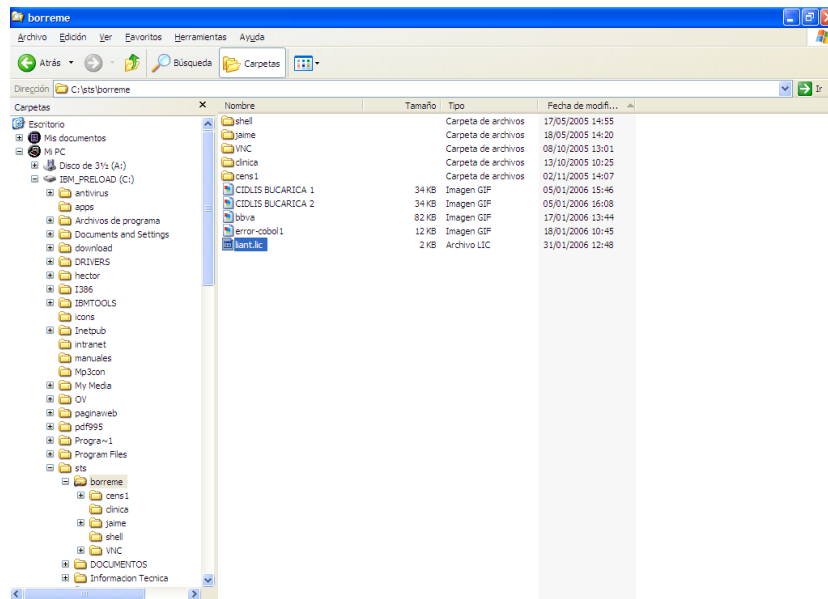
3.11. MANEJO DE SISTEMAS DE ARCHIVOS ENTRE LINUX Y WINDOWS

Si tenemos nuestra máquina Linux en ambiente dual, es decir podemos bootear linux o windows, según sea el caso, podemos tener desde ambiente Linux, acceso a la partición windows y a sus carpetas. Pero aquí nos centraremos en el acceso desde windows a carpetas Linux que residen en otra máquina o viceversa.

3.11.1. MONTAJE DE CARPETAS WINDOWS EN LINUX

Desde el sistema Linux, por medio de samba podemos acceder a los discos windows de una máquina que este en la red.

En la máquina Windows se debe compartir la carpeta que se desea prestar. En este caso la carpeta borreme.



Desde la máquina linux se montó esa carpeta del PC compartida (con la dirección IP 192.168.1.240) , con el comando de samba smbmount, pero se debe crear previamente la carpeta donde se va a montar, por ejemplo llamada windows.

```
# mkdir /windows
# smbmount //192.168.1.240/borreme /windows
Password:
[root@demos ~]# df -k
S.ficheros      Bloques de 1K  Usado   Dispon  Uso%  Montado en
/dev/hda2       1486108      366252 1043148 26% /
/dev/shm        225340        0      225340 0% /dev/shm
/dev/hda9       5952252     1608924 4036088 29% /home
/dev/hda5       2972236     196516 2622304 7% /opt
/dev/hda7       1984016     35868 1845736 2% /tmp
/dev/hda3       9920624     6964204 2444352 75% /usr
/dev/hda6       2972236     312804 2506016 12% /var
//192.168.1.240/borreme
28894208 26502144 2392064 92% /windows
```

Se observa que la carpeta montada ya se ve como una partición de la máquina y los usuarios la pueden desde /windows.

3.11.2. USO DE SAMBA (SERVIDOR DE ARCHIVOS E IMPRESORAS)

Nos permite colocar a disposición de la red windows , un sistema de archivos para almacenar información, con la seguridad de los entornos conocidos por ustedes. También podemos compartir otros recursos como impresoras.

Ahora si entraremos en la configuración del SAMBA para permitir que desde el entorno de red de windows se acceden carpetas de usuarios de la máquina Linux que tiene mayor capacidad de almacenamiento.

Recordemos que ya tenemos una serie de usuarios linux , que son los mismos usuarios de correo.

Podemos proceder a manipular el archivo de configuración o por los intefaz gráficos de webmin.

Aquí se modificó directamente el archivo /etc/samba/smb.conf (incluido en el CD).

Se colocaran algunas explicaciones en rojo, pero no hacen parte del archivo:

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
#===== Global Settings
#=====
[global]
    workgroup = coa NOMBRE DEL GRUPO DE TRABAJO
    netbios name = linux NOMBRE QUE DESEO DAR A MI SERVIDOR LINUX
    smb passwd file = /etc/samba/smbpasswd ruta del archivo de claves
    remote announce = 192.168.1.255
    printing = lprng
    dns proxy = no
    encrypt passwords = yes
    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
    printcap name = /etc/printcap
    max log size = 0
    hosts allow = 192.168.1. 127. REDES ADMITIDAS
    interfaces = 192.168.1.1/24 INTERFAZ PERMITIDA PARA ESTO
    writeable = yes
    security = user
    server string = Servidor Archivos
    log file = /var/log/samba/%m.log
    load printers = yes
    public = yes
    password level = 0
    min passwd length = 3
    unix password sync = yes
    passwd program = /usr/bin/passwd %u
    passwd chat = *password* %n\n *password* %n\n *successfull*
    passwd chat debug = yes

[comun] SE EMPIEZA DESCRIPCIÓN DE CADA CARPETA COMPARTIDA
    path = /home/comun
    comment = Directorio compartido todos los user
    writeable = yes
    create mode = 0744
    directory mode = 0775
    guest ok = yes SE PERMITE USUARIO INVITADO
    guest account = coa SE DECLARA A COA COMO USUARIO INVITADO
    revalidate = yes

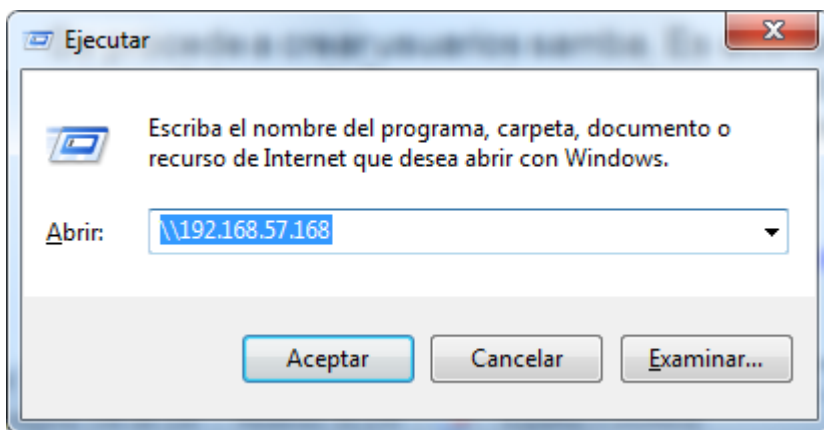
[hector] DESCRIPCIÓN DE UNA CARPETA NORMAL DE USUARIO
    path = /home/hector
    comment = Home hector
    valid users = hector SOLO ADMITE ESTE USER
    create mode = 0644
    writeable = yes
    directory mode = 0755
    revalidate = yes
```

```
[diana]
  path = /home/diana
  valid users = diana
  comment = Home diana
  create mode = 0744
  writeable = yes
  directory mode = 0775
  revalidate = yes
.....
.....
.....
semejante para el resto de usuarios
```

Luego se puede reiniciar el servicio samba :

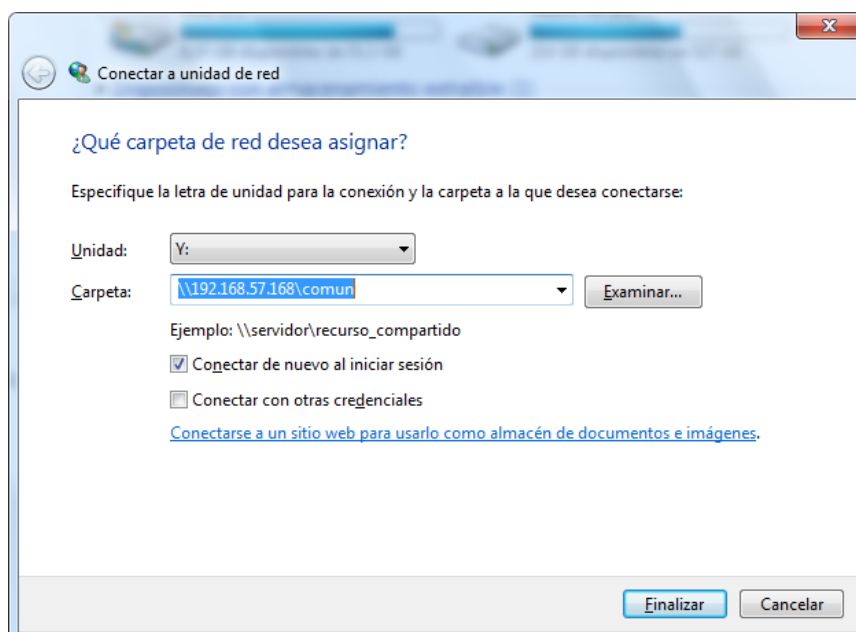
```
service smb restart
```

desde Windows se puede hacer uso de la carpeta que se comparte , accediendo el recurso:

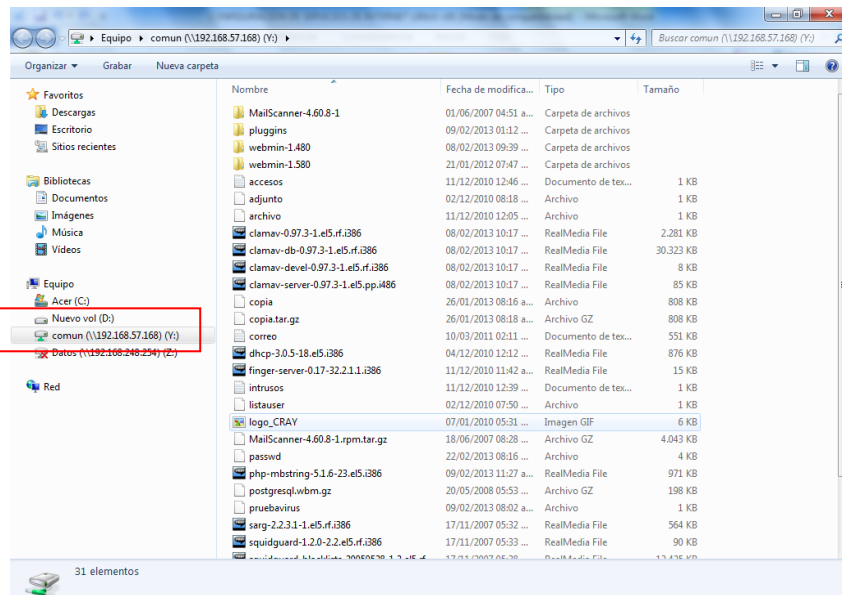


Y allí se deben observar la lista de carpetas compartidas.

Si se desea que esta carpeta siempre sea una unidad de red en el PC:



Y ahora siempre que detecte la red , se conecta automáticamente y la ve como unidad y:



Se procede a crear usuarios samba. Es aconsejable que el nombre del usuario samba sea el mismo del usuario linux, así como el password (así se evita que se le pregunte al picar sobre la carpeta compartida , una vez se ha logeado en XP con el usuario samba creado (es el mismo usuario creado en los perfiles de XP).

Se usa el comando linux `smbadduser nombreuserlinux:nombreuserwindows`

```
# smbadduser hector:hector
```

```
-----
ENTER password for hector
New SMB password:
Retype new SMB password:
```

```
# smbadduser diana:diana
```

```
-----
ENTER password for diana
New SMB password:
```

Si se desea cambiar el password de un usuario samba , se puede recurrir al comando linux : `smbpasswd`

Ya se puede proceder a acceder estas carpetas compartidas desde el entorno de red de windows XP, entrando primero con el perfil de XP y el nombre del usuario samba creado.

Los archivos involucrados , residen en la carpeta `/etc/samba/`

3.11.3. TALLER CONECTIVIDAD CON WINDOWS

Como las máquinas linux trabajan en ambiente dual, se solicita.

- Estando en ambiente Linux, copiar un archivo de la carpeta Mis Documentos de windows a `/opt`.
- Estando en ambiente Linux, copiar un archivo de una carpeta compartida en windows de la máquina vecina a `/opt` de linux.

- Configurar un Servidor Linux de cada fila, para que comparta una carpeta llamada /Linux (previamente creada), con las máquinas windows, de su misma fila.

3.11.3.1.PARA COMPLEMENTAR

Ya se han tratado algunos comandos para que Linux trabaje como servidor, pero se puede presentar el caso de que se desee trabajar como cliente. Por ejemplo deseamos que desde linux se pueda imprimir en las impresoras de los equipos Windows. Como se hace esto, revisar los comandos smbclient.

4. PROTECCIÓN DE LOS SERVICIOS DE INTERNET Y EL SERVIDOR

4.1. USO DE TCPWRAPPER (TCP/IP CONFIABLE)

TCP Wrappers permite controlar y proteger los servicios de red, limitando el acceso como sea posible, y registrado todos las conexiones para hacer el trabajo de detectar y resolver problemas de forma más fácil.

TCP Wrappers es una herramienta simple que sirve para monitorear y controlar el tráfico que llega por la red. Esta herramienta ha sido utilizada exitosamente en la protección de sistemas y la detección de actividades ilícitas. Fue desarrollada por **Wietze Zweitze Venema** y esta basada en el concepto de Wrapper; es una herramienta de seguridad libre y muy útil.

Un Wrapper es un programa para controlar el acceso a un segundo programa. El Wrapper literalmente cubre la identidad del segundo programa, obteniendo con esto un más alto nivel de seguridad.

Los Wrappers son usados dentro de la Seguridad en Sistemas UNIX.

Debo configurar 2 archivos, donde especifico quien accederá a los servicios de mi servidor tcpwrapper, estos archivos son: /etc/hosts.allow y /etc/hosts.deny.

La sintaxis de estos archivos es muy simple:

servicio: host: acción

servicio: es el nombre del servicio , que generalmente esta dentro de los archivos respectivos del directorio xinet.d, por ejemplo son servicios el in.telnetd,in.fingerd. Si queremos referirnos a todos los puertos bastará con poner *ALL*, también podemos poner una lista de servicios separados por espacios en blanco.

host: es una o mas direcciones de red separadas por espacios en blanco, esta direccion se contrasta con la del sistema que nos hace la petición de conexión. La dirección puede ser del tipo IP numerica, IP/mask, rango de IP (por ejemplo 195.116.), dominio (como por ejemplo sts.com), grupo de dominios (como por ejemplo .com).

acción: puede tener 4 valores, *accept* (acepta la conexion si se cumplen las condiciones impuestas por servivio/host), *deny* (rechaza la conexion, *spawn* (acepta la conexion y realiza el comando bash que se le pasa como parametro) y *twist* (rechaza la conexion y realiza el comando bash).

A los comandos se les pueden pasar parámetros relacionados con la conexión, estos son:

%a, *%c*, *%h* y *%n*: nombre de la maquina que intenta acceder
%d: demonio que controla el puerto por el que accede
%p: PID del proceso que controla la conexión

Ejemplo :

- Archivo /etc/hosts.allow

Se le dieron todos los servicios a las máquinas que aparecen en esta pantalla

```

Telnet - 192.1.1.240
Conectar Edición Terminal Ayuda
# hosts.allow This file describes the names of the hosts which are
# allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
ALL : 192.1.1.221
ALL : 192.1.1.222
ALL : 192.1.1.230
~

```

- deny
Para impedir el acceso a otras redes debo agregar:
Se le denego todos los servicios a todas las máquinas cliente a menos de que estén especificadas en el archivo hosts.allow

```

Telnet - 192.1.1.240
Conectar Edición Terminal Ayuda
# hosts.deny This file describes the names of the hosts which are
# *not* allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow. In particular
# you should know that NFS uses portmap!
ALL : ALL
~

```

Ejemplo 2:

/etc/hosts.deny

Niega todos los servicios a todas las máquinas excepto a una en
específico: 192.1.1.221
ALL:ALL EXCEPT 192.1.1.221

```

Telnet - 192.1.1.240
Conectar Edición Terminal Ayuda
#
# hosts.deny This file describes the names of the hosts which are
#
# *not* allowed to use the local INET services, as decided
#
# by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
#
# the new secure portmap uses hosts.deny and hosts.allow. In particular
#
# you should know that NFS uses portmap!
ALL : ALL EXCEPT 192.1.1.221
~
~
~

```

Ejemplo 3:

/etc/hosts.deny

*# Solamente se permite el servicio de ftp para todo mundo excepto
para la máquina 192.1.1.222
ALL EXCEPT in.ftpd:ALL EXCEPT 192.1.1.222*

Ejemplo 4:

Cerrado para todos excepto para las conexiones locales (que se emitan desde la misma máquina:

```

#/etc/hosts.allow
ALL:127.0.0.1
ALL: ALL: deny

```

Ejemplo 5.

Conexion local total, red local acceso por telnet y ftp, resto cerrado:

```

#/etc/hosts.allow
ALL:127.0.0.1

in.telnetd in.ftpd: LOCAL

ALL: ALL: deny

```

Ejemplo 6.

Sistema abierto para algunas máquinas con informe de accesos:

```
#/etc/hosts.allow

in.telnetd:192.168.57.69:spawn( /bin/echo -e "Permitido %a en puerto %d" >> /opt/accesos.txt )

In.fingerd:192.168.57.151:spawn( /bin/echo -e "Permitido %a en puerto %d" >> /opt/accesos.txt
)

ALL: ALL: twist ( /bin/echo -e "Intruso %a en puerto %d" >> /opt/intrusos.txt )
```

Ejemplo 7:

Sistema abierto a la red local con reporte y cerrado al exterior con reporte:

```
#/etc/hosts.allow

ALL: LOCAL: spawn ( echo -e "Acceso autorizado de %a por %d" ) &

ALL: ALL: twist ( /bin/echo -e "INTRUSO! %a, usando puerto %d" ) &
```

Otro ejemplo:

```
[root@juan etc]# cat /etc/hosts.allow
#
# hosts.allow This file describes the names of the hosts which are
#             allowed to use the local INET services, as decided
#             by the '/usr/sbin/tcpd' server.
#
in.telnetd: 192.168.45.39: spawn (/bin/echo -e "Registro de usuario permitido %a en
puerto %d " >>/etc/permitidos.txt)
```

Taller : Permitir telnet a los equipos del mismo dominio (dejando rastro), permitir finger (dejando rastro) al vecino , permitir SSH al docente (IP 192.168.45.233) dejando rastro y cerrar todos los demas servicios (dejando rastro). El rastro de los permitidos deben quedar en : /opt/permitidos.txt , y los cerrados en /opt/intrusos.txt.

4.2. TALLER CON TCPWRAPPERS

Se desean permitir algunos servicios e implementar un mecanismo de detección de intrusos en cada máquina Linux de los estudiantes. Cada máquina de los grupos de trabajo , deben permitir hacer ftp desde las máquinas de la misma fila exclusivamente (desde ninguna otra máquina de la sala , ni de internet), pero se desea llevar un rastro de que máquinas han usado este servicio (el rastro debe quedar en un archivo llamado "/etc/rastroftp"). Todos los demás

servicios manejados por el xinetd no deben ser permitidos , y se desea dejar rastro de los intentos de las otras máquinas de utilizarlos en un archivo llamado “/etc/intrusos”).

4.3. FILTRADO CON IPTABLES

Una vez montados los servicios de internet, nos debemos preocupar por la seguridad de los mismos. Algunos de ellos tienen implementaciones propias , pero es conveniente tomar todas las medidas que nos permitan minimizar el riesgo.

Por tal razón trataremos como hacer un pequeño filtrado de tráfico hacia estos servicios.

Existe un artículo obtenido por internet , que nos ilustra esta situación y no amerita detallar más al respecto. El artículo es:

Iptables y el servicio de Traducción de Direcciones de Redes (NAT)

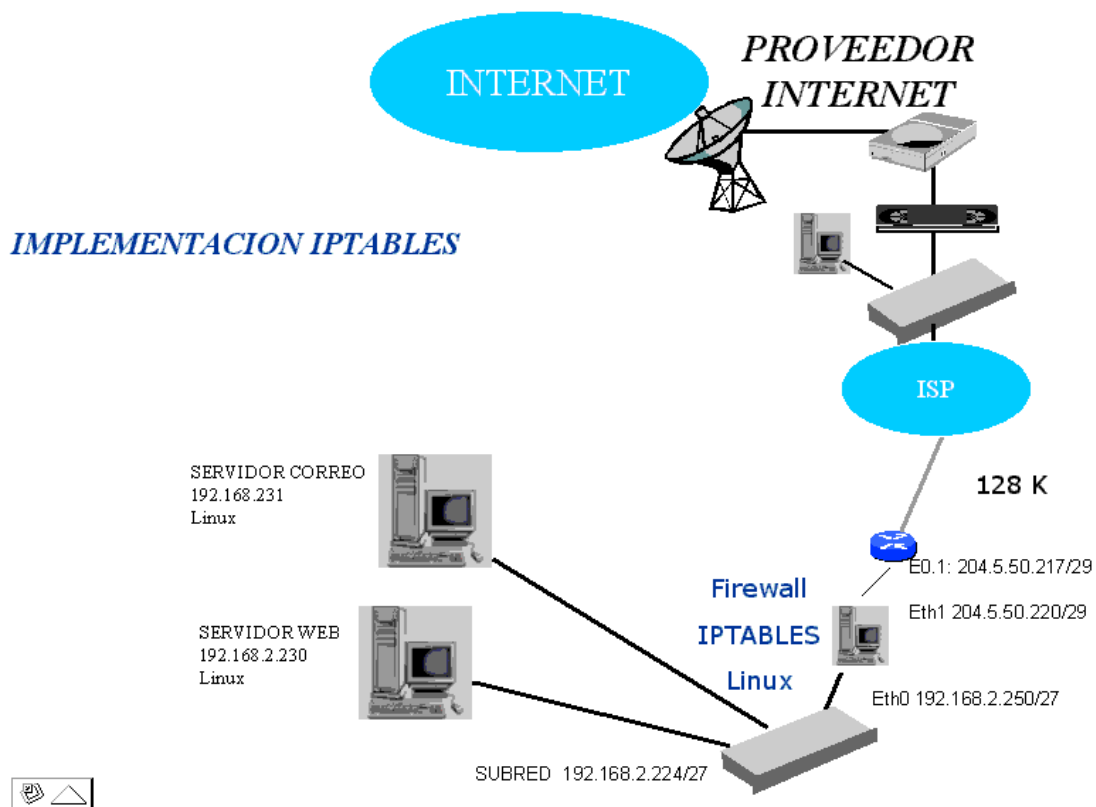
Por Haller Javier Bracho Hernández hbracho@linux.org.ve

Objetivo: Implementar un router/firewall con NAT

El archivo PDF lo anexo en el CD.

4.4. EJERCICIO TEORICO CON IPTABLES

Según el diagrama:



Se deben escribir las reglas correspondientes (iptables) que permitan implementar un pequeño firewall en una máquina Linux así:

- En la red hay 20 Pcs y dos servidores y se requiere que estos PCs y servidores pueden acceder internet sin requerir a un proxy.

- Se desea implementar proxy transparente. A diferencia del punto anterior se desea colocar un proxy con su cache y restricciones de sitios web , pero que los usuarios no sepan de la existencia de este o deban hacer cambios en las configuraciones.
- Las conexiones externas dirigidas al firewall por el puerto 80 , se deben dirigir internamente al servidor web por ese puerto.
- Las conexiones dirigidas al firewall para entregarle correo se deben dirigir internamente al servidor de correo por el puerto correspondiente.
- Algunos usuarios pueden leer correo de forma encriptada desde el exterior de la red usando el outlookp con SSL. Las conexiones dirigidas al firewall para pedir correo se deben dirigir internamente al servidor de correo por el puerto correspondiente.
- No se deben permitir más conexiones ni servicios hacia adentro de ninguna clase ni hacia ninguna otra máquina .

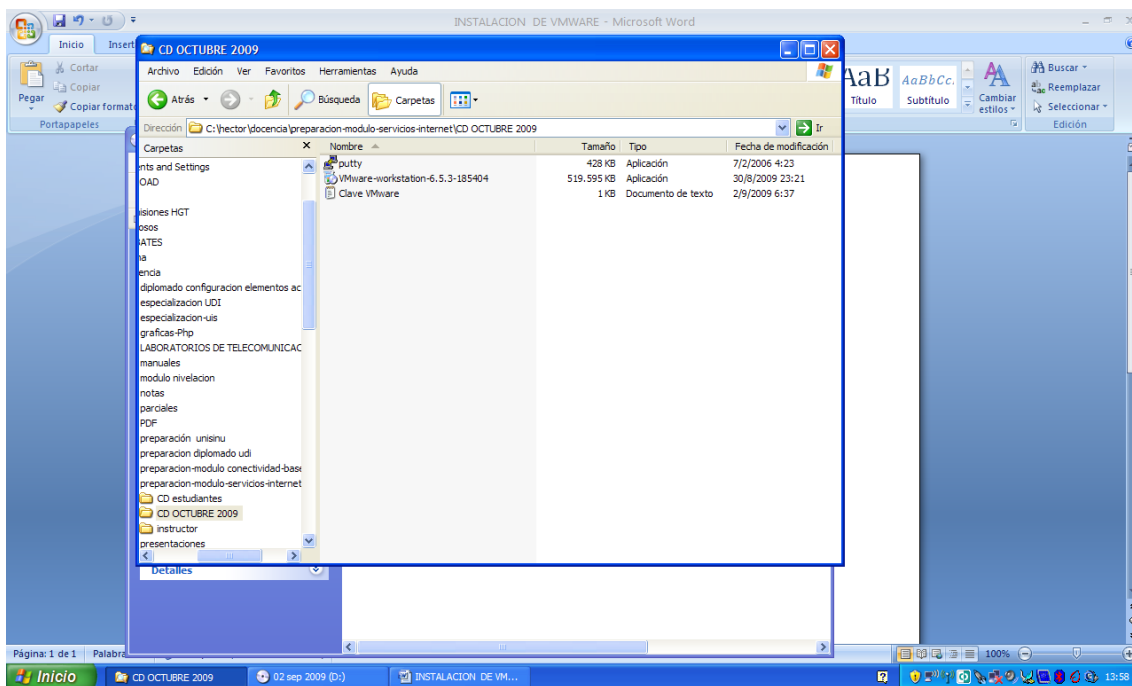
5. VIRTUALIZACION

Para efectos de estas practicas, veremos herramientas que permiten en el PC Windows, tener virtualizado un equipo Linux.

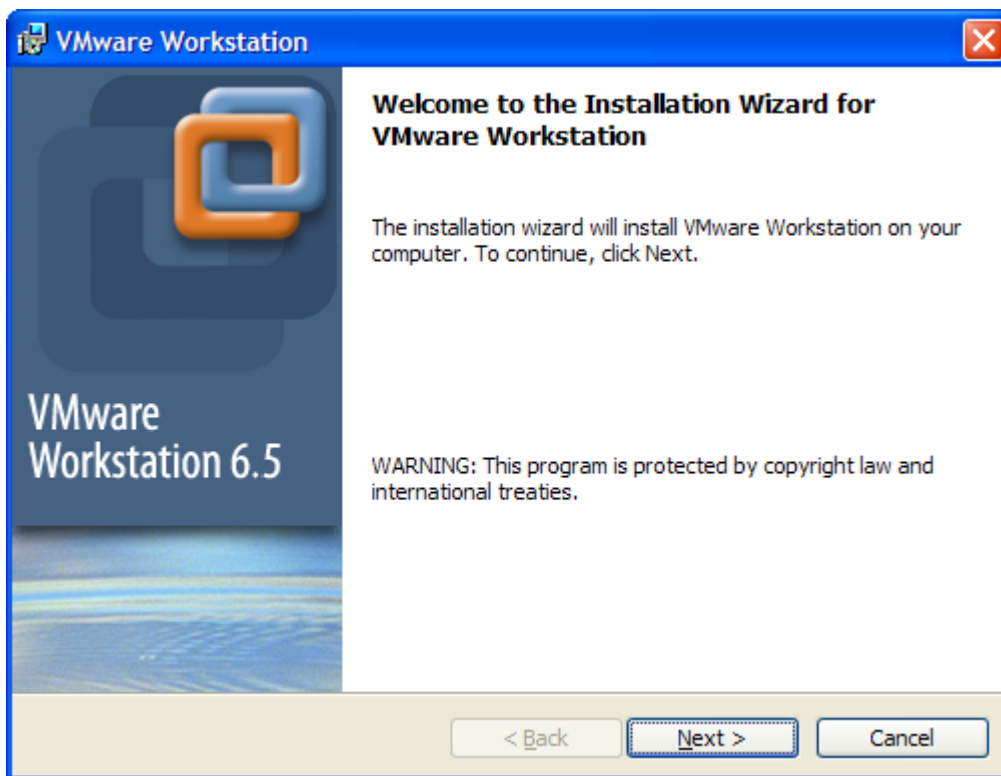
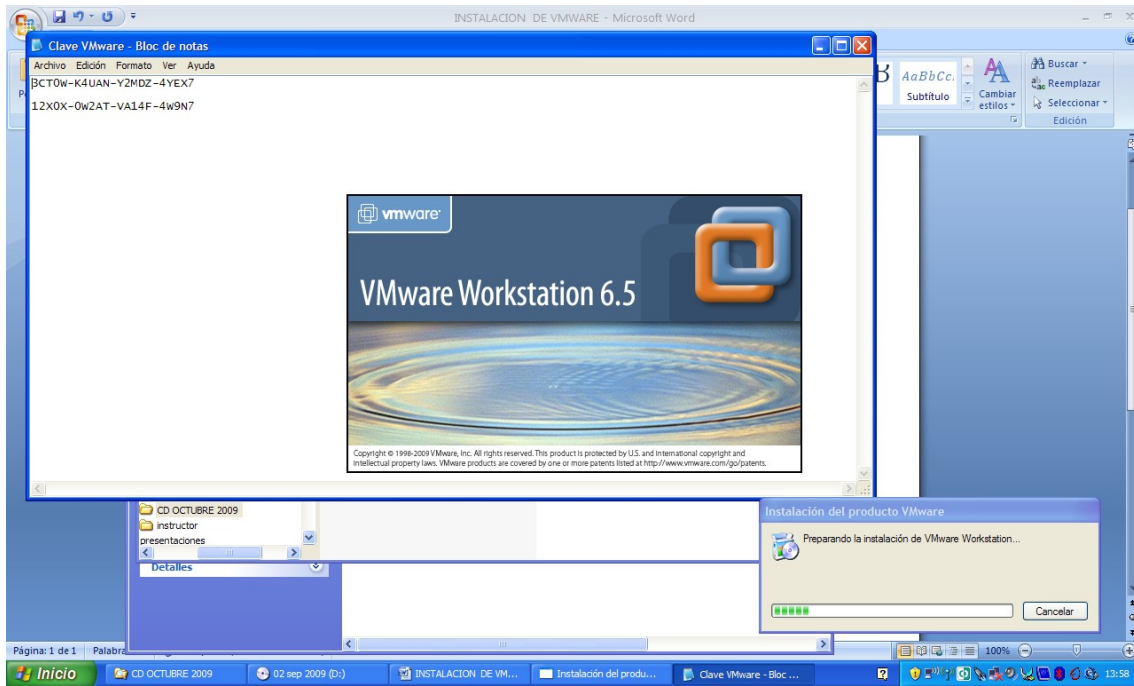
5.1. VIRTUALIZACION CON VMWARE

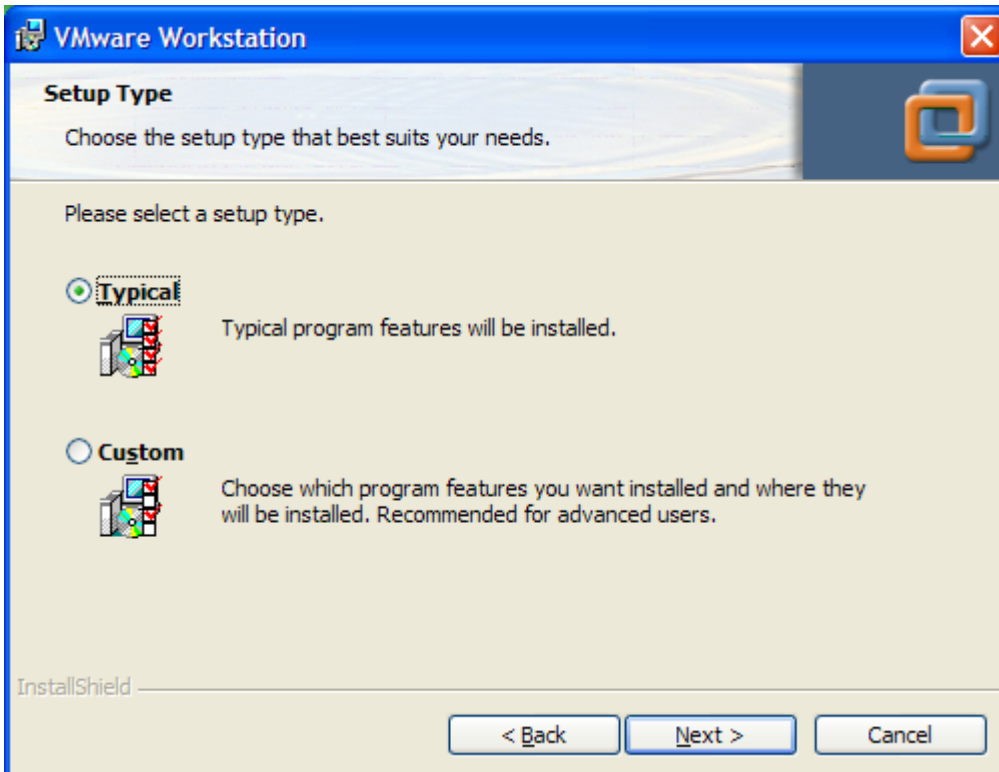
Con la herramienta VMWARE, se permitirá crear una máquina virtual en el PC, donde se realizará la instalación del sistema Linux. Así se tendrá los dos ambientes activos en el mismo equipo, y para cambiar de ambiente de trabajo, simplemente se procede a cambiar de ventana activa.

Ubicados en la capeta donde reside el instalador se ejecuta.

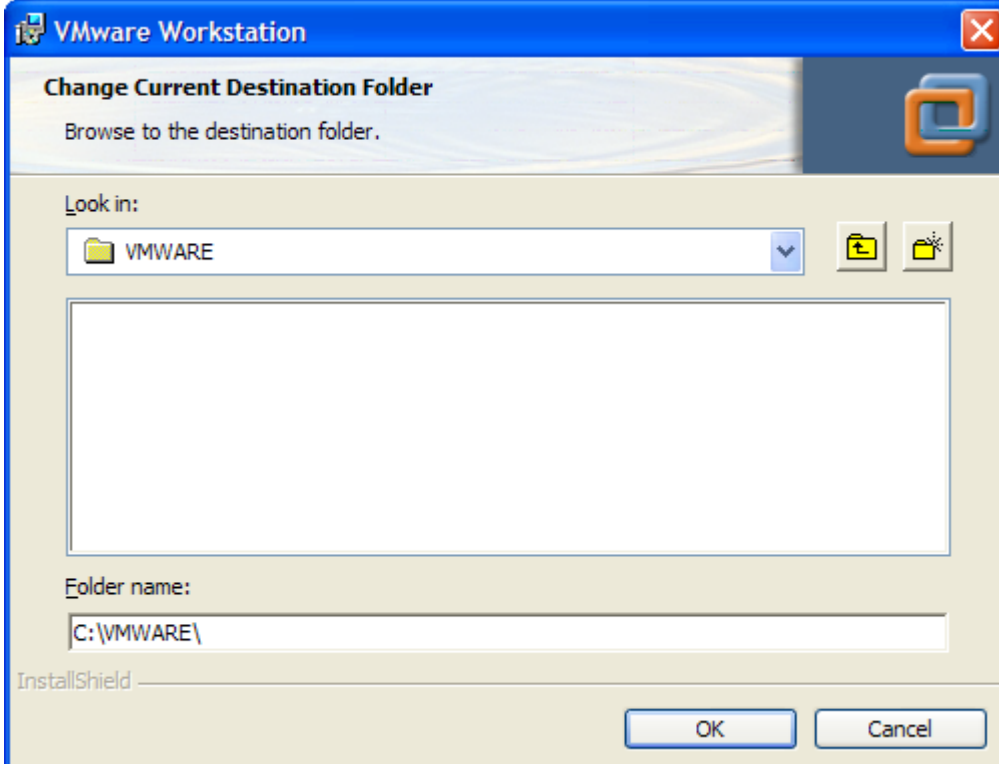


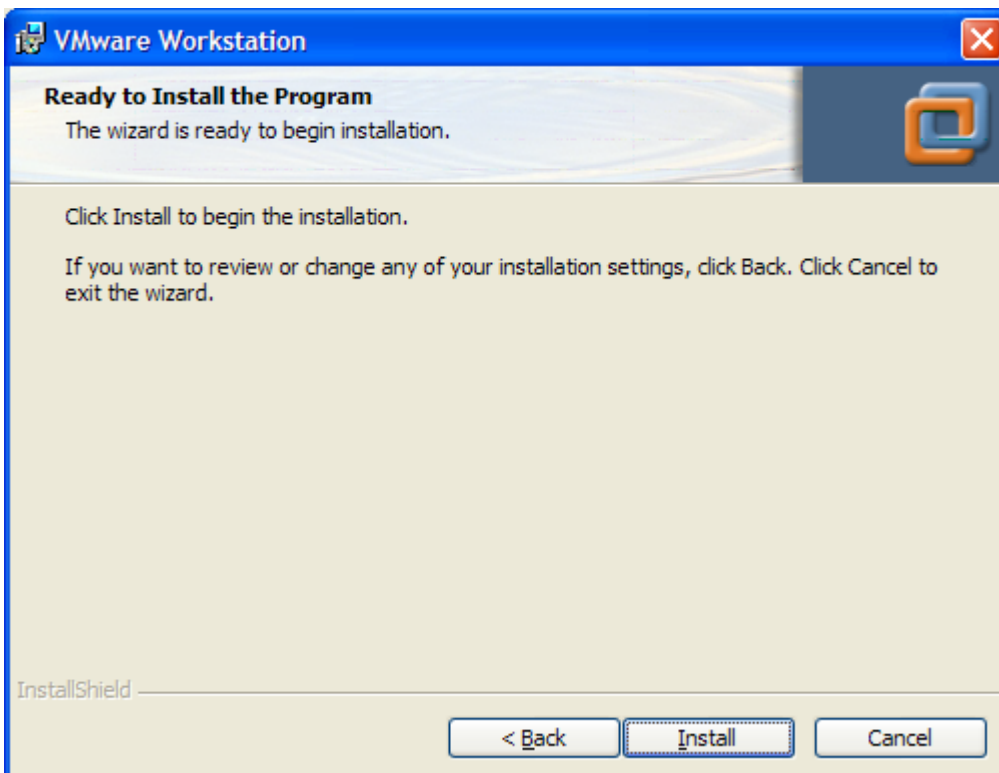
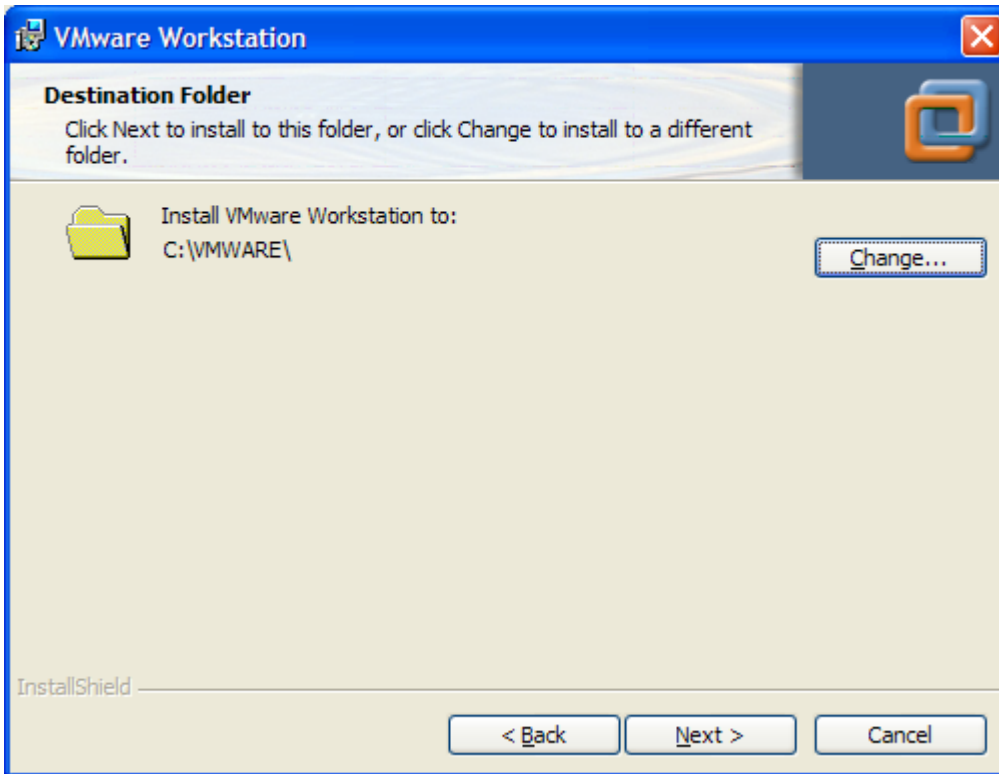
Se inicia la instalación, y se debe contar con el numero de licencia

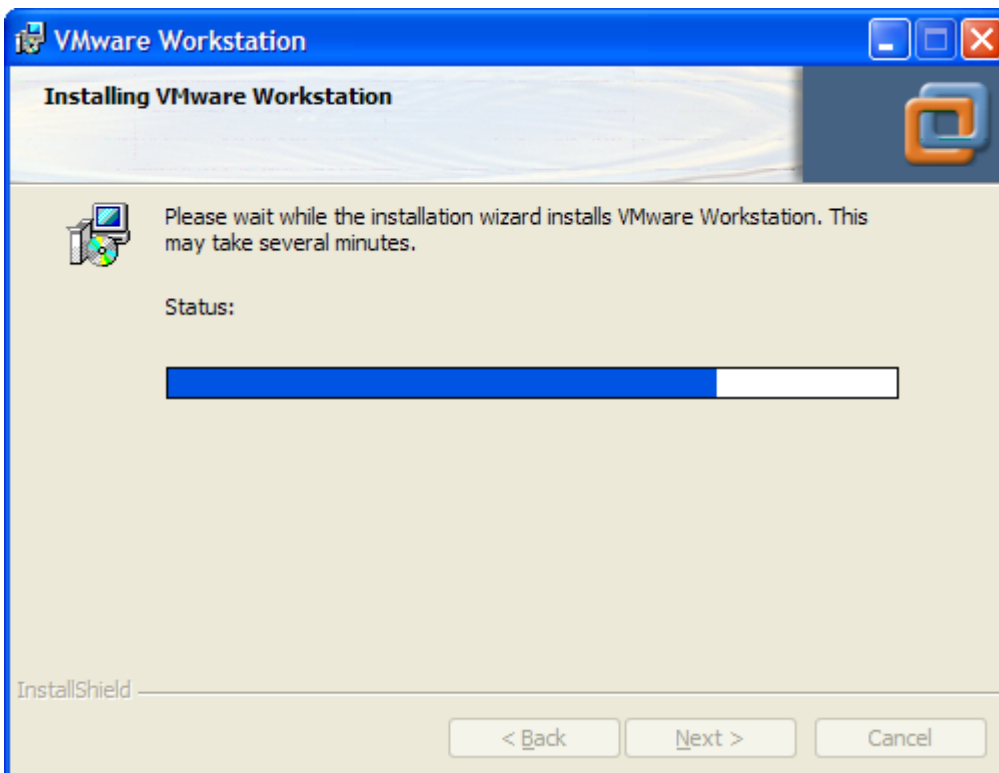
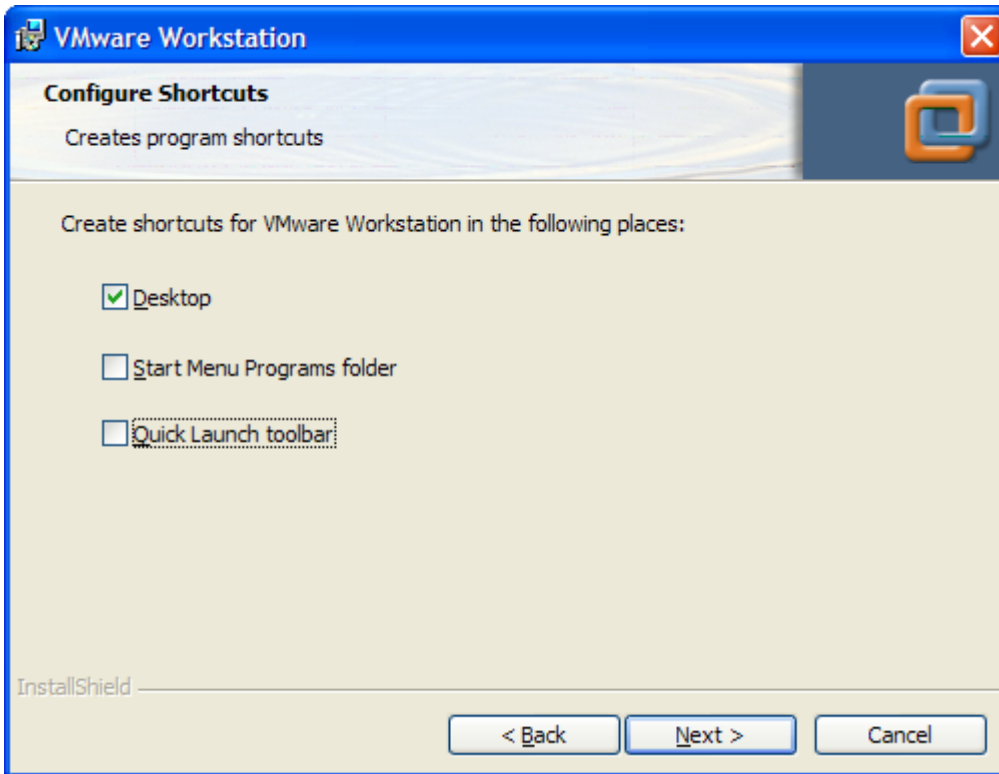


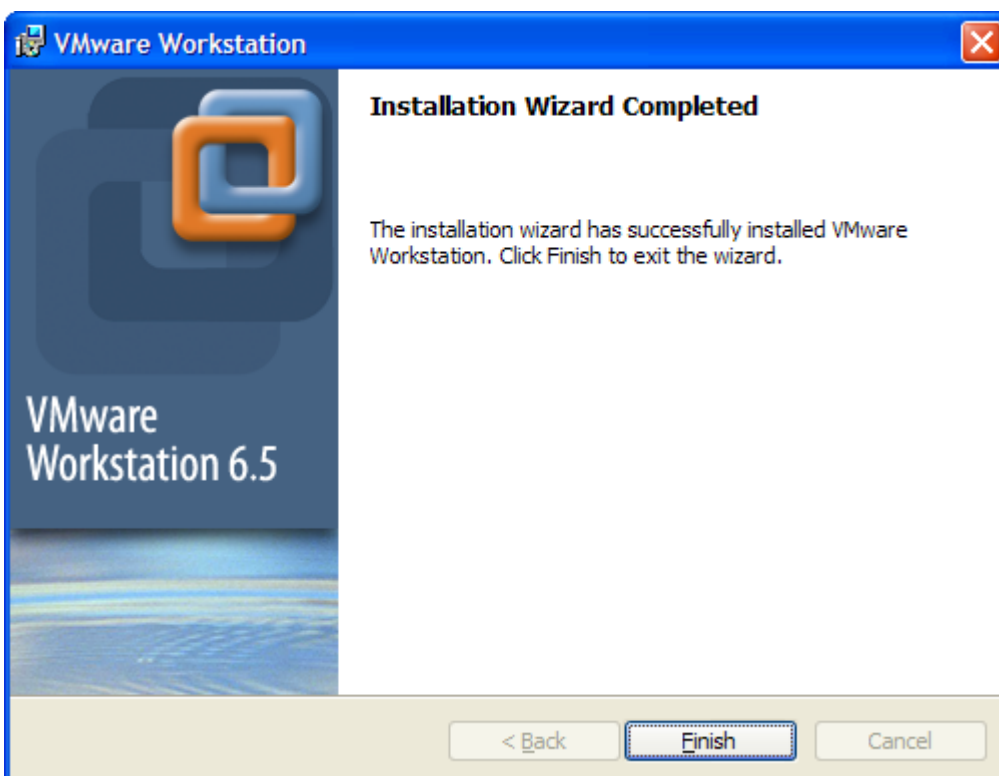
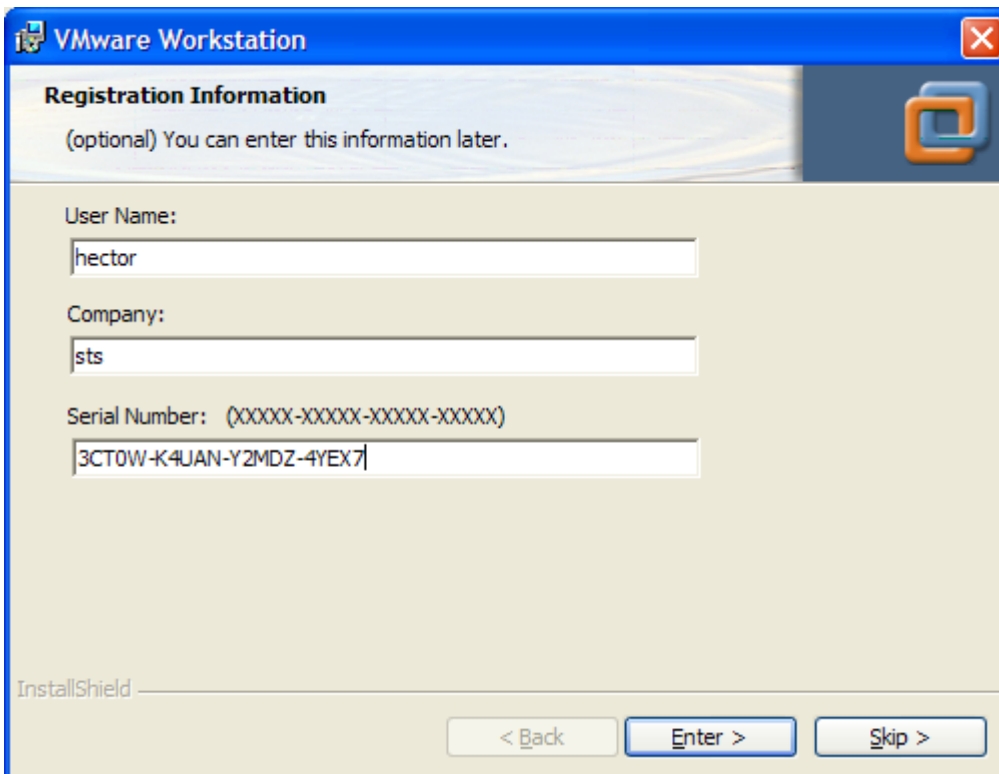


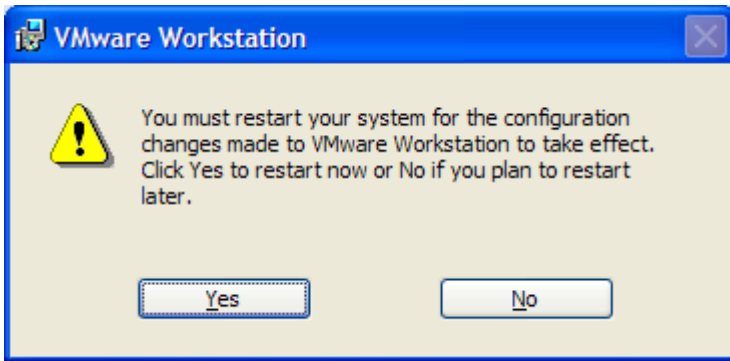
Se deja los archivos de configuración en una carpeta especifica, que puede estar en C: o D: .



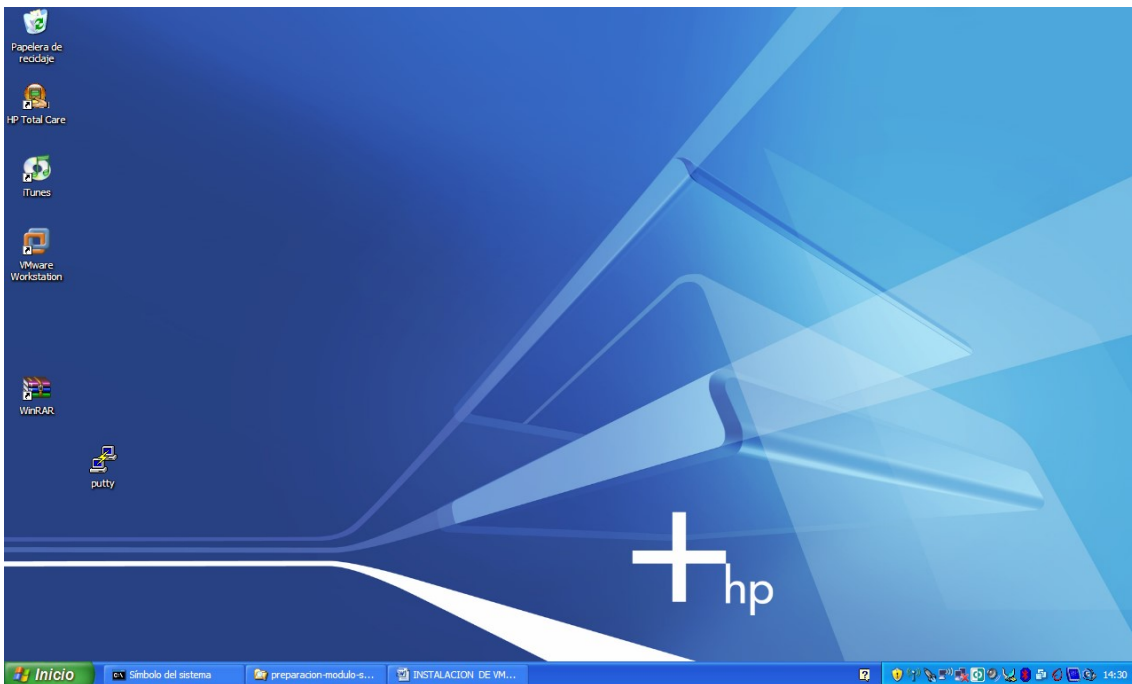


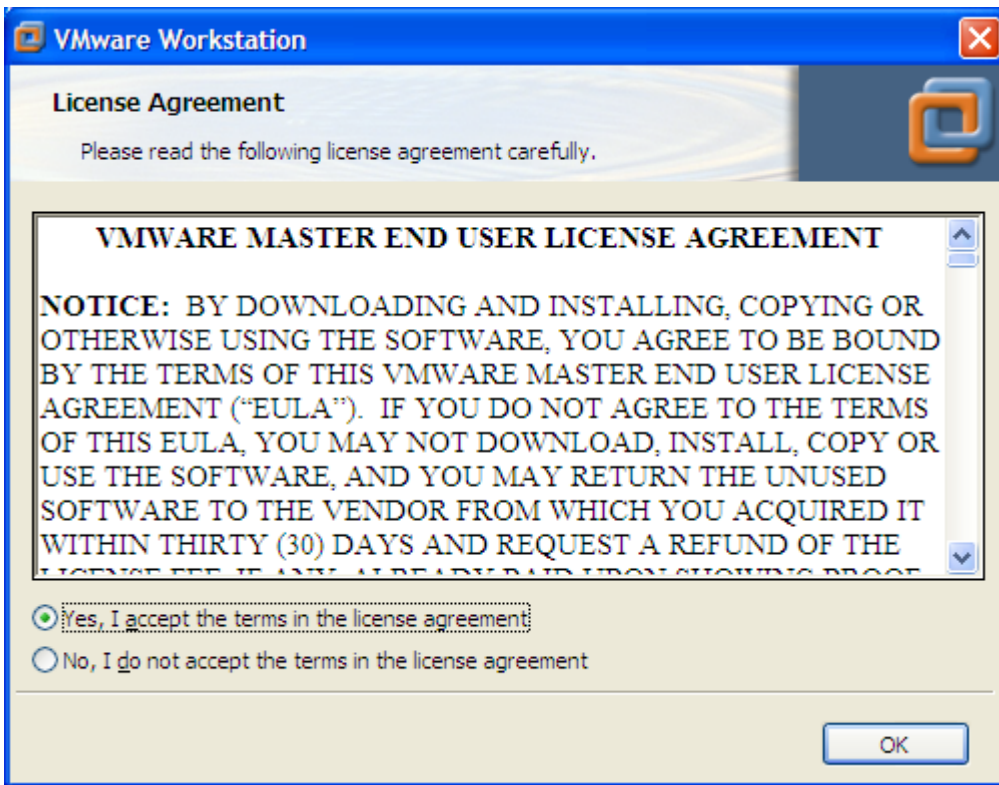




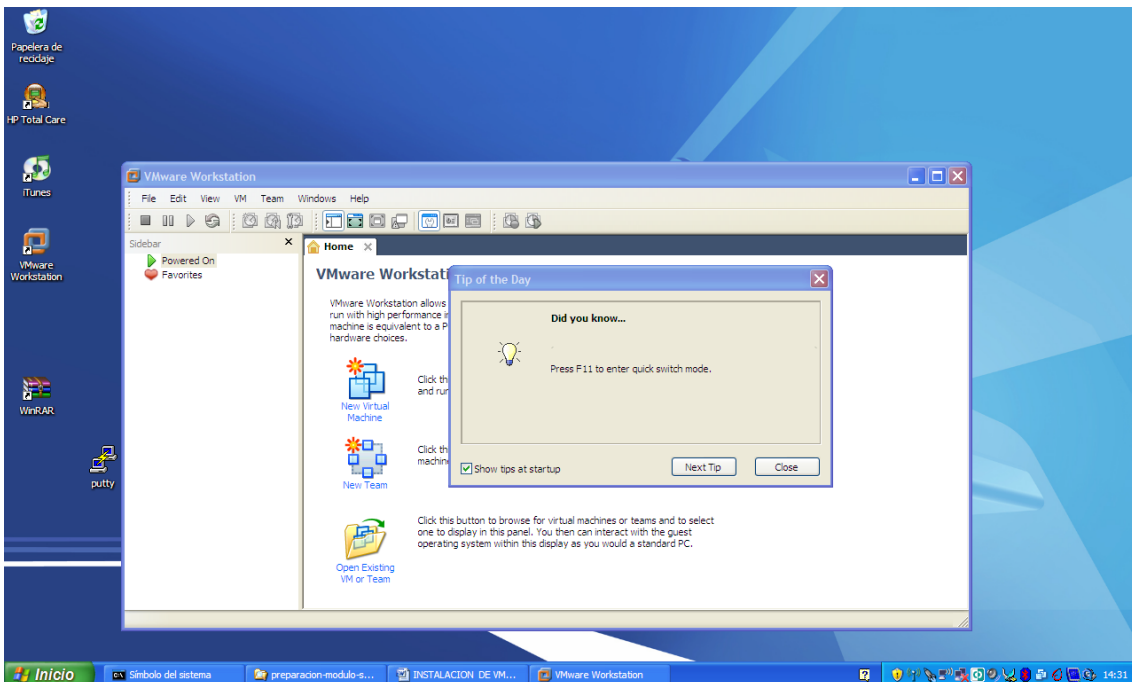


Una vez el reboot se efectuó , al iniciar se observa el icono del vmware en el escritorio. Se carga este

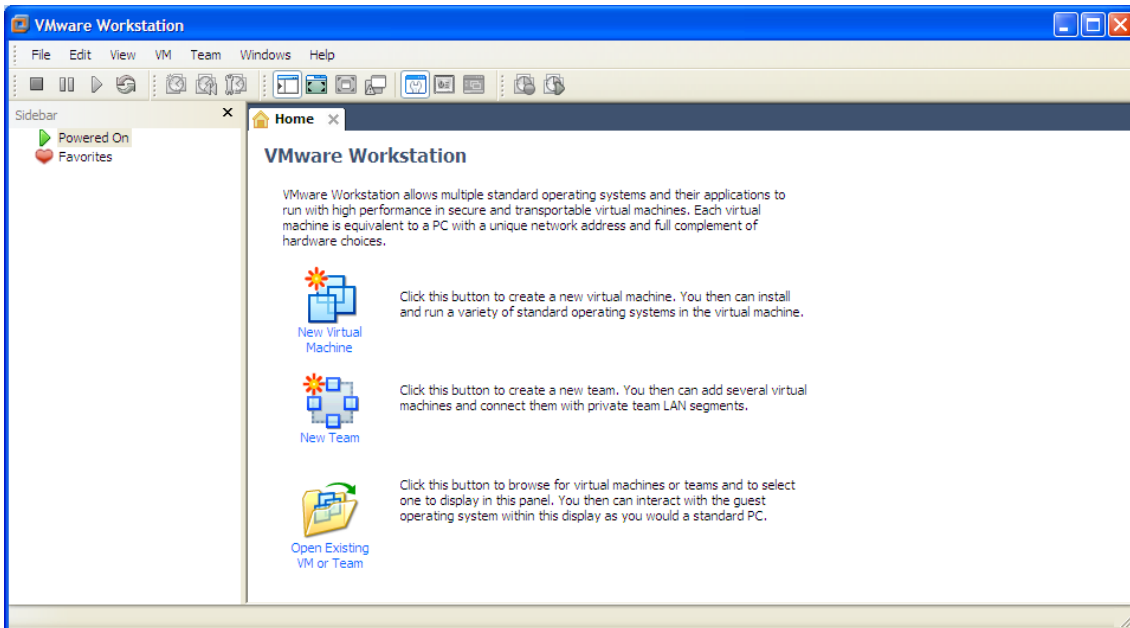




Se acepta y carga mostrando indicaciones. Se escoge que no vuelva a mostrarlas



Se cierra la ventana de tips o trucos



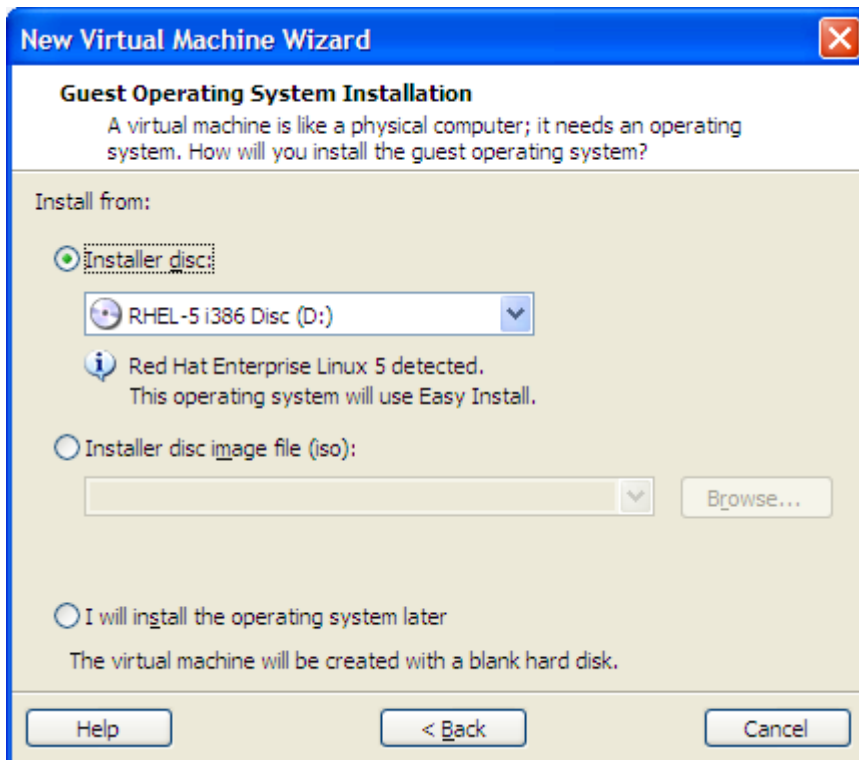
Hasta aquí se tiene el producto instalado y se pueden crear las máquinas virtuales para instalación de los sistemas operativos huéspedes (guest).

Para efectos de las prácticas a realizar, se puede proceder de varias formas en este momento:

5.1.1.INSTALACION DE UNA MAQUINA VIRTUAL Y UN SISTEMA OPERATIVO CON UNA CONFIGURACION POR DEFECTO

Se escoge crear una nueva maquina virtual

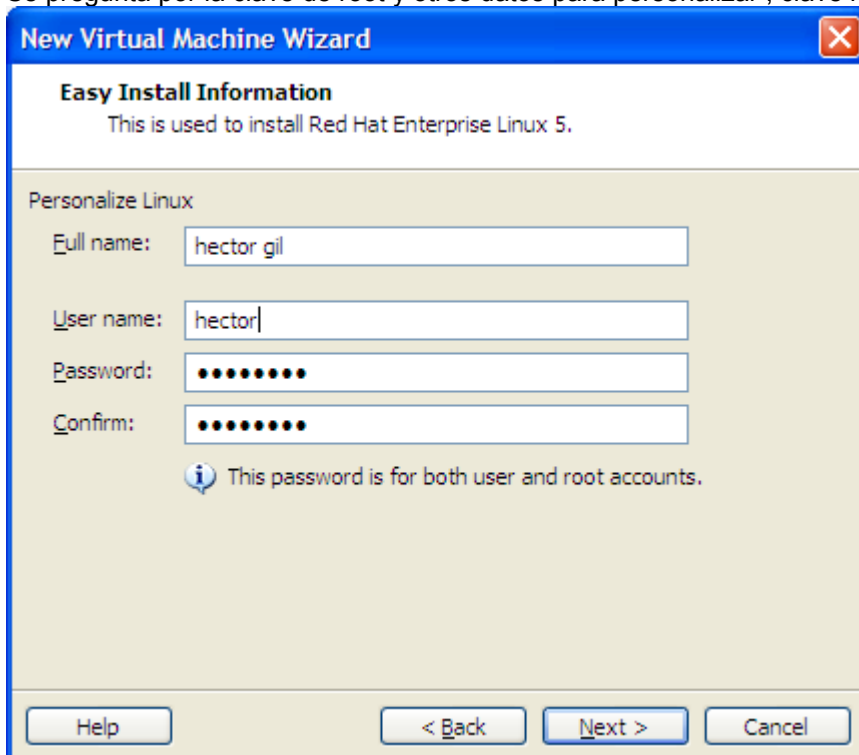




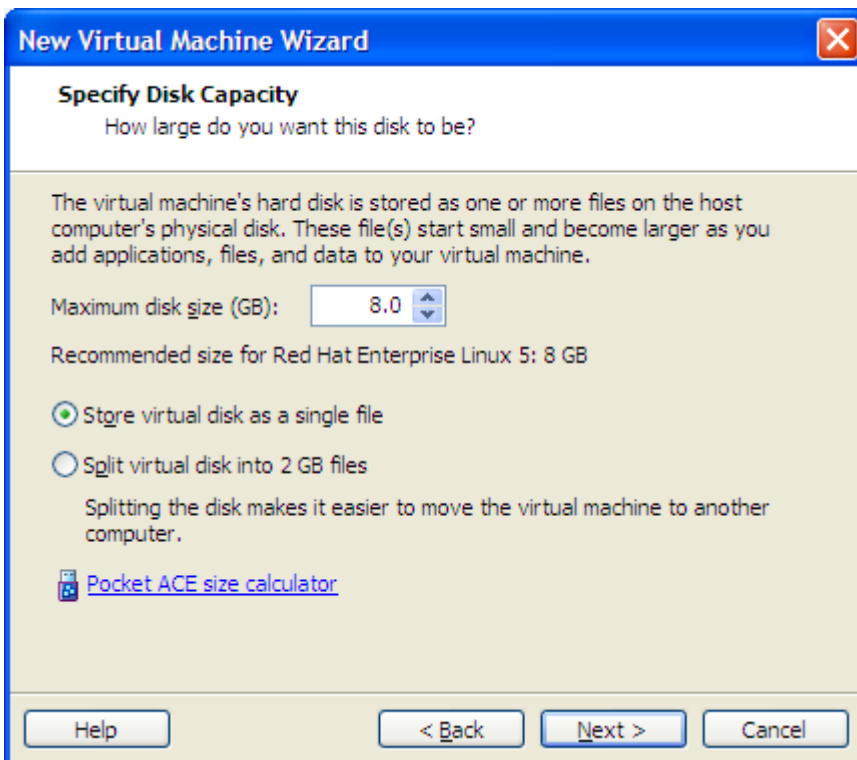
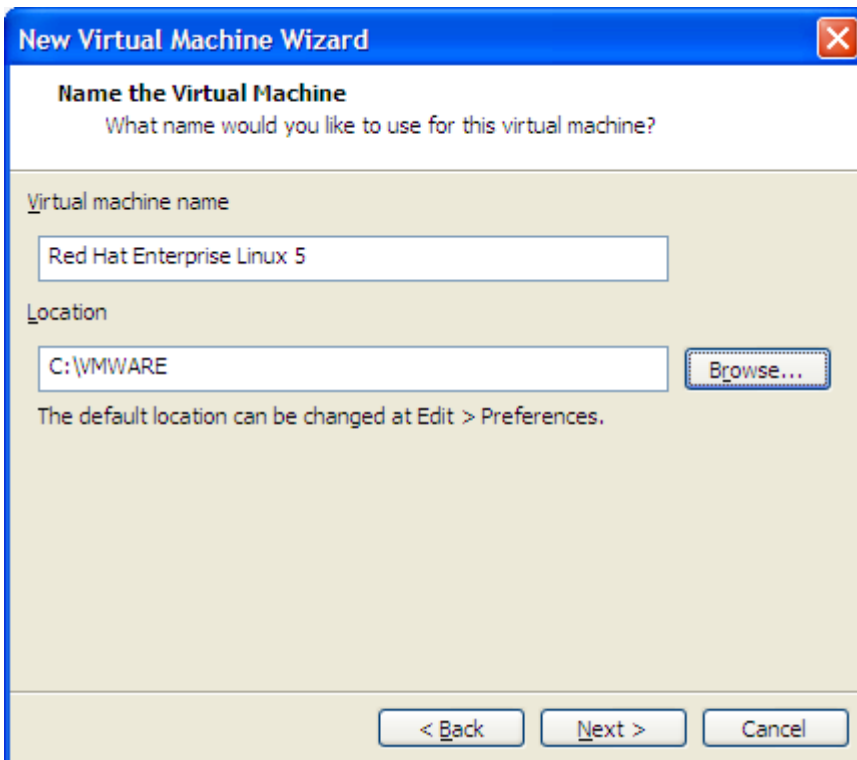
Si se va a hacer una instalación de un sistema operativo desde CD, se escoge. Pero se puede cargar desde una imagen ISO. Para este caso , voy a instalar el sistema Linux desde CDs (pero es el mismo proceso para DVD)..

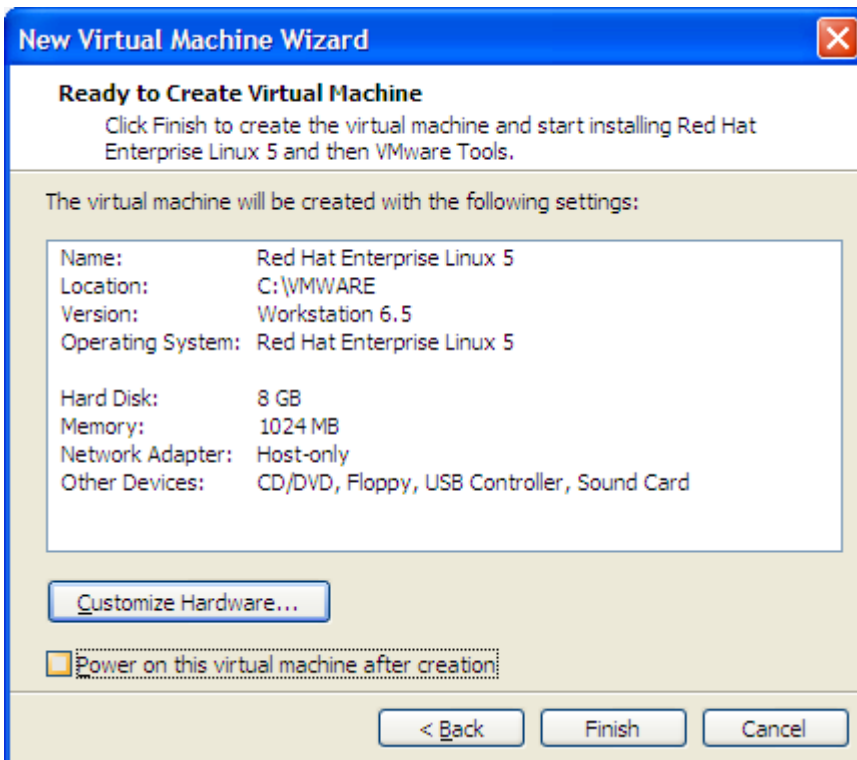
Al colocar el CD de redhat Enterprise 1 e 5 , muestra en la ventana desplegable la versión. Esta versión es para equipos de 32 bits.

Se pregunta por la clave de root y otros datos para personalizar , clave root2009

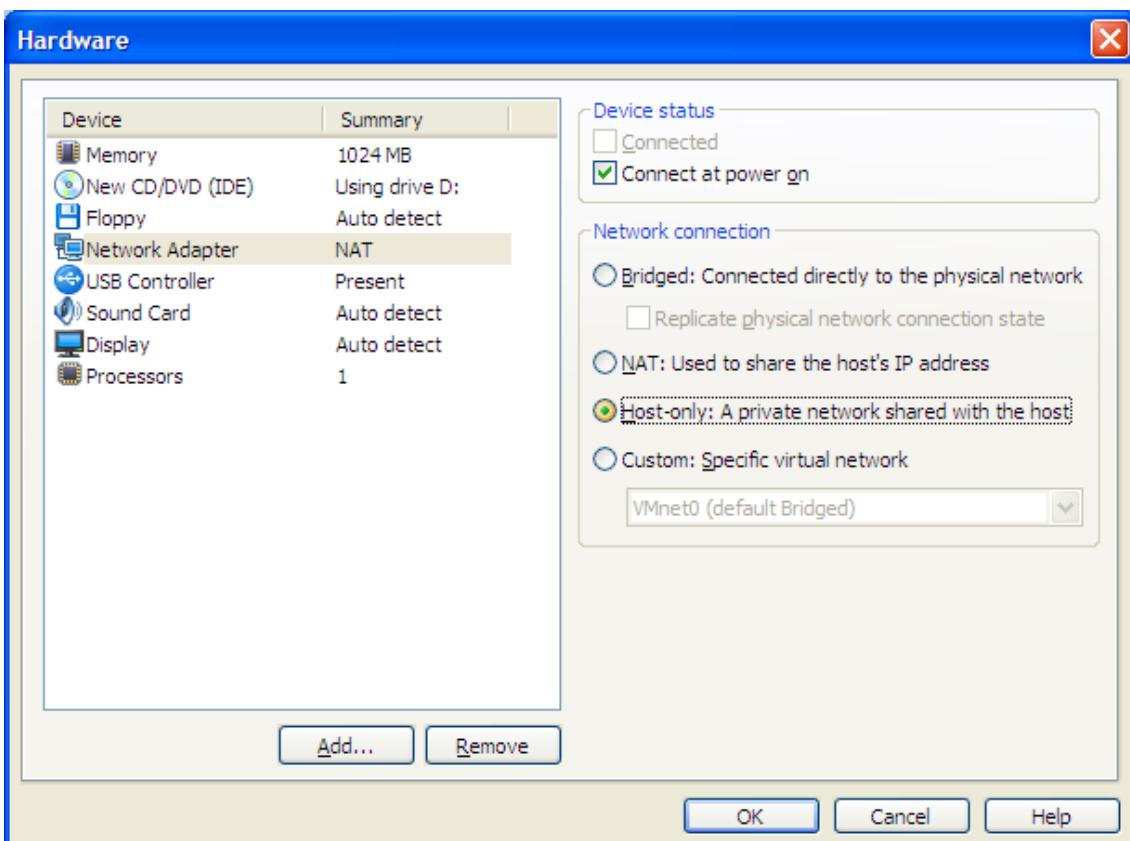


Se indica la ubicación de los archivos de la maquina virtual



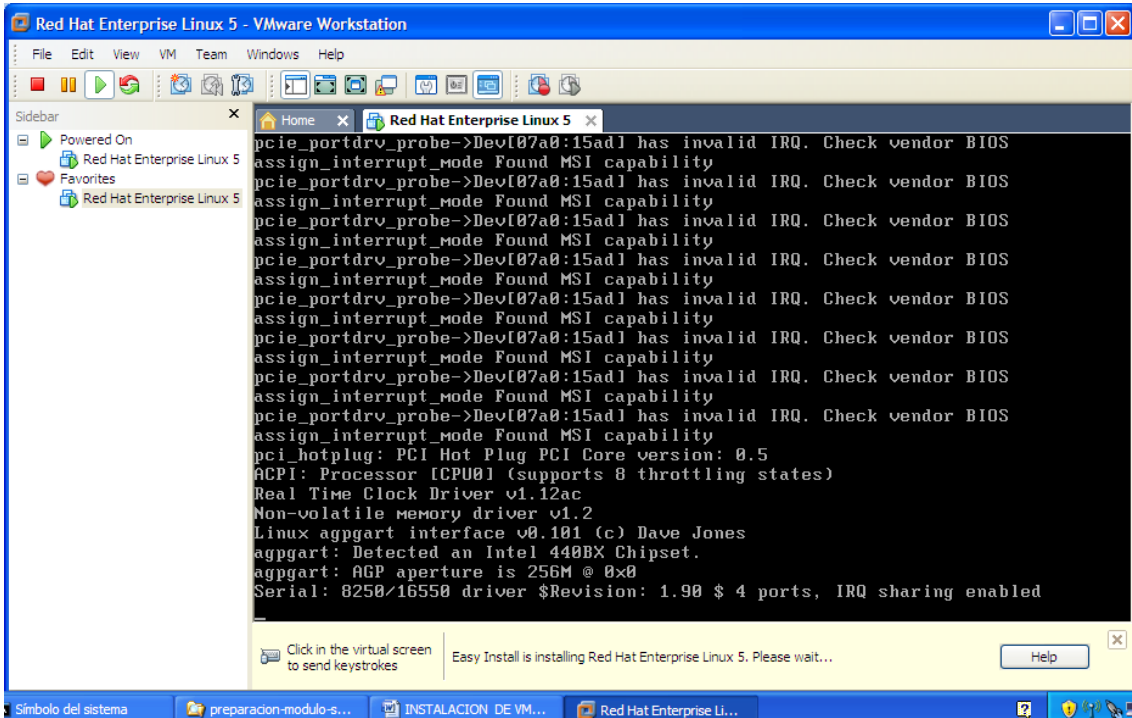


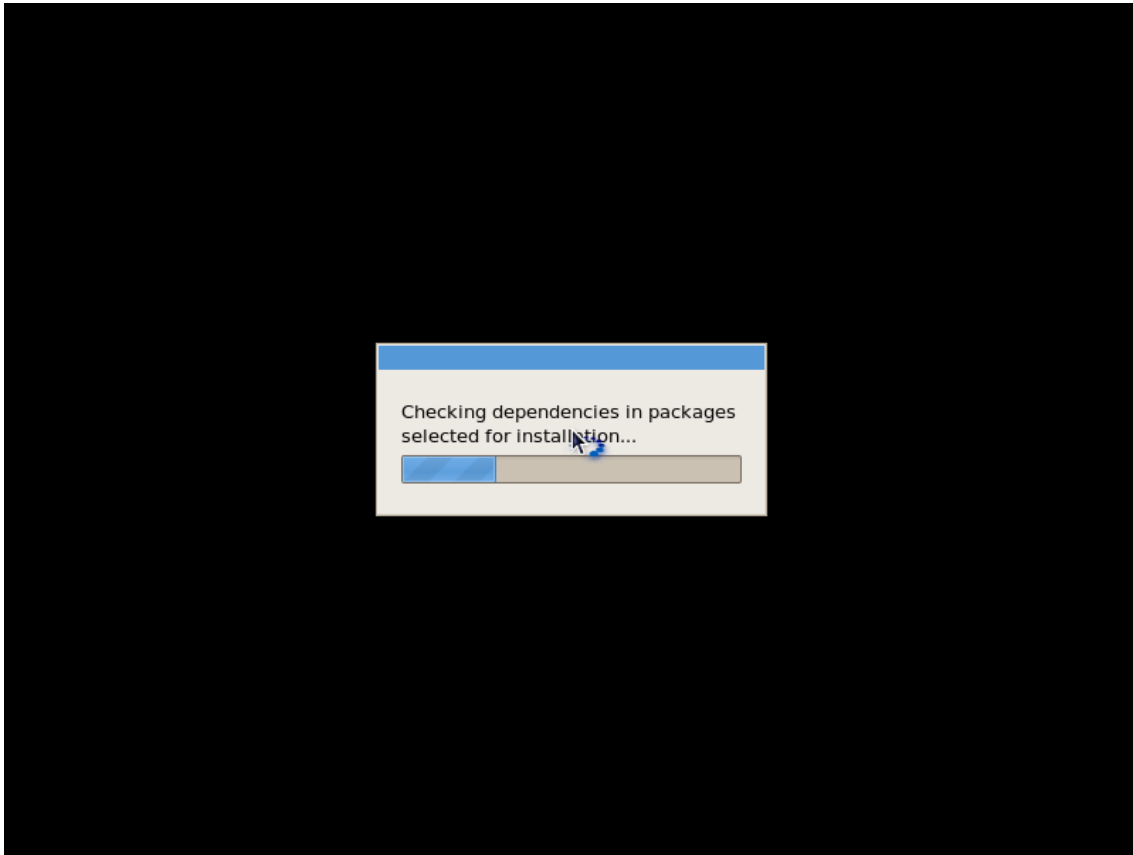
Se cambio el tipo de adaptador de red por customizar hardware



Al regresar a la ventana. Al final se indica que arranque la maquina virtual al terminar la instalación

De aquí en adelante , se procede con una instalación de Linux convencional, pero con una configuración de paquetes y particiones por defecto.

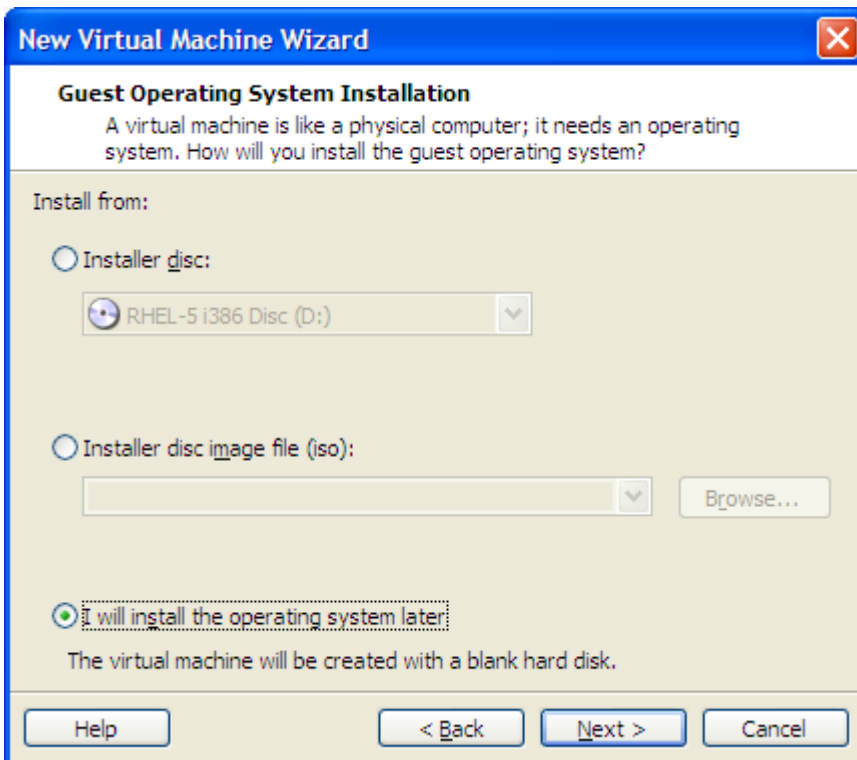




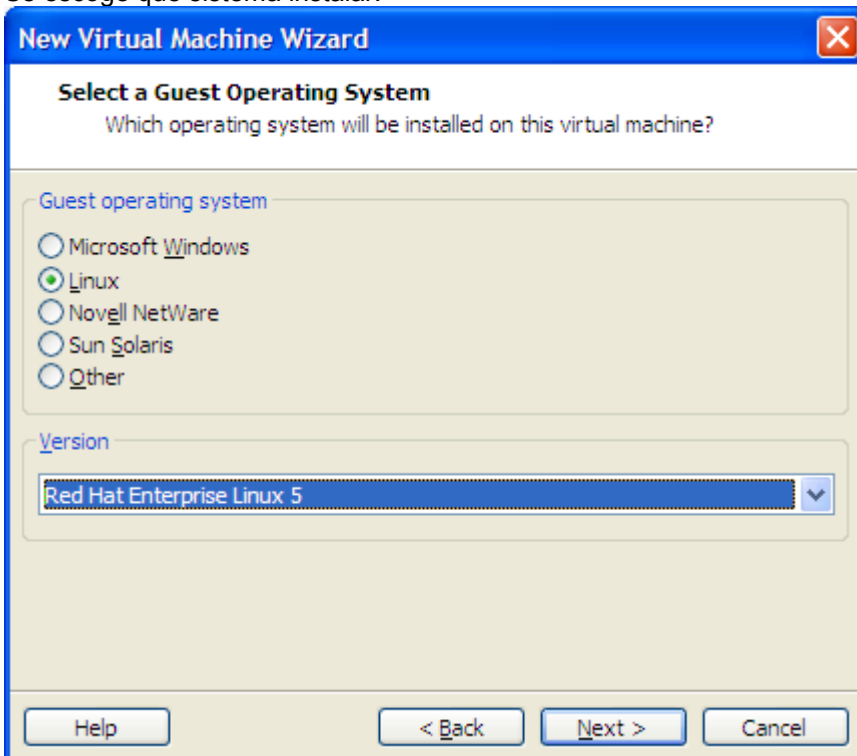
Como no se indico que tipo de instalación es, procede automáticamente e instalará RedHat Linux ,con unos paquetes por defecto, y de igual forma las particiones, y otros parámetros del sistema. El resto de instalación es semejante, a la que se verá en el numeral 2, una ves se llegue a la etapa de seleccionar los productos de software deseados.

5.1.2.INSTALACION DE UNA MAQUINA VIRTUAL CON UN SISTEMA OPERATIVO PERSONALIZADO

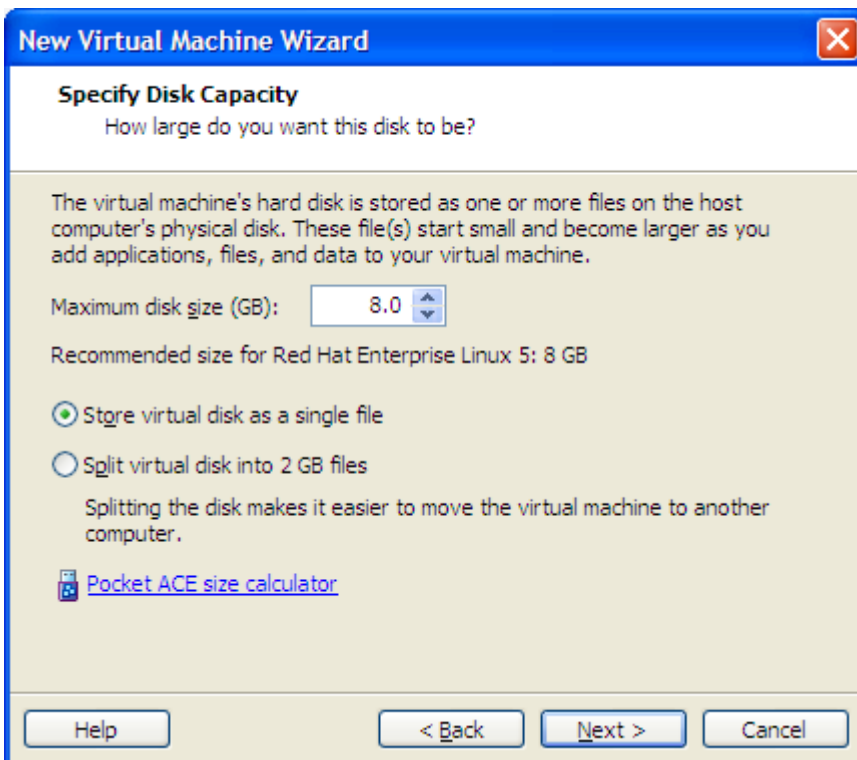
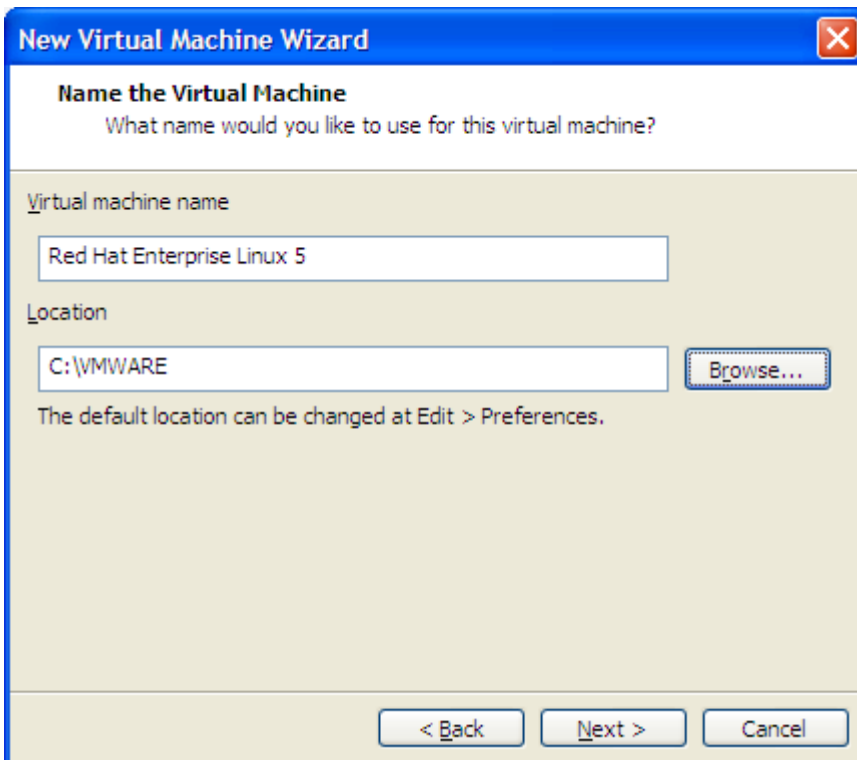
Al crear la maquina virtual se escoge el sistema huésped pero al final de la ventana se indica que se instalará más tarde.

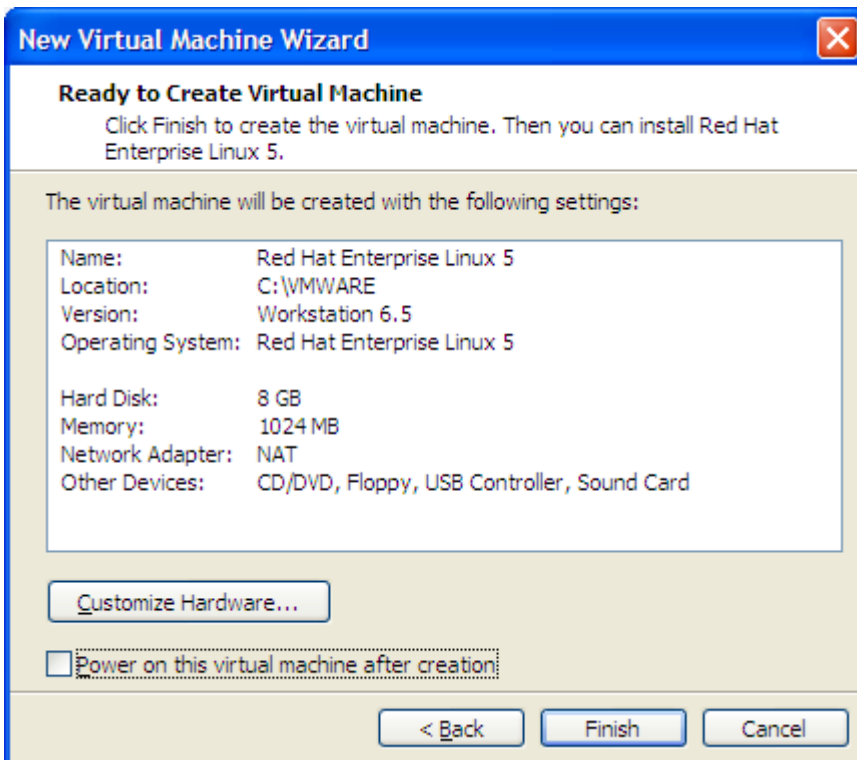


Se escoge que sistema instalar.

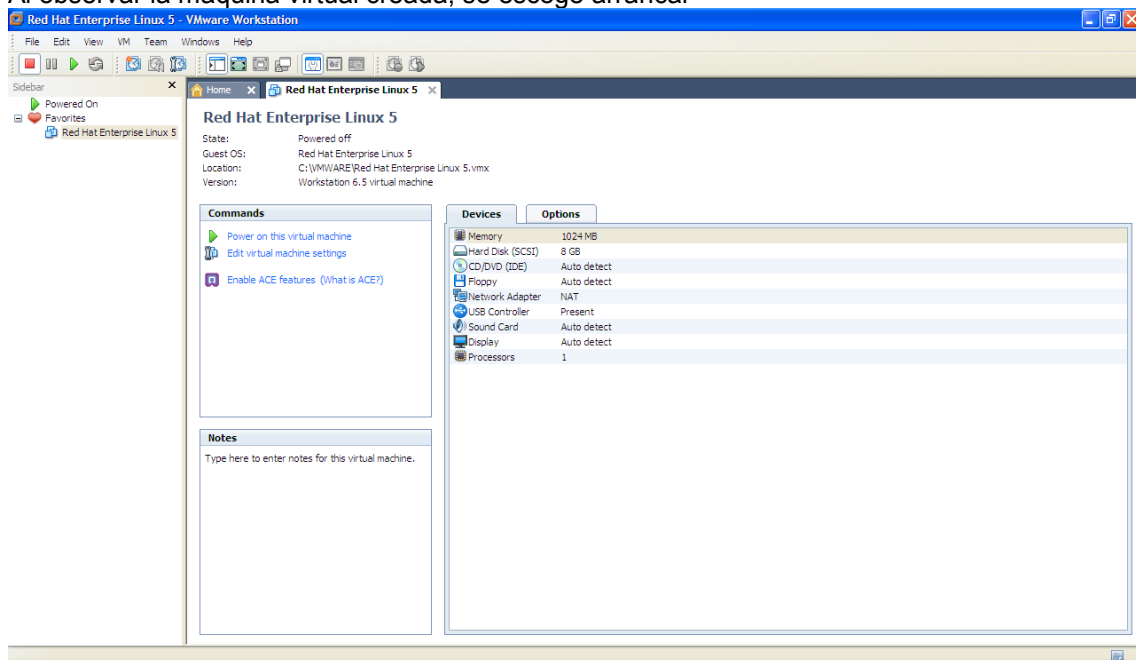


La ruta de los archivos de configuración y de la imagen creada de esa máquina virtual.





Al observar la máquina virtual creada, se escoge arrancar

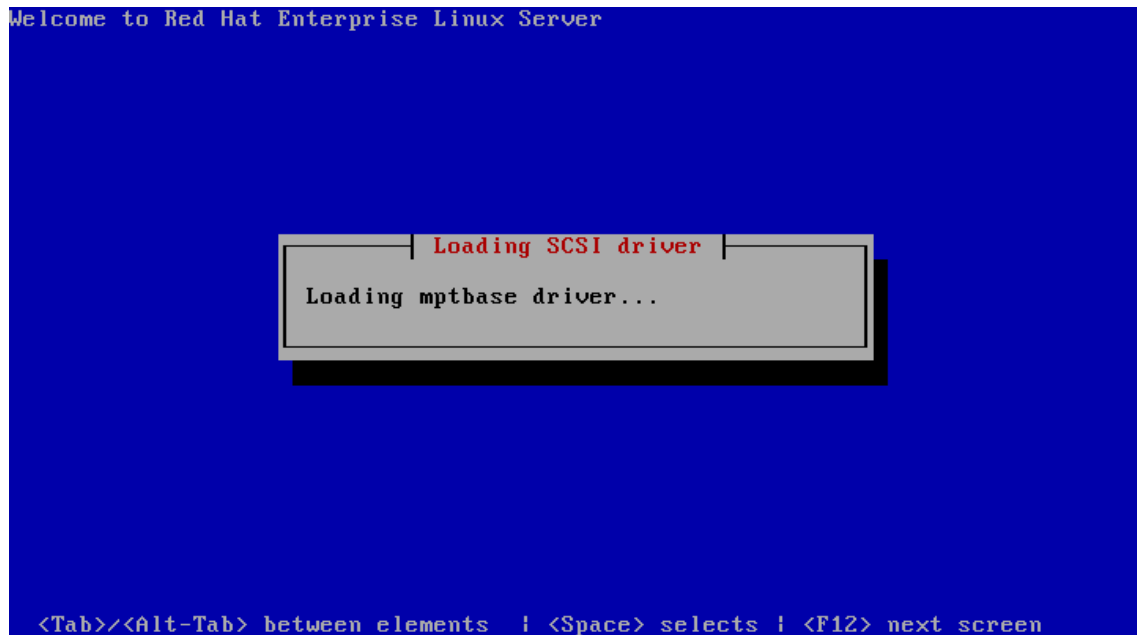


Se arranca con power y en el dialogo se escribe Linux expert para que que pregunte por todo (frente al prompt boot:)




De aquí en adelante se realiza una instalación de Linux personalizada.

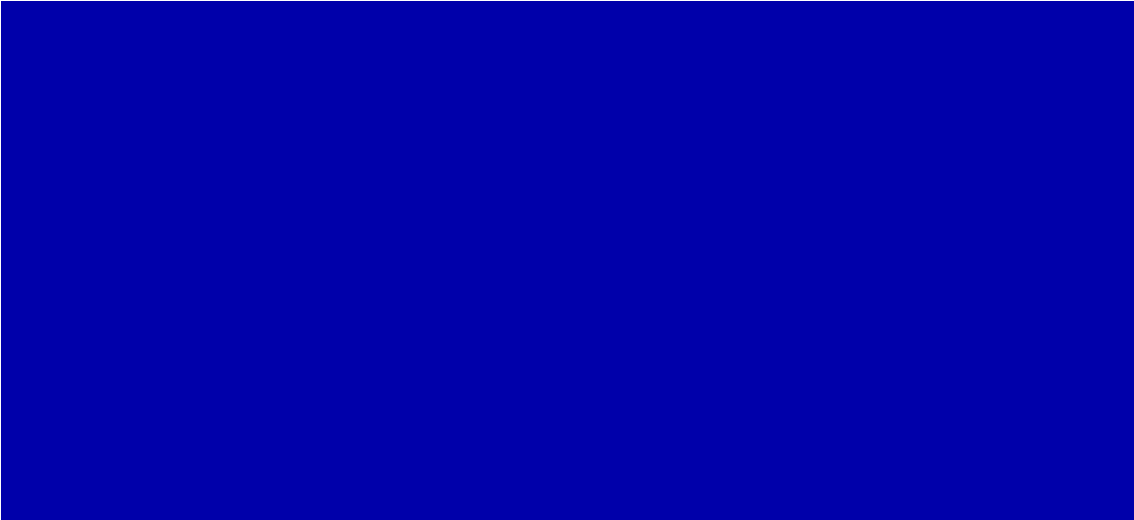
```
assign_interrupt_mode Found MSI capability
pci_portdrv_probe->Dev[07a0:15ad] has invalid IRQ. Check vendor BIOS
assign_interrupt_mode Found MSI capability
pci_hotplug: PCI Hot Plug PCI Core version: 0.5
ACPI: Processor [CPU0] (supports 8 throttling states)
Real Time Clock Driver v1.12ac
Non-volatile memory driver v1.2
Linux agpgart interface v0.101 (c) Dave Jones
agpgart: Detected an Intel 440BX Chipset.
agpgart: AGP aperture is 256M @ 0x0
Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
serial8250: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
00:09: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
00:0a: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
RAMDISK driver initialized: 16 RAM disks of 16384K size 4096 blocksize
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller at PCI slot 0000:00:07.1
PIIX4: chipset revision 1
PIIX4: not 100% native mode: will probe irqs later
   ide1: BM-DMA at 0x10c8-0x10cf, BIOS settings: hdc:DMA, hdd:pio
hdc: VMware Virtual IDE CDROM Drive, ATAPI CD/DVD-ROM drive
ide1 at 0x170-0x177,0x376 on irq 15
```

Se indicó que no se chequearan los medios de instalación.




```
Running anaconda, the Red Hat Enterprise Linux Server system installer - please  
wait...
```



```
Running anaconda, the Red Hat Enterprise Linux Server system installer - please  
wait...  
Probing for video card:  VMware Inc [VMware SUGA III] PCI Display Adapter
```

RED HAT ENTERPRISE LINUX 5



 Release Notes

 Back

 Next


Se escoge el idioma:

RED HAT ENTERPRISE LINUX 5



What language would you like to use during the installation process?

- Russian (Русский)
- Serbian (српски)
- Serbian(Latin) (srpski(latinica))
- Sinhala (සිංහල)
- Slovak (Slovensky)
- Slovenian (slovenščina)
- Spanish (Español)
- Swedish (Svenska)
- Tamil (தமிழ்)
- Telugu (తెలుగు)
- Turkish (Türkçe)
- Ukrainian (Українська)

 Release Notes

 Back

 Next



Se pregunta por el número de la licencia adquirida, pero si no se tiene, se puede omitir.



Se ratifica que se va a omitir. Se escoge el teclado.



Y se advierte que se va a recrear las particiones de disco. Si se desea un particionamiento personalizado, escogiendo cada partición, su tamaño, etc, se indica que se revise y modifique.



RED HAT ENTERPRISE LINUX 5

La instalación requiere la partición de su disco duro. Por defecto, una capa de partición razonable es escogida, ésta es suficiente en la mayoría de los casos. Usted puede predeterminada o c

Remove particione

Seleccione la(s)

sda 81

Aviso

Ha seleccionado borrar todas las particiones (TODOS LOS DATOS) en las siguientes unidades:

/dev/sda

¿Está seguro que quiere hacerlo?

[+ Configuración Avanzada de almacenamiento](#)

Revise y modifique la capa de particiones

[Notas de lanzamiento](#)

[← Atrás](#)

[→ Siguiente](#)

Para efectos de este ejercicio, las particiones se dejaran como están.

RED HAT ENTERPRISE LINUX 5

Disco /dev/sda (8189 MB) (Modelo: VMware, VMware Virtual S)

sda2
18087 MB

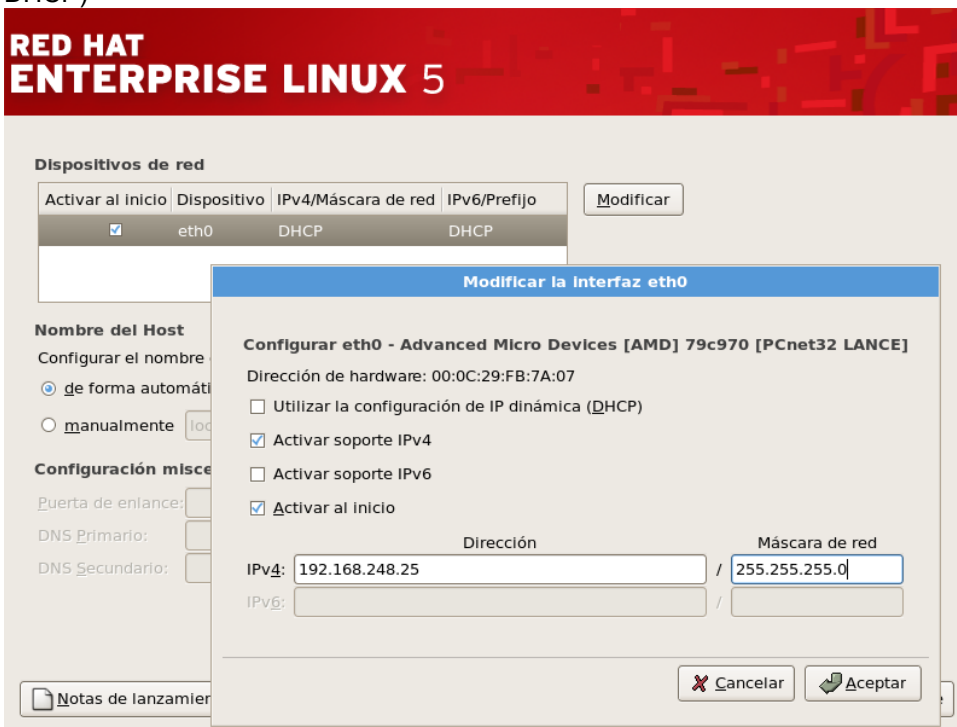
Dispositivo	Punto de Montaje/ RAID/Volumen	Tipo	Formato	Tamaño (MB)	Inicio	Fin
LogVol100	/	ext3	✓	6080		
▼ Discos duros						
▼ /dev/sda						
/dev/sda1	/boot	ext3	✓	102	1	13
/dev/sda2	VolGroup00	LVM PV	✓	8087	14	1044

Esconder el dispositivo RAID/los miembros del grupo de volumen LVM

[Notas de lanzamiento](#)
[← Atrás](#)
[→ Siguiente](#)



Se configura la tarjeta de red, para la máquina virtual con Linux, de forma estática (no por DHCP)



Luego se da un nombre al sistema y se definen los DNS.

RED HAT ENTERPRISE LINUX 5

Dispositivos de red

Activar al inicio	Dispositivo	IPv4/Máscara de red	IPv6/Prefijo
<input checked="" type="checkbox"/>	eth0	192.168.248.25/24	Desactivado

[Modificar](#)

Nombre del Host
Configurar el nombre del host:

de forma automática a través de DHCP

manualmente (ej. "mipc.dominio.com.ar")

Configuración miscelánea

Puerta de enlace:

DNS Primario:

DNS Secundario:

[Notas de lanzamiento](#) [← Atrás](#) [→ Siguiente](#)

Se define una clave para el usuario root (para este caso root2009)

RED HAT ENTERPRISE LINUX 5

La cuenta root se utiliza para la administración del sistema. Introduzca una contraseña para el usuario root.

Contraseña de root:

Confirmar:

[Notas de lanzamiento](#) [← Atrás](#) [→ Siguiente](#)

Personalizar instalación de software (aquí es clave escoger todos los paquetes de software requeridos para las prácticas). Por lo tanto se indica que personalizar ahora.

RED HAT ENTERPRISE LINUX 5

The default installation of Red Hat Enterprise Linux Server includes a set of software applicable for general internet usage. What additional tasks would you like your system to include support for?

- Desarrollo de software
- Servidor de web

La selección de software se puede personalizar ahora o con el sistema de administración de software después de la instalación.

Personalizar luego Personalizar ahora

[Notas de lanzamiento](#) [Atrás](#) [Siguiete](#)

Aparecen a la izquierda grupos de paquetes y a la derecha se seleccionan los deseados dentro de de cada grupo:

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio

- Aplicaciones
- Desarrollo
- Servidores
- Sistema Base
- Idiomas

Entorno de escritorio de GNOME

KDE (K Desktop Environment)

KDE es una interfaz de usuario gráfica y potente que incluye un panel, un escritorio, iconos del sistema y un gestor gráfico de archivos.

seleccionados 6 de 7 paquetes opcionales

[Paquetes opcionales](#)

[Notas de lanzamiento](#) [Atrás](#) [Siguiete](#)

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio

- Aplicaciones
- Desarrollo**
- Servidores
- Sistema Base
- Idiomas

- Gráficos
- Ingeniería y científico
- Internet basada en texto
- Internet gráfica
- Juegos y entretenimiento
- Oficina/Productividad**
- Sonido y vídeo

Las aplicaciones incluyen los paquetes de ofimática, los visualizadores de PDF y mucho más.

seleccionados 1 de 2 paquetes opcionales

Paquetes opcionales

Notas de lanzamiento

Atrás Siguiete

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio

- Aplicaciones
- Desarrollo**
- Servidores
- Sistema Base
- Idiomas

- Bibliotecas de desarrollo
- Desarrollo de software anticuado
- Desarrollo de software de GNOME
- Desarrollo de software para KDE
- Desarrollo de software para X
- Desarrollo en Java
- Herramientas de desarrollo**

Estas herramientas incluyen las principales herramientas de desarrollo, como por ejemplo automake, gcc, perl, python y depuradores.

seleccionados 29 de 39 paquetes opcionales

Paquetes opcionales

Notas de lanzamiento

Atrás Siguiete

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio

Aplicaciones

Desarrollo

Servidores

Sistema Base

Idiomas

- Base de datos MySQL
- Base de datos PostgreSQL
- Herramientas de configuración d
- Servidor FTP
- Servidor Web
- Servidor de archivos Windows
- Servidor de correo


Estos paquetes le permiten configurar un servidor de correo IMAP o SMTP.

seleccionados 5 de 11 paquetes opcionales

Paquetes opcionales

 Notas de lanzamiento

 Atrás

 Siguiente

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio

Aplicaciones

Desarrollo

Servidores

Sistema Base


Idiomas

- Servidor de archivos Windows
- Servidor de correo
- Servidor de nombres DNS
- Servidor de noticias
- Servidores de red
- Servidores de red anticuados
- Soporte para la impresión


Estos paquetes incluyen servidores para antiguos protocolos de red, tales como rsh y telnet.

seleccionados 3 de 10 paquetes opcionales

Paquetes opcionales

 Notas de lanzamiento

 Atrás

 Siguiente

RED HAT ENTERPRISE LINUX 5

Entornos de escritorio
Aplicaciones
Desarrollo
Servidores
Sistema Base
Idiomas

- Base
- Herramientas de administración
- Herramientas del sistema
- Java
- Sistema X Window
- Soporte de red mediante discado
- Soporte para software anticuado

Soporte para software anticuado

seleccionados 3 de 10 paquetes opcionales

Paquetes opcionales

 [Notas de lanzamiento](#)

[← Atrás](#) [→ Siguiente](#)

RED HAT ENTERPRISE LINUX 5



Pulse en Siguiente para iniciar la instalación de Red Hat Enterprise Linux Server.

El registro completo de la instalación puede encontrarse en el archivo `'/root/install.log'` luego de reiniciar su sistema.

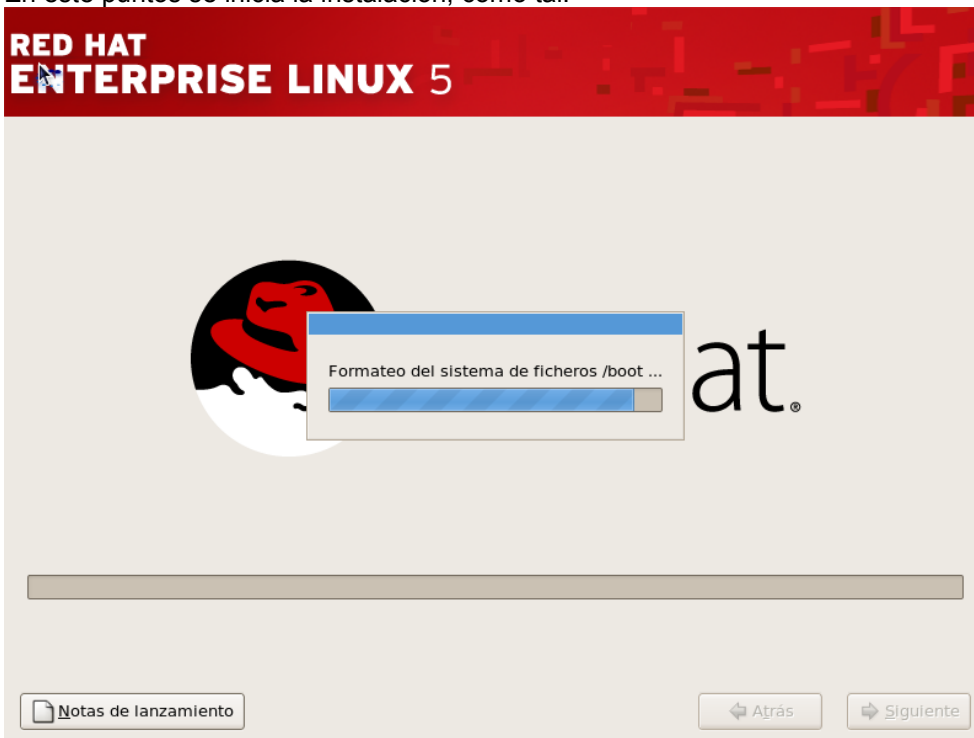
Podrá encontrar un archivo kickstart con las opciones de instalación seleccionadas en el archivo `'/root/anaconda-ks.cfg'` luego de reiniciar el sistema.

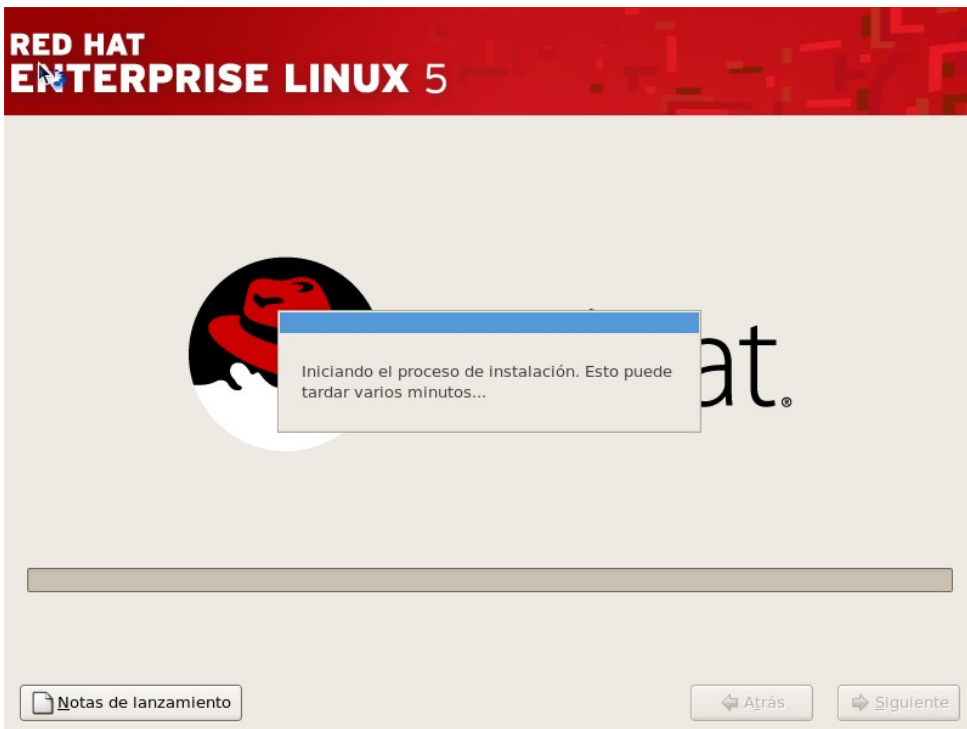
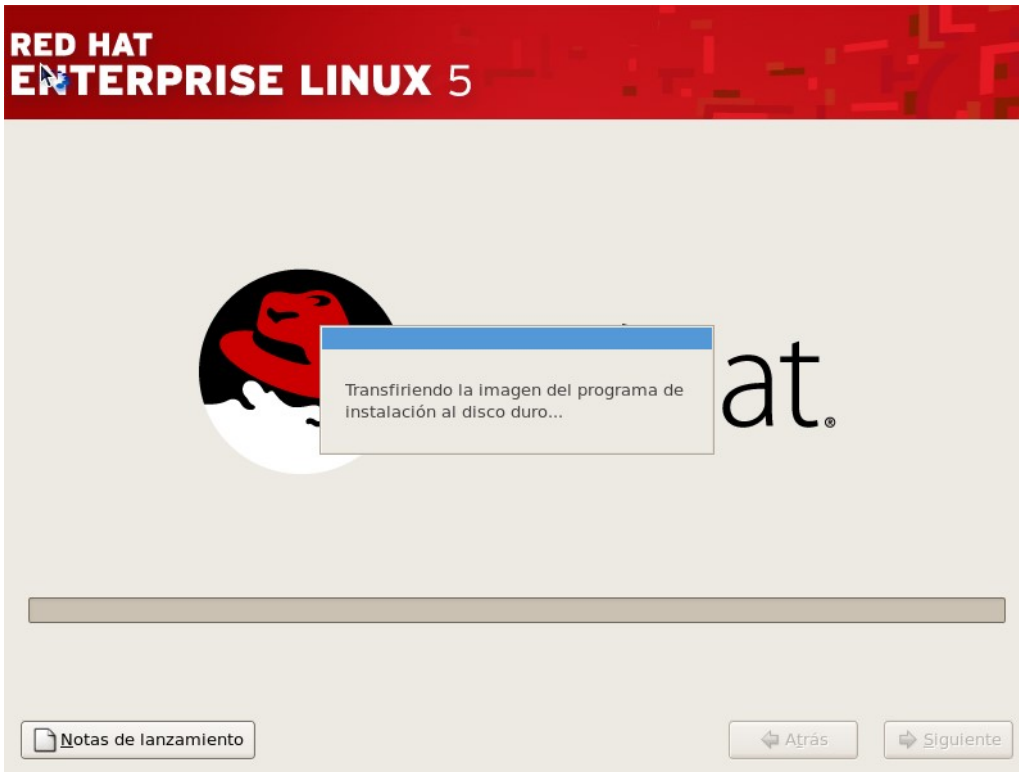
 [Notas de lanzamiento](#)

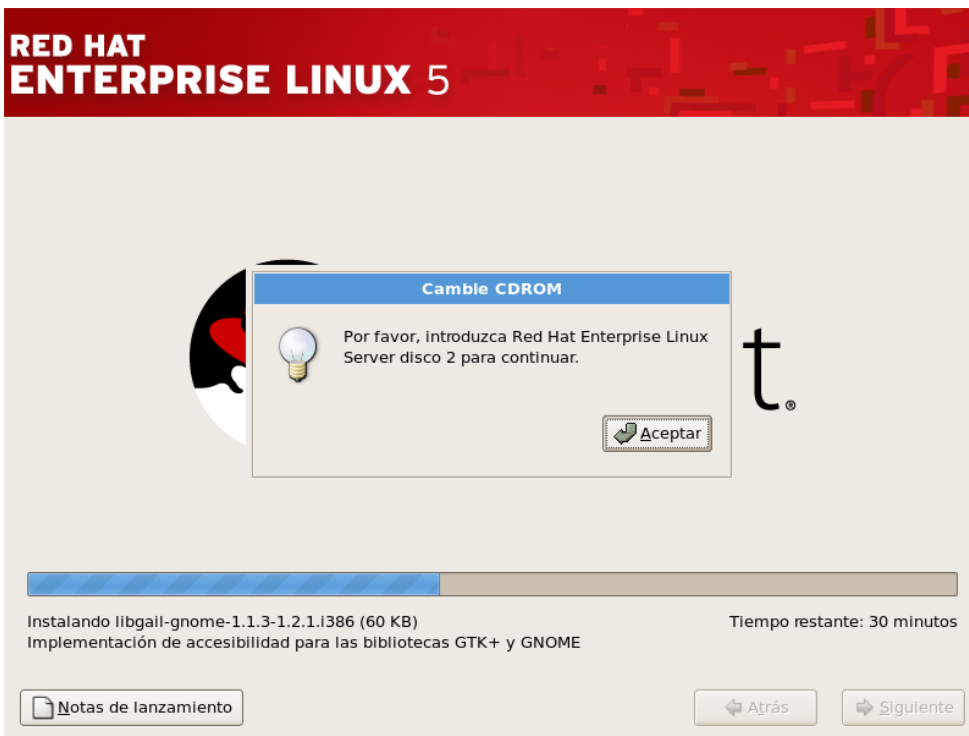
[← Atrás](#) [→ Siguiente](#)



En este puntos se inicia la instalación, como tal.







Y así. Continúa pidiendo los otros CDs.



Se reinicia

Press any key to enter the menu

Booting Red Hat Enterprise Linux Server (2.6.18-8.el5) in 1 seconds... █

The background of the boot screen is a solid red color with a complex, abstract pattern of white and dark red lines and shapes, resembling a stylized maze or circuitry. In the bottom left corner, the text "RED HAT ENTERPRISE LINUX 5" is displayed in white, bold, uppercase letters.

Se procede con unas tareas postinstalación:

> Bienvenido
 Acuerdo de Licencia
 Cortafuegos
 SELinux
 Kdump
 Fecha y Hora
 Configurando actualizaciones
 Crear Usuario
 Tarjeta de sonido
 CDs adicionales

Bienvenido

Hay algunos pasos más que debe realizar antes de que su sistema esté listo para ser utilizado. El Agente de configuración lo guiará a través de una configuración básica. Pulse "Adelante" en la esquina inferior derecha para continuar.

Atrás Adelante

Bienvenido
 > Acuerdo de Licencia
 Cortafuegos
 SELinux
 Kdump
 Fecha y Hora
 Configurando actualizaciones
 Crear Usuario
 Tarjeta de sonido
 CDs adicionales

Acuerdo de Licencia

ACUERDO DE LICENCIA PARA USUARIO FINAL RED HAT® ENTERPRISE LINUX® Y RED HAT A

Este acuerdo de licencia para usuario final ("EULA") rige el uso de todas las versiones de Red Hat Enterprise Linux, cualquier Aplicación de Red Hat (según se fija en www.redhat.com/licenses/products), y todas sus actualizaciones, código fuente, apariencia, estructura y organización (los "Programas"), cualquiera que sea la forma de entrega.

1. Concesión de la licencia. Sin perjuicio de lo dispuesto en las estipulaciones siguientes, Red Hat, Inc ("Red Hat") le otorga a usted ("Usuario") una licencia por plazo indefinido y de ámbito mundial para los Programas, de conformidad con la GNU General Public License v.2. Los Programas constituyen un sistema operativo integrado por módulos o una aplicación compuesta por ciertos componentes de software. Salvo ciertos archivos de imagen identificados en la Sección 2 siguiente, el acuerdo de licencia para cada componente de software está localizado en el código fuente del componente del software y permite al Usuario ejecutar, copiar, modificar y redistribuir (sujeto a ciertas obligaciones en algunos casos) el componente de software, tanto en código fuente como en código binario. Este EULA se refiere únicamente a los Programas y no limita los derechos del Usuario bajo los términos de la licencia, ni le otorga derechos que prevalezcan sobre los

Sí, acepto el Acuerdo de Licencia
 No, no estoy de acuerdo

Atrás Adelante

Para estas prácticas se va a desactivar el firewall, para garantizar que todos los servicios que se configuraran, puedan ser disponibles desde otras máquinas y desde el sistema Windows.

Bienvenido

Acuerdo de Licencia

▶ Cortafuegos

SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales





Cortafuegos

Puede usar el cortafuego para permitir el acceso a servicios específicos desde otros computadores hacia el suyo y prevenir accesos no autorizados desde el mundo exterior. ¿A qué servicios, si alguno, desea permitir el acceso?

Cortafuegos: Deshabilitado

Servicios confiables:

- Correo (SMTP)
- FTP
- NFS4
- SSH
- Samba
- Telnet

▶ Otros puertos

← Atrás
Adelante →

Bienvenido

Acuerdo de Licencia

Cortafuegos

▶ SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales





SELinux

Security Enhanced Linux (SELinux Linux con Seguridad Mejorada) provee un control de seguridad adicional al disponible en el tradicional sistema Linux. Puede ser configurado en estado inhabilitado, estado de sólo advertencias sobre lo que será negado, o un estado activo total. La mayoría conserva la configuración por defecto.

Configuración SELinux: Deshabilitado

← Atrás
Adelante →

Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales



SELinux

Security Enhanced Linux (SELinux Linux con Seguridad Mejorada) provee un control de seguridad adicional al disponible en el tradicional sistema Linux. Puede ser configurado en estado inhabilitado, estado de sólo advertencias sobre lo que será negado, o un estado activo total. La mayoría conserva la configuración por defecto.

Configuración SELinux Deshabilitado

 Cambiar esta configuración de SELinux requerirá reiniciar el sistema para que el sistema de archivos pueda ser reetiquetado. Reetiquetar toma mucho tiempo dependiendo del sistema de archivos. ¿Desea continuar con esta configuración y reiniciar el sistema despues que se complete el primer arranque?

No se escoge que se haga vaciado de memoria, en un crash (caída del sistema)

Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump


Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales



Kdump

Kdump is a kernel crash dumping mechanism. In the event of a system crash, kdump will capture information from your system that can be invaluable in determining the cause of the crash. Note that kdump does require reserving a portion of system memory that will be unavailable for other uses.

Enable kdump?

Total System Memory (MB): 1011

Kdump Memory (MB): 128

Usable System Memory (MB): 883

Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

➤ Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales





Fecha y Hora

Configure la fecha y la hora para el sistema.

Fecha y hora
Protocolo de Tiempo de Red (NTP)

Fecha

octubre
2009

lun	mar	mié	jue	vie	sáb	dom
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	8

Hora

Tiempo actual : 18:39:31

Hora :

Minuto :

Segundo :

← Atrás
→ Adelante

Como no se tiene la licencia de RedHat, se le indica que no busque actualizaciones.

Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

Fecha y Hora

➤ Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

CDs adicionales





Configurando actualizaciones

Este asistente lo guiará a través del proceso de registro de su sistema en la Red de Red Hat (RHN en inglés) para recibir actualizaciones de software, tales como:

- Su login de Red Hat Network o Red Hat Network Satellite
- Un nombre para el perfil Red Hat Network de su sistema
- La dirección de si Red Hat Network Satellite (opcional)

Si no tiene un login de Red Hat, este asistente le ayudará a crear uno.

¿Por qué me debo conectar a RHN? ...


¿Le gustaría registrar su sistema ahora?
(Altamente recomendado).


Sí, me gustaría registrarme ahora


No, prefiero registrarme posteriormente.


← Atrás
→ Adelante

¿Está seguro de no querer conectar su sistema con Red Hat Network? Perderá los beneficios de una suscripción de Red Hat Enterprise Linux:


Seguridad y actualizaciones:
 Reciba las últimas actualizaciones de software, incluyendo actualizaciones de seguridad, para mantener su sistema Red Hat Enterprise Linux **actualizado y seguro**.

Descargas y actualizaciones:
 Descargue las imágenes de instalación para Red Hat Enterprise Linux, incluyendo los nuevos lanzamientos.

Asistencia:
 Obtenga acceso a la asistencia técnica por parte de los expertos de Red Hat o de los socios de Red Hat para obtener ayuda con cualquier problema que pueda encontrar con este sistema.

Conformidad:
 Permanezca en conformidad con los acuerdos de suscripción y administre las suscripciones para los sistemas que se conectan a su cuenta en <http://rhn.redhat.com>.

Usted **no** podrá aprovechar las ventajas de los privilegios de esta suscripción si no conecta su sistema a Red Hat Network.



Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

▶ **Crear Usuario**

Tarjeta de sonido

CDs adicionales

Crear Usuario

Se recomienda que cree un nombre de usuario para uso normal (no administrativo) del sistema. Para crear un nombre de usuario del sistema, proporcione la información requerida a continuación.

Nombre de usuario:

Nombre completo:

Contraseña:

Confirmar contraseña:

Si necesita utilizar una autenticación de red tal como Kerberos o NIS, por favor pulse en el botón Utilizar conexión de red.



Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

Crear Usuario

▶ **Tarjeta de sonido**

CDs adicionales



Tarjeta de sonido

Se ha detectado un dispositivo de audio en su máquina.

Pulse el botón de reproducción para escuchar un sonido de prueba. Debería oír una serie de tres sonidos. El primero estará en el canal de la derecha, el segundo en el izquierdo y el tercero en el canal del centro.

Se detectó el siguiente dispositivo de audio.

Placa seleccionada

Fabricante: Ensoniq

Modelo: ES1371 [AudioPCI-97]

Módulo: snd-ens1371

Prueba de Sonido

--- Detenido ---
 Repetir

Configuración de Volumen

Configuración de Dispositivo

Dispositivo PCM ES1371 DAC2/ADC ▾

Bienvenido

Acuerdo de Licencia

Cortafuegos

SELinux

Kdump

Fecha y Hora

Configurando actualizaciones

Crear Usuario

Tarjeta de sonido

▶ **CDs adicionales**

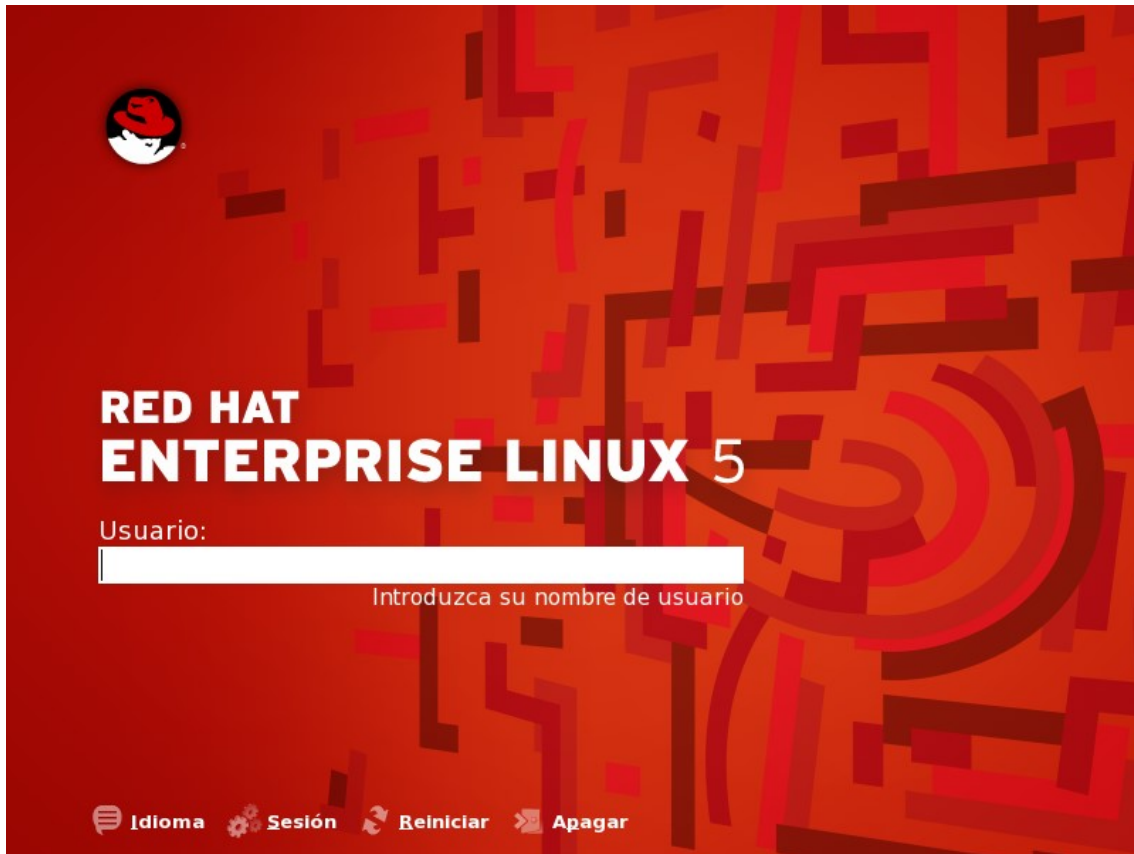


CDs adicionales

Por favor inserte cualquier cd de instalación de software adicional.

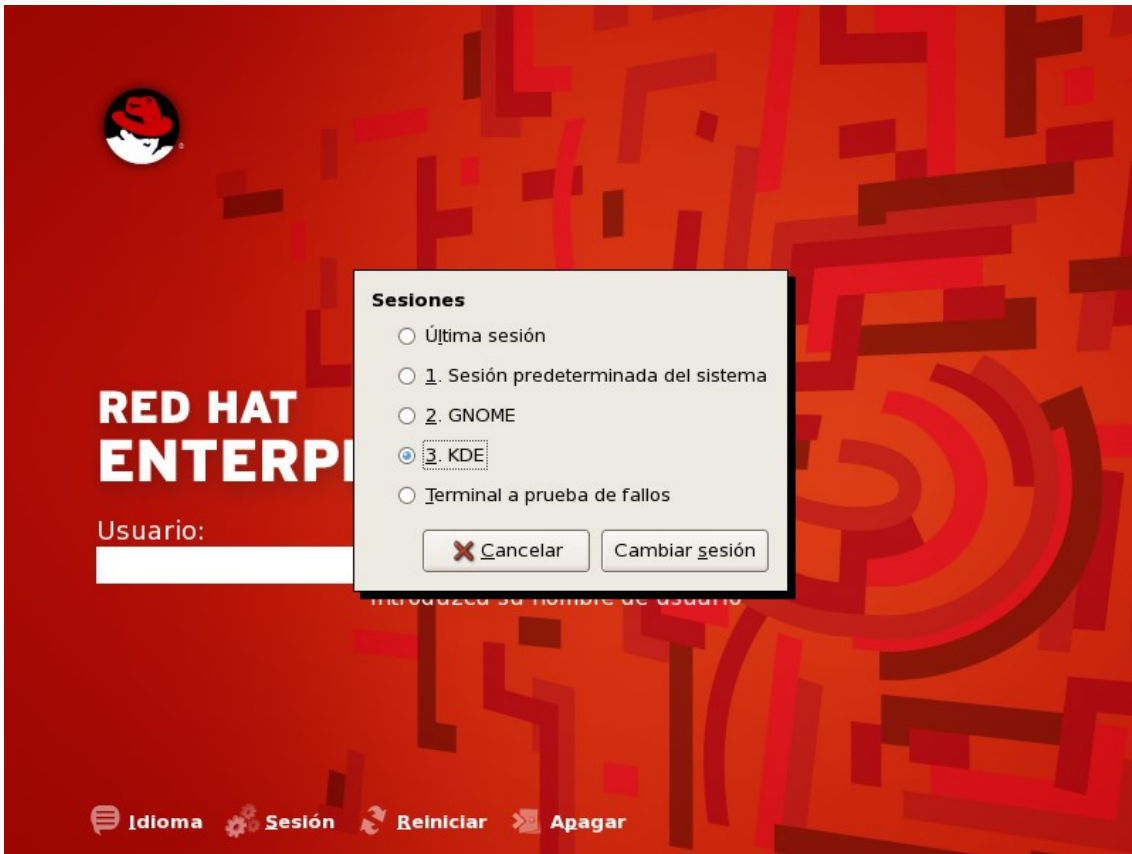

CDs adicionales

Y termina con un reinicio por que se desactivo el selinux

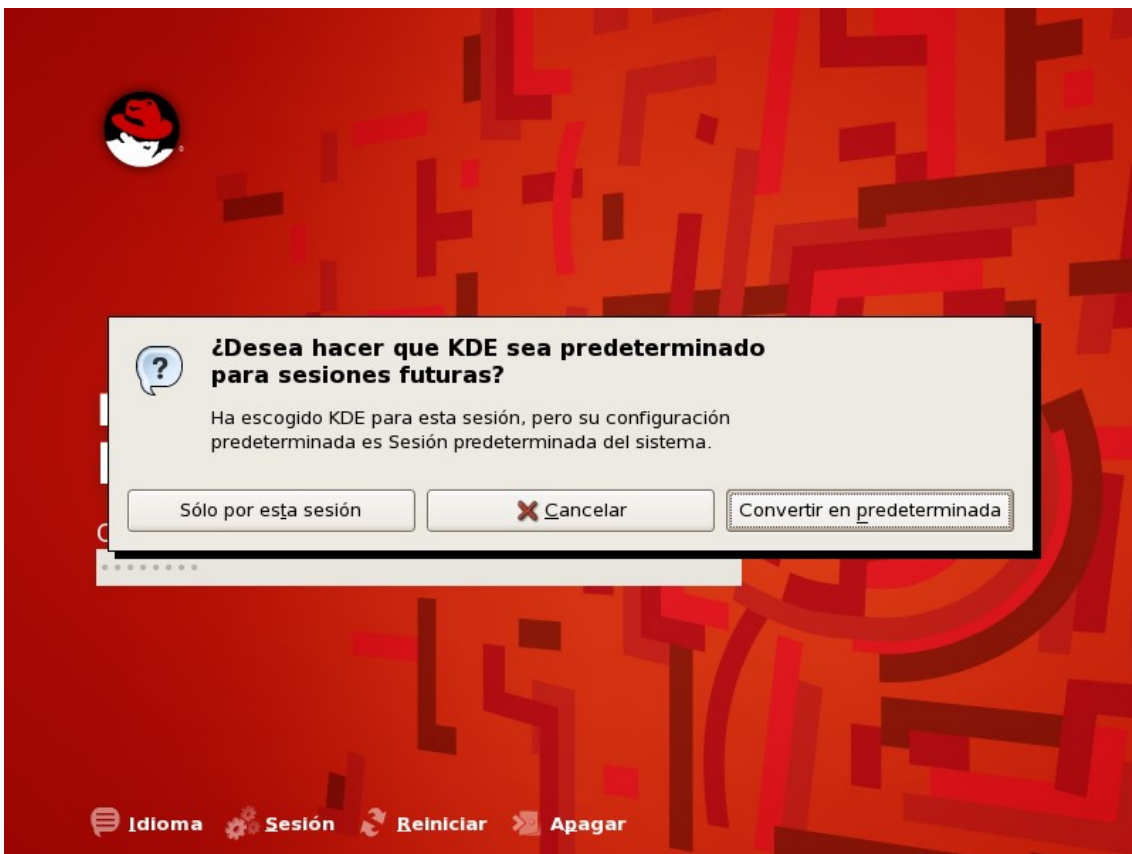


En este punto se culmina completamente la instalación. En la parte inferior de la ventana del VMWARE hay un botón que dice , I finish installing y se debe escoger. Se va a trabajar con sesión KDE y se debe proceder así

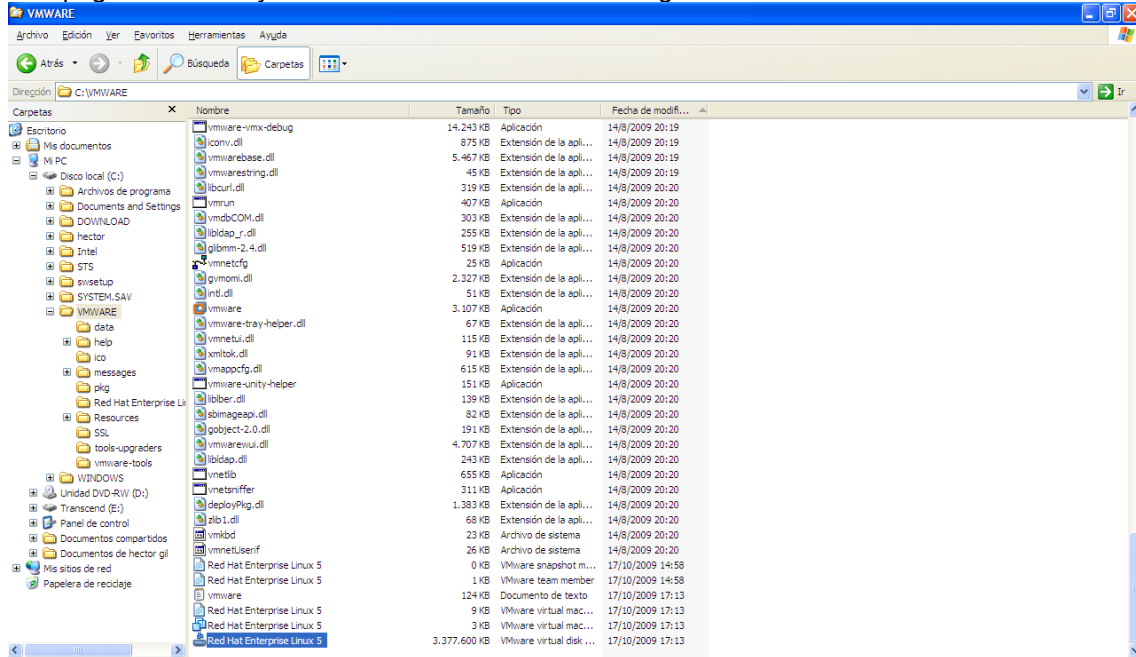
En la parte inferior Sesión escoger KDE



Y se procede a ingresar como root y la clave root2009. Se pregunta si la sesión KDE será a predeterminada



Se apaga el sistema y se observa el archivo con la imagen vmdk

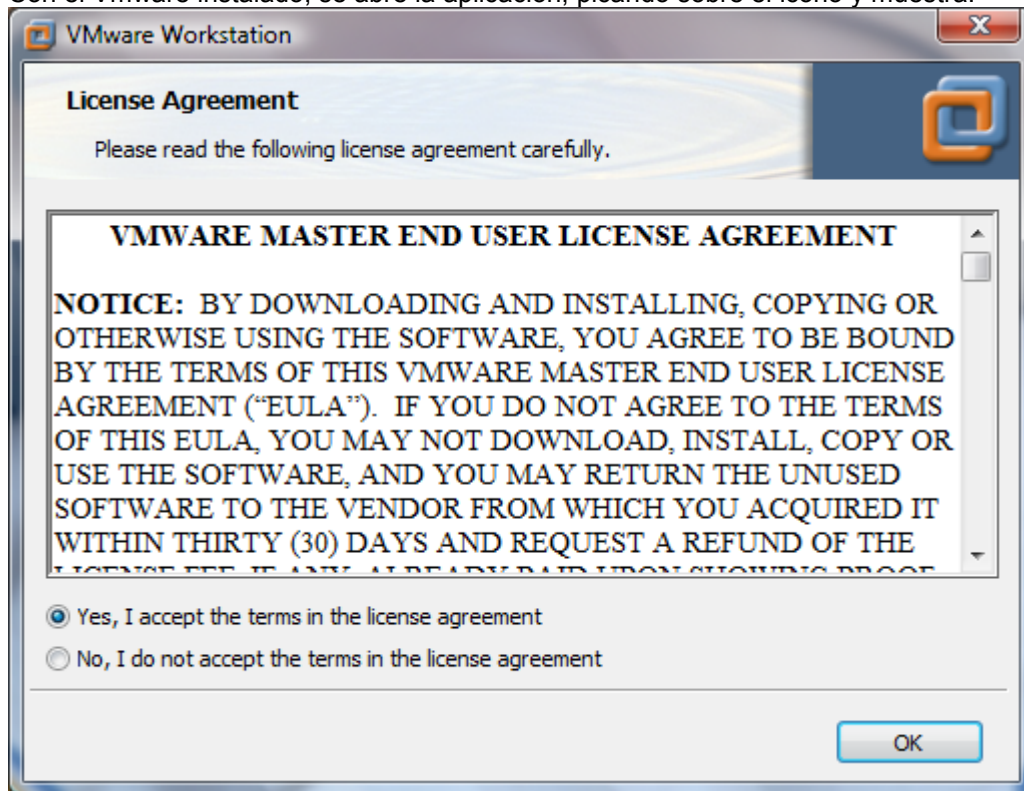


Esta imagen, puede ahora ser copiada a otros equipos que ya tengan instalado el producto VMWARE y quedan con el sistema Linux completamente instalado, como se detalla en la sección siguiente:

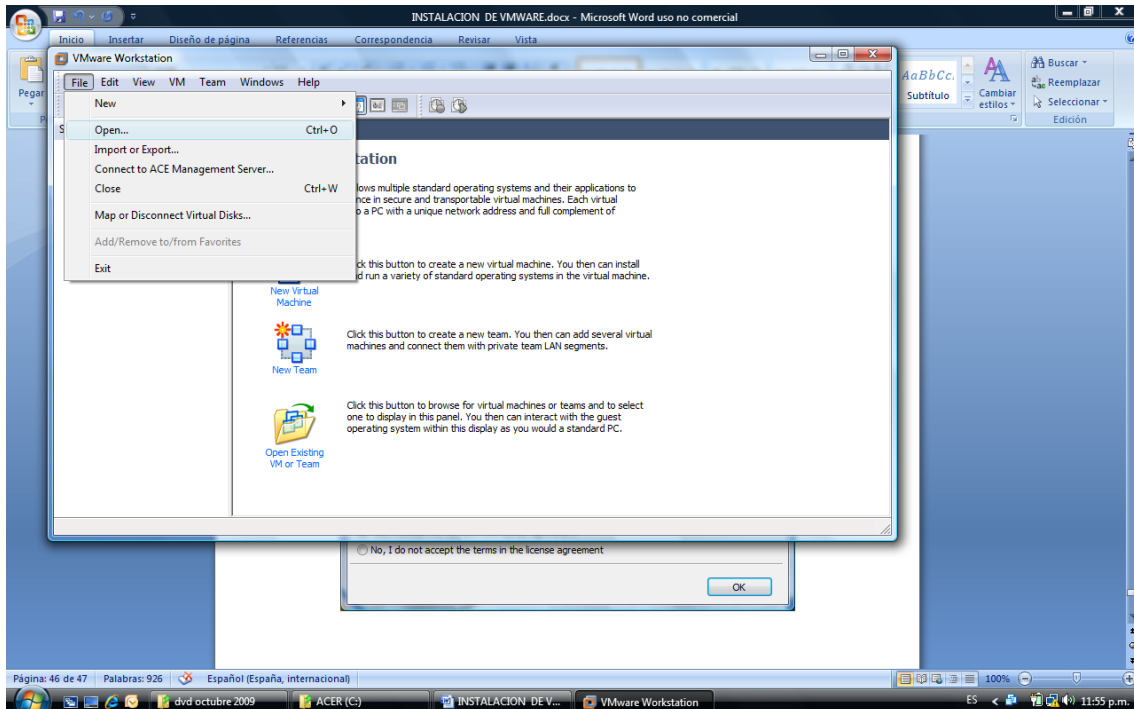
5.1.3.CARGUE DE UN SISTEMA OPERATIVO A PARTIR DE UNA IMAGEN

Si ya se cuenta con una imagen de una instalación completa de un sistema operativo, se puede cargar.

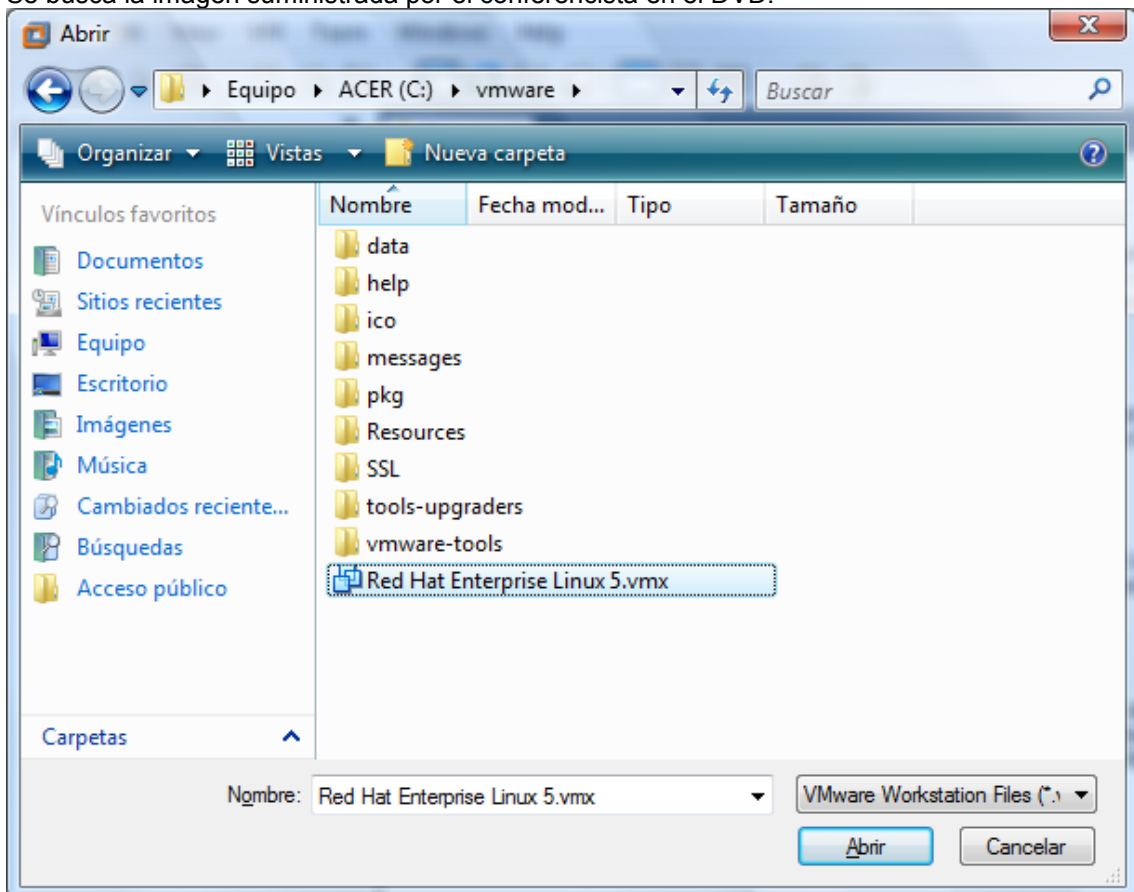
Con el Vmware instalado, se abre la aplicación, picando sobre el icono y muestra:



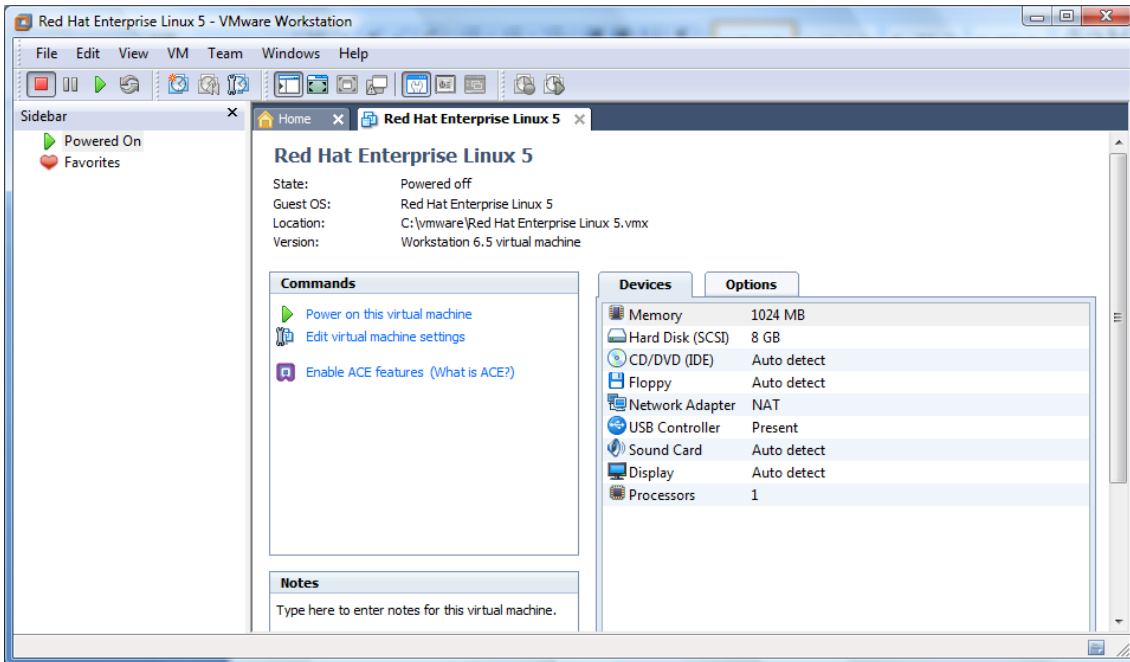
En la parte superior, se escoge File y luego Open:



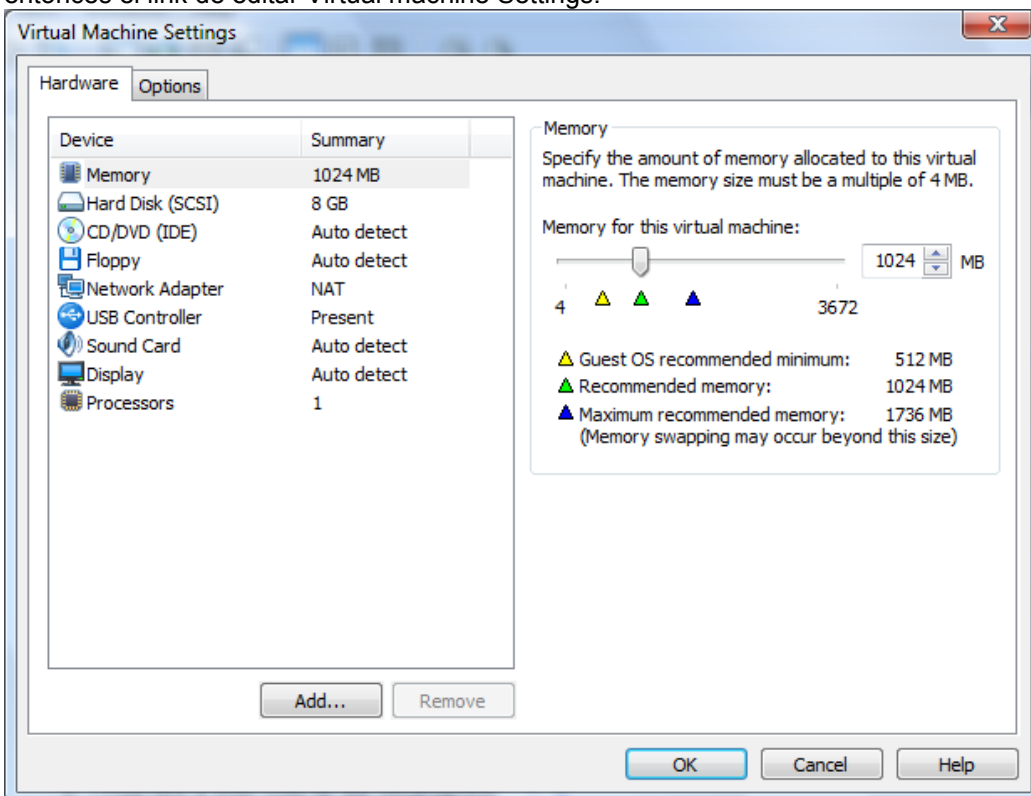
Se busca la imagen suministrada por el conferencista en el DVD.



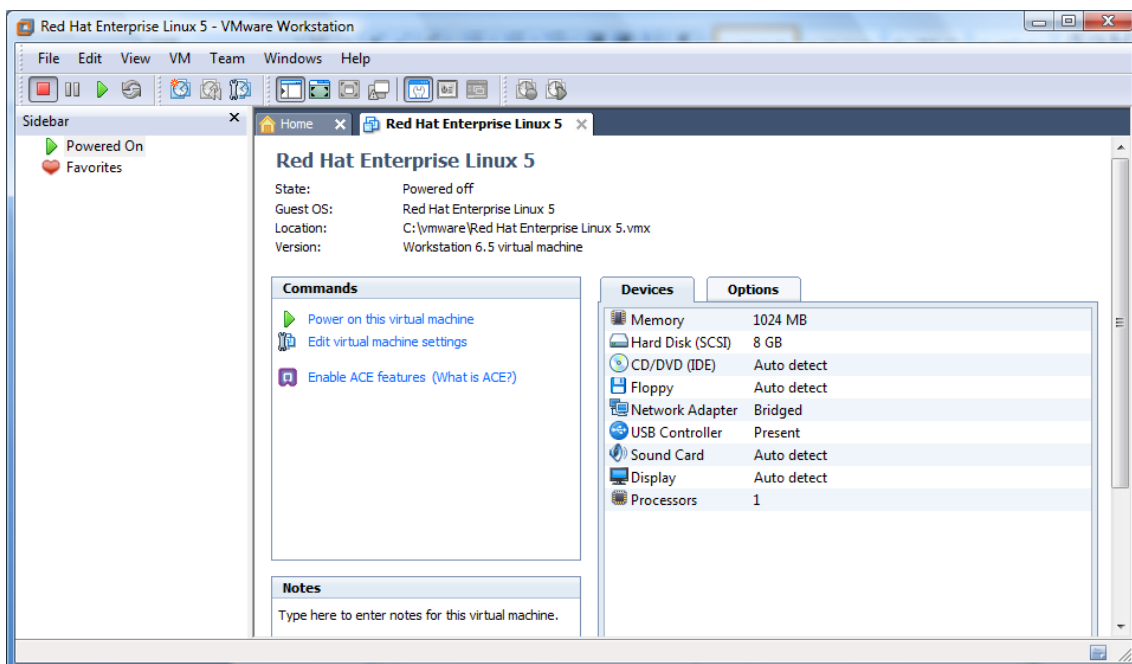
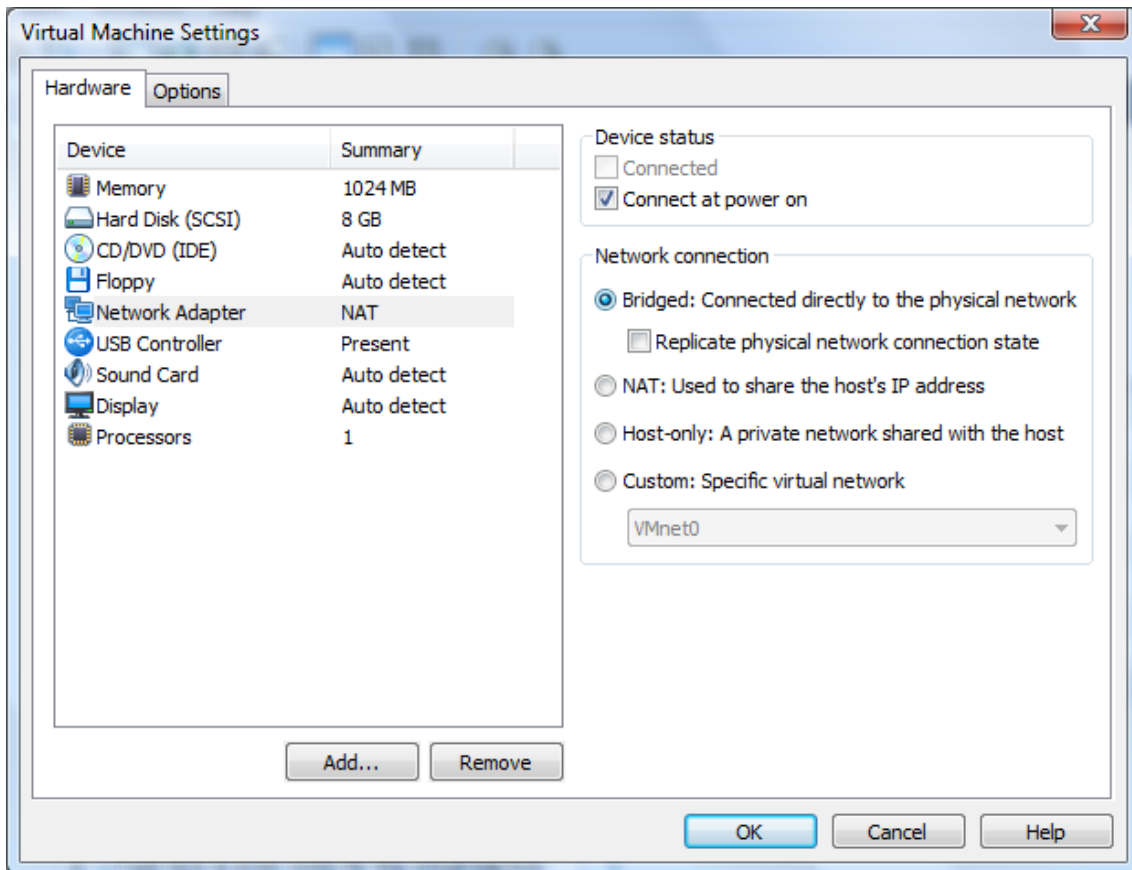
Y se procede a indicarle que abra. Debe mostrar ahora la información de esta imagen:



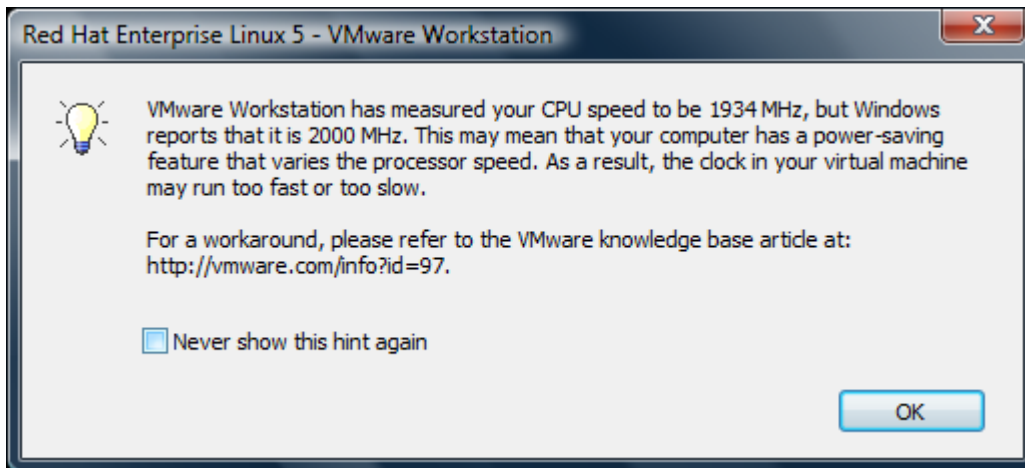
Si se desea hacer un cambio en la forma de trabajo de la tarjeta de red, se debe proceder antes de arrancar la máquina virtual. Por ejemplo se va a trabajar en modo bridge. Se escoge entonces el link de editar Virtual machine Settings.



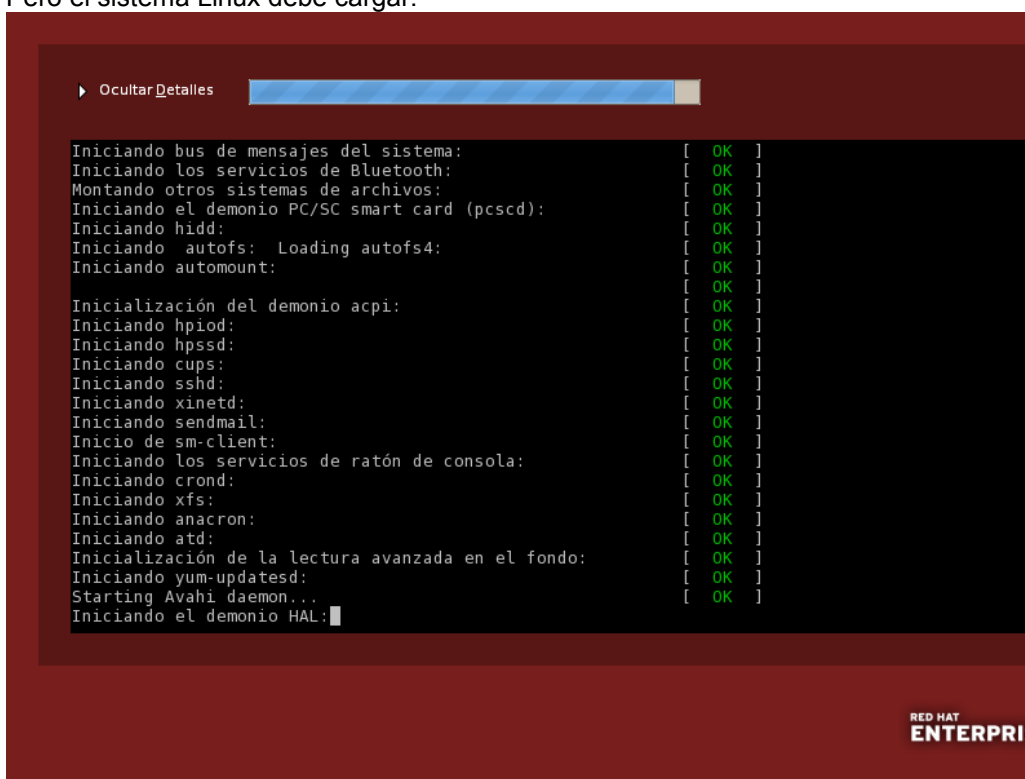
Se escoge Network Adapter (que actualmente esta en modo NAT). Se cambia a modo bridge.

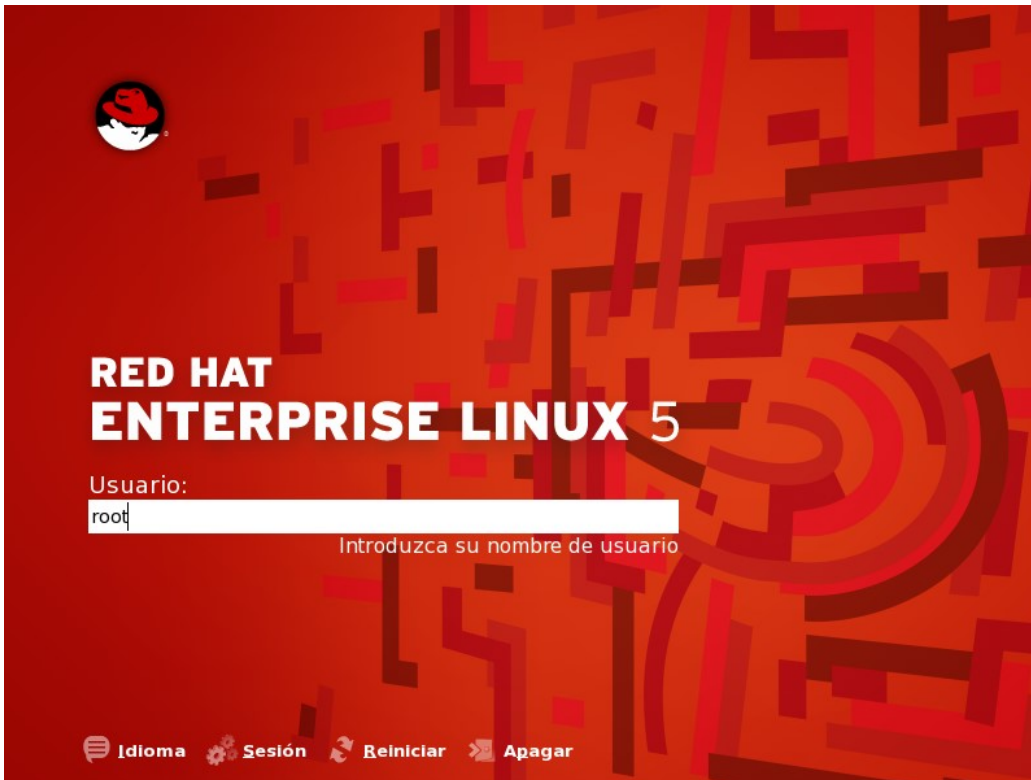


Se procede a subir la máquina virtual cargada (escogiendo power on). Puede salir una advertencia, que se indica no vuelva a mostrar.



De igual forma si la imagen cargada de la máquina virtual fue creada en un equipo con algunas características de hardware diferentes, va a presentar una advertencia sobre esto. Pero el sistema Linux debe cargar.





Se ingresa en sesión modo KDE, con user root y clave root2009.

Para cambiar de la ventana del Vmware y las ventanas Windows se presiona CTRL y ALT.

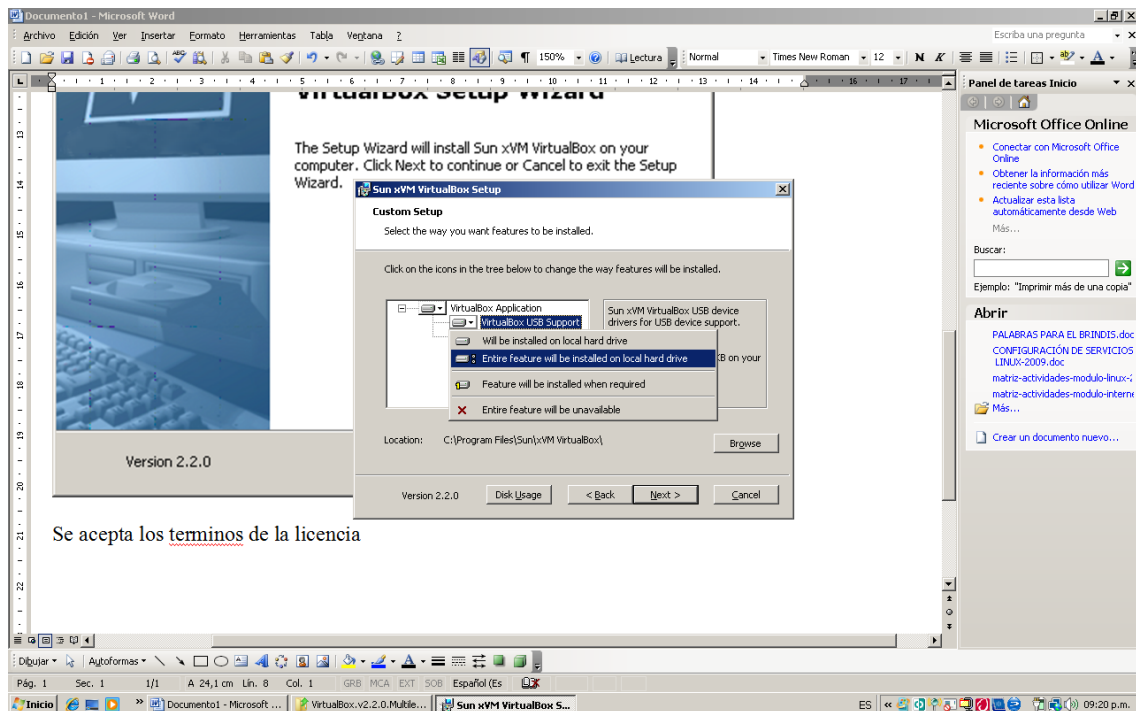
Se tiene ya la máquina virtual Linux, completamente instalada. Todos los cambios, configuraciones de Linux, etc que se hagan se ven reflejados en el archivo imagen de la máquina virtual, desde el sitio o carpeta de donde se cargo. Se puede copiar para llevar todo el sistema configurado.

5.2 VIRTUALIZACION CON VIRTUAL BOX

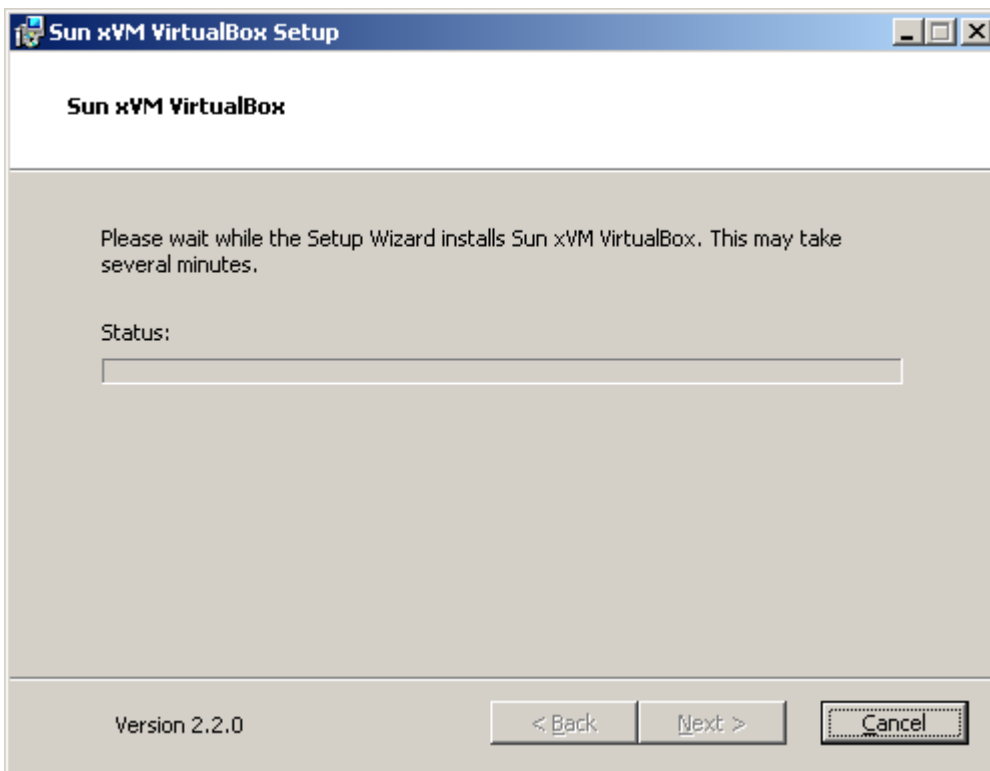
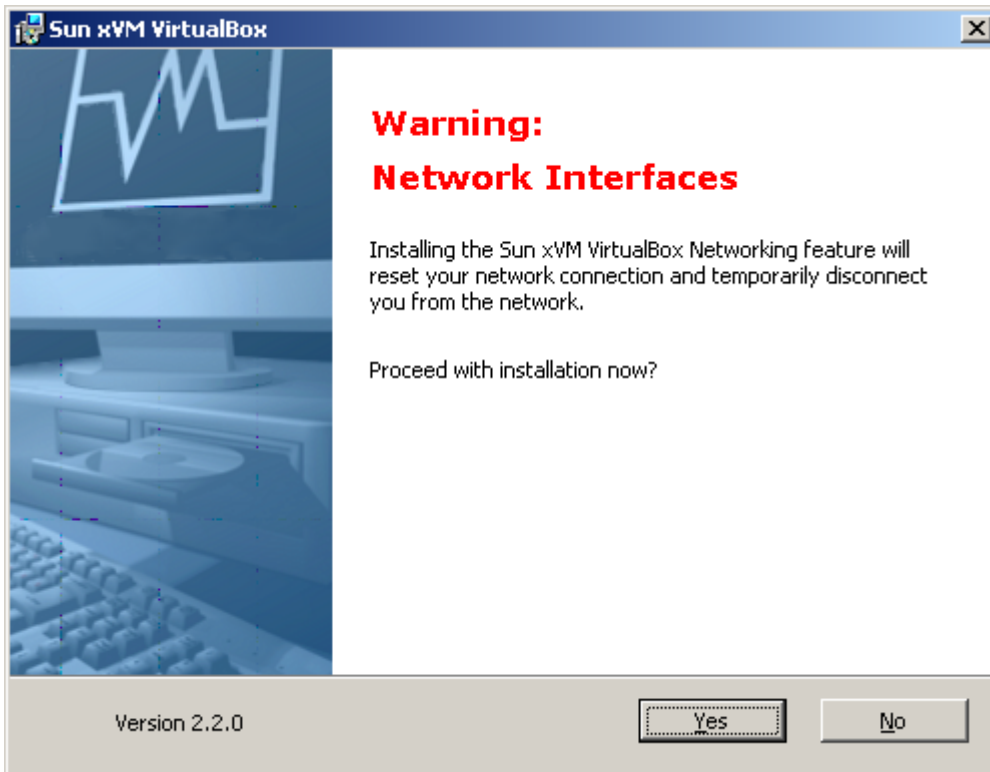
Con la herramienta Virtual Box (de SUN), se permitirá crear una máquina virtual en el PC, donde se realizará la instalación del sistema Linux. Así se tendrá los dos ambientes activos en el mismo equipo, y para cambiar de ambiente de trabajo, simplemente se procede a cambiar de ventana activa.

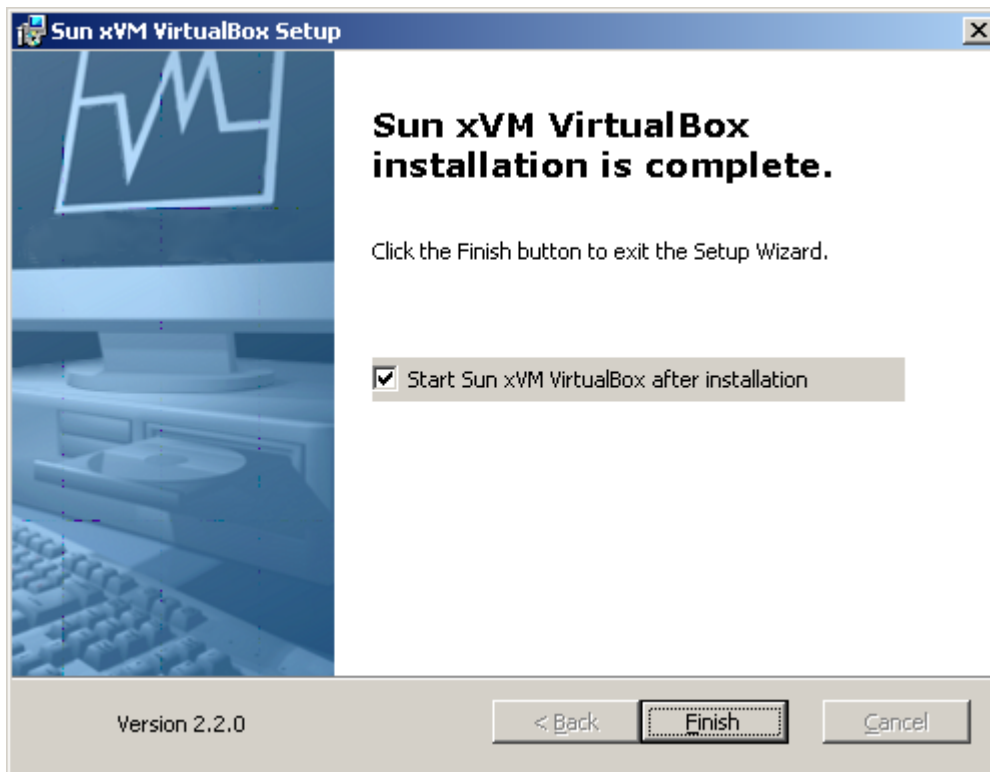


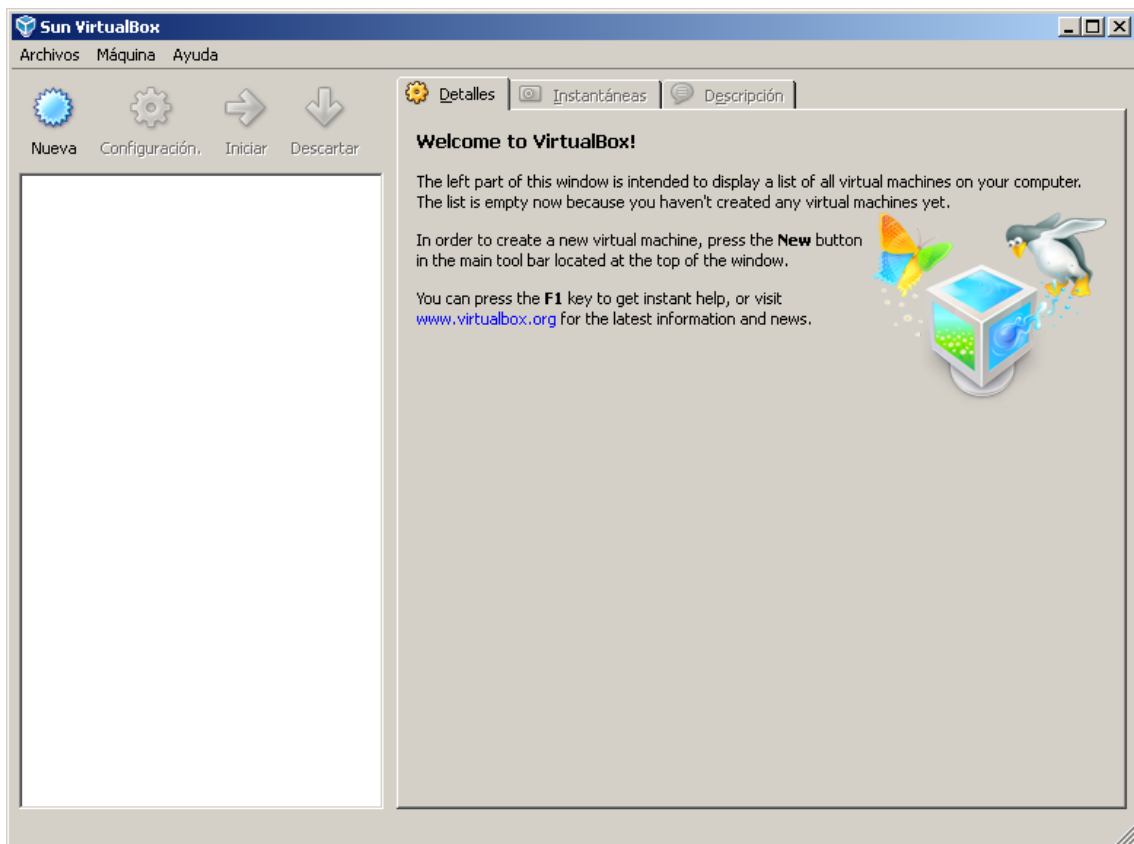
Se acepta los términos de la licencia



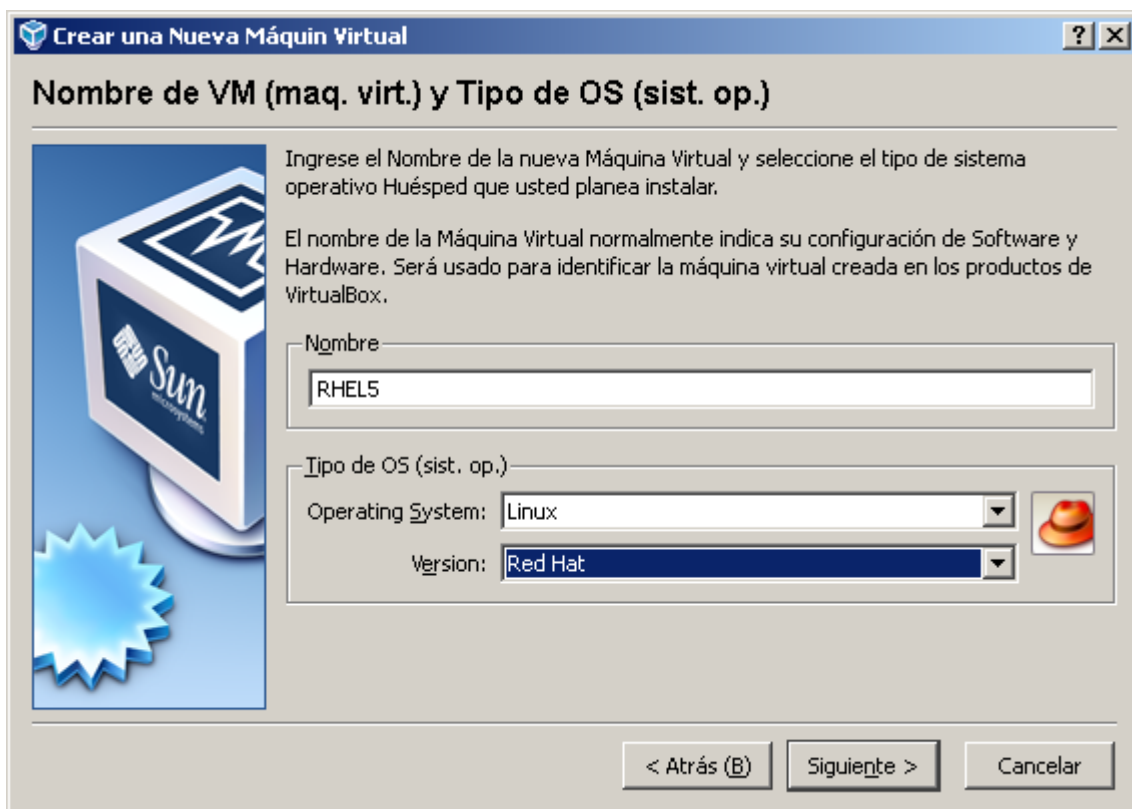
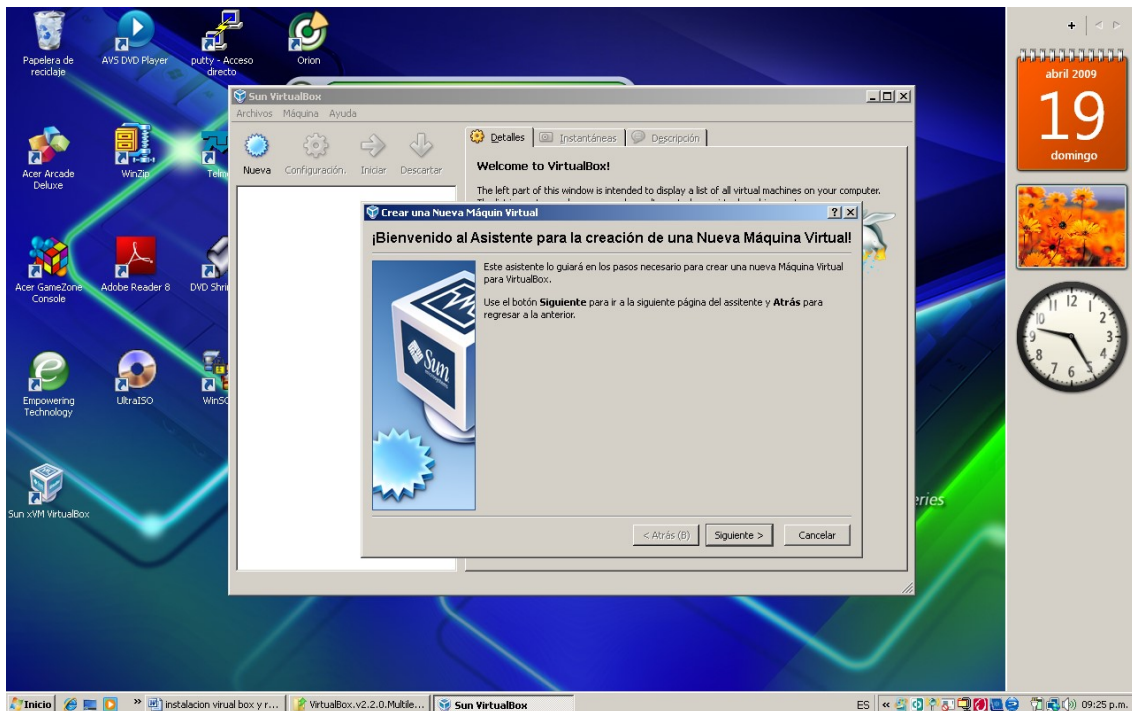
Se acepta los terminos de la licencia

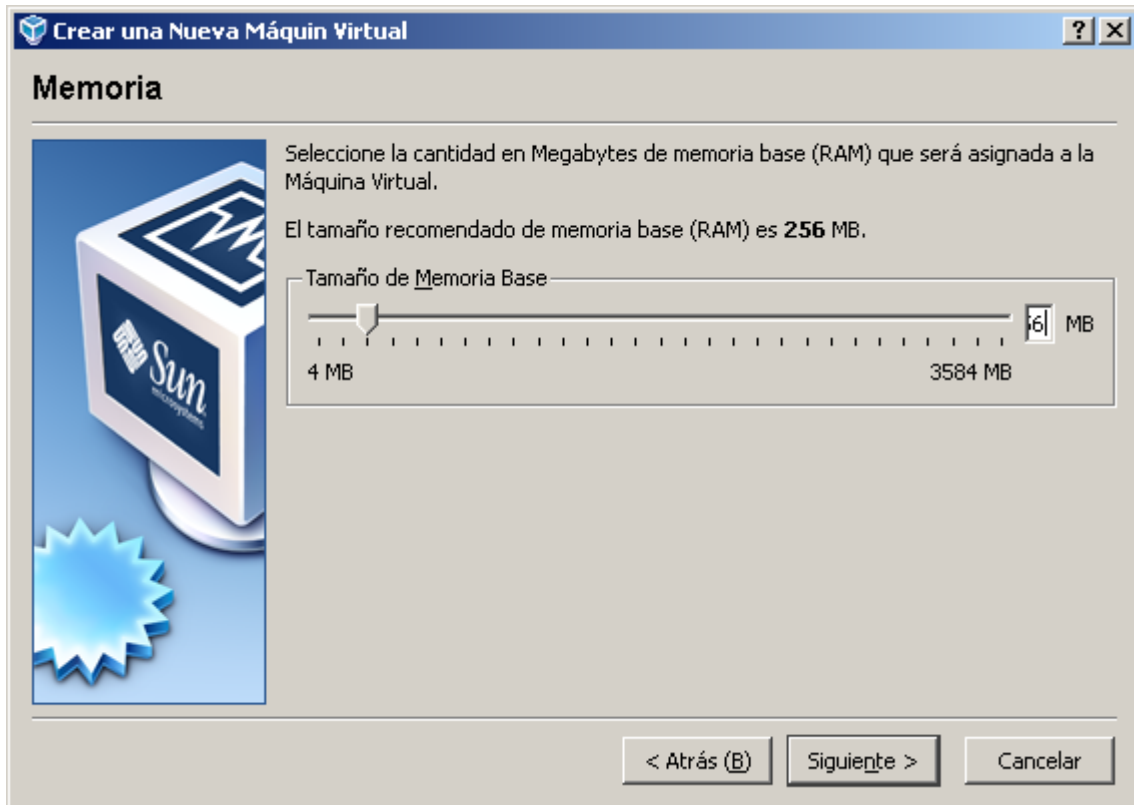


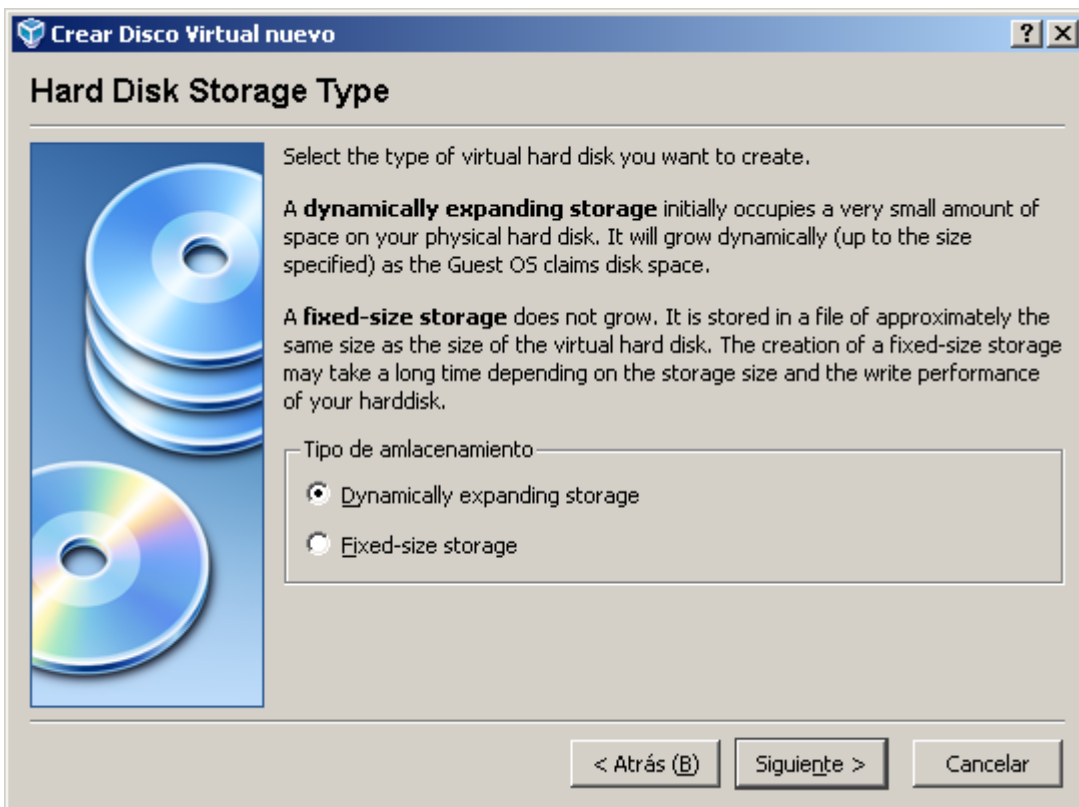
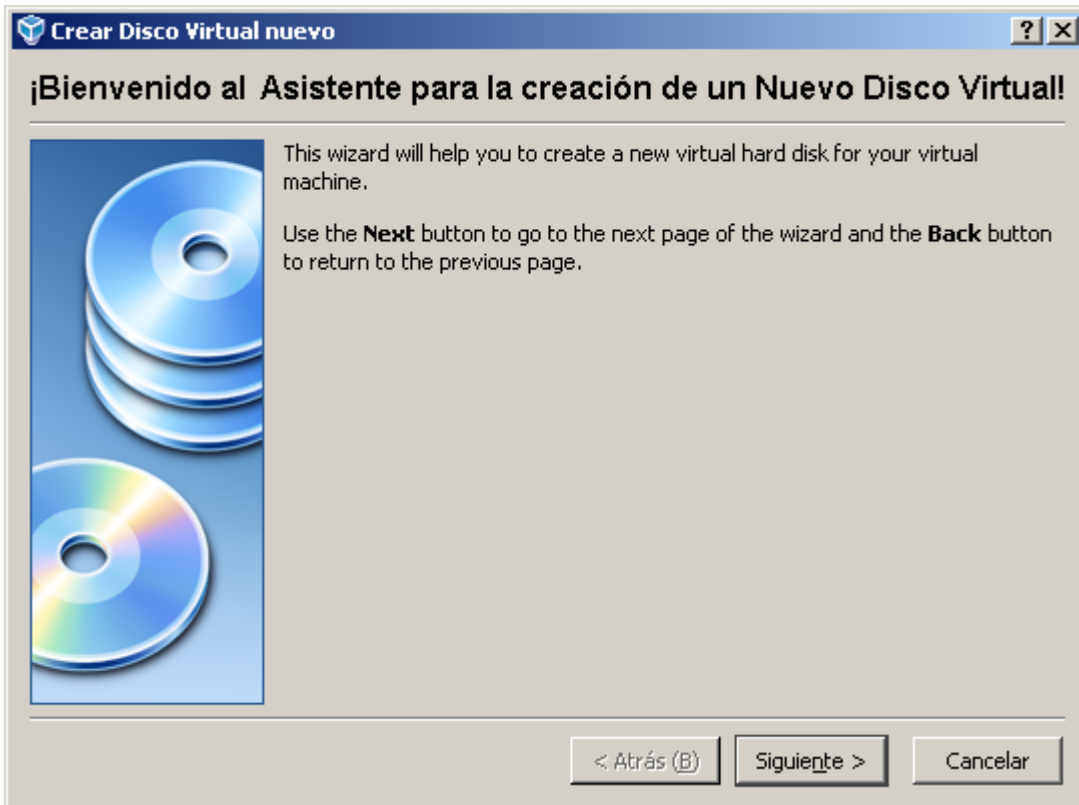


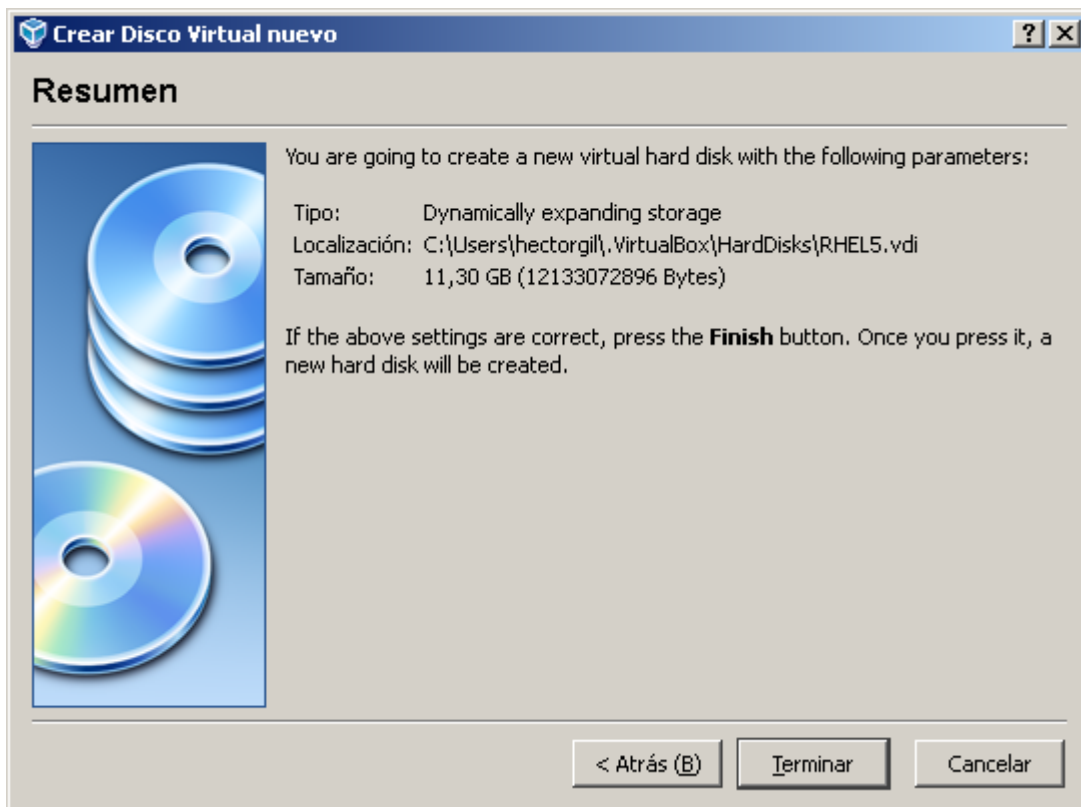
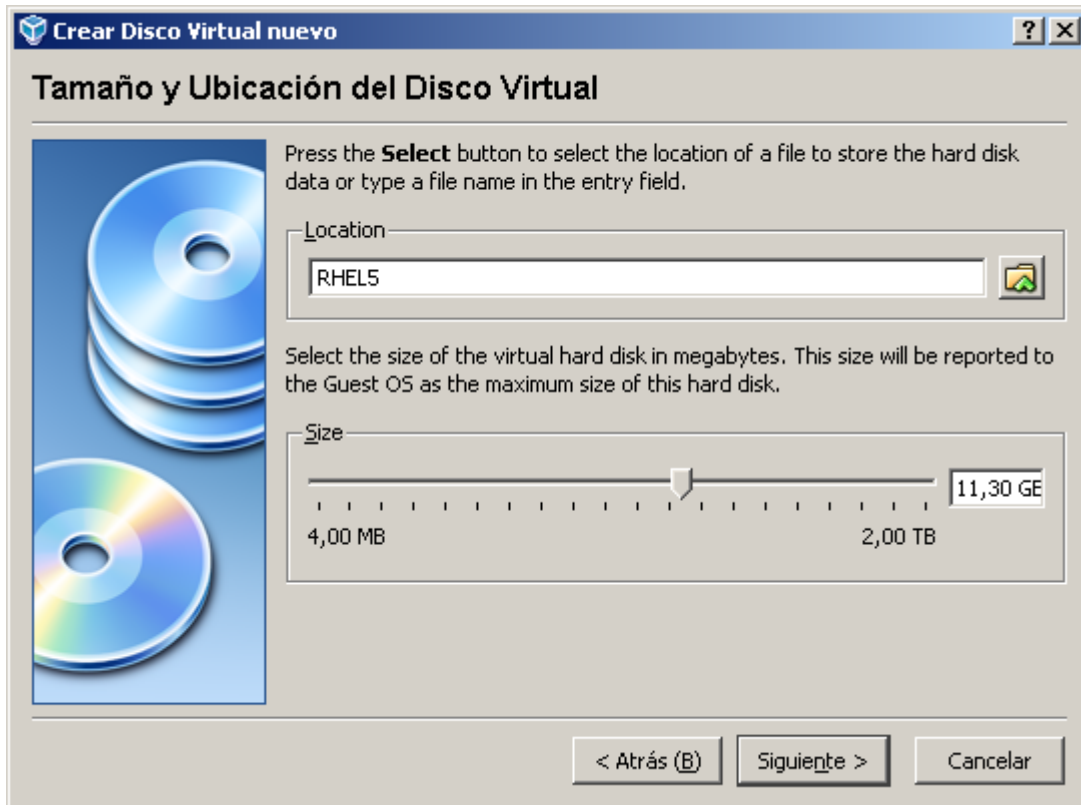


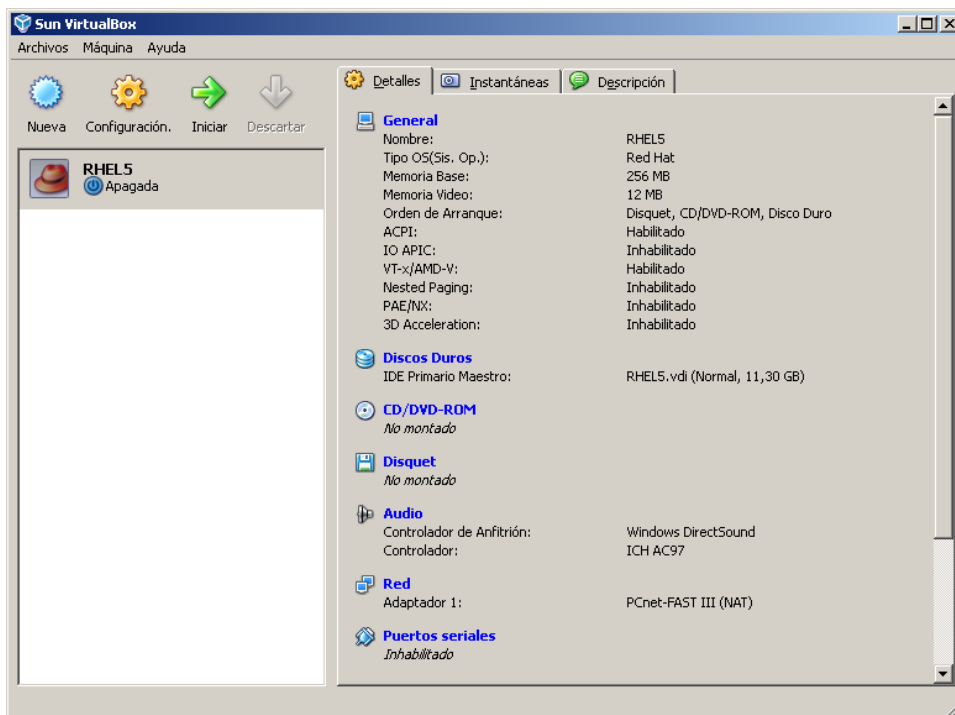
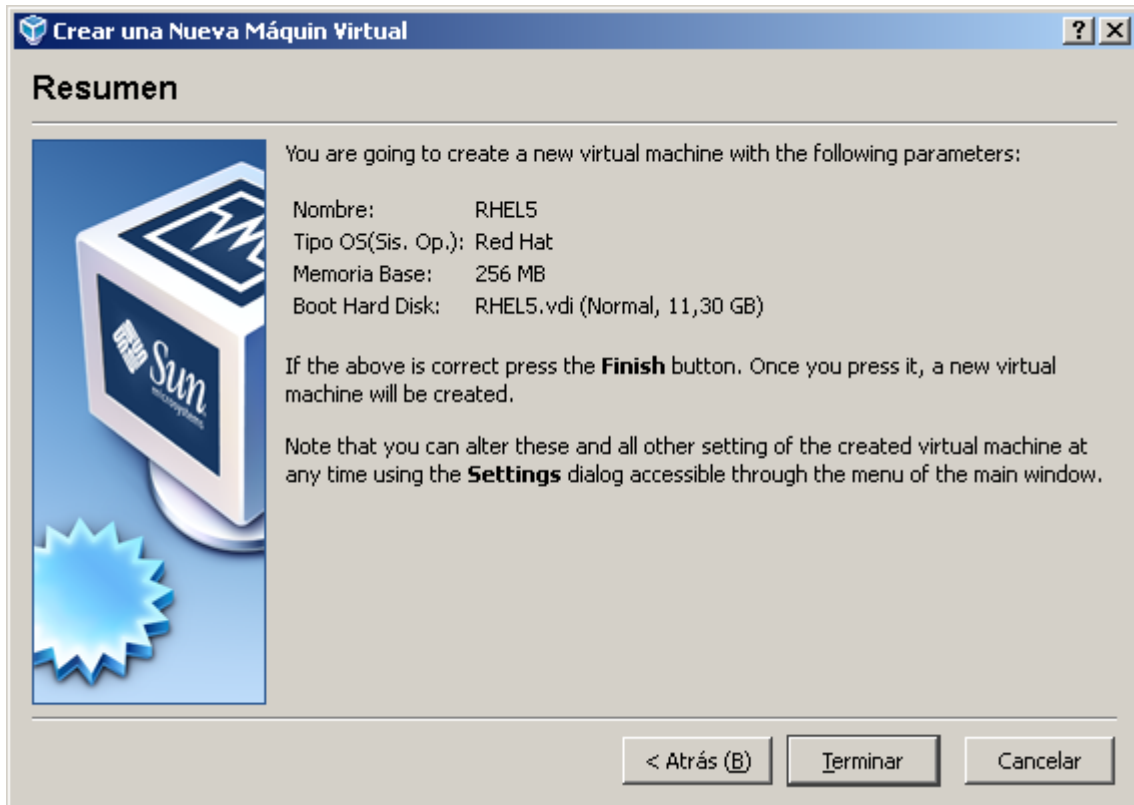
Se crea una nueva maquina virtual



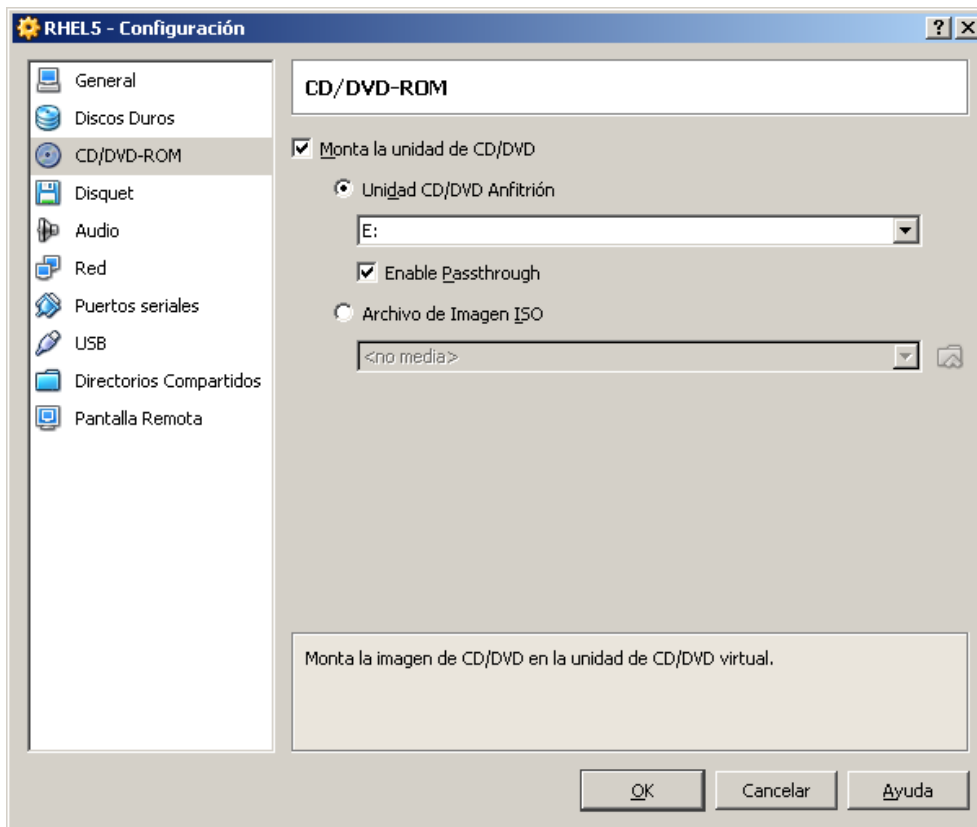




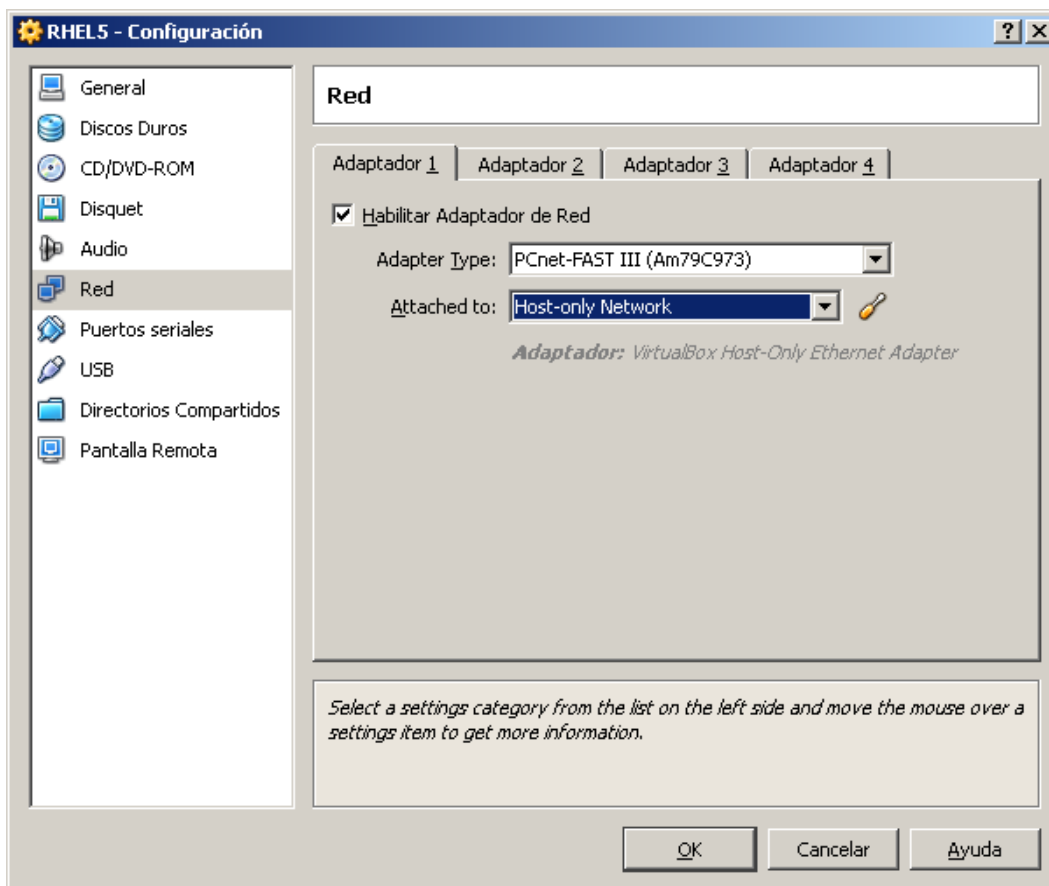




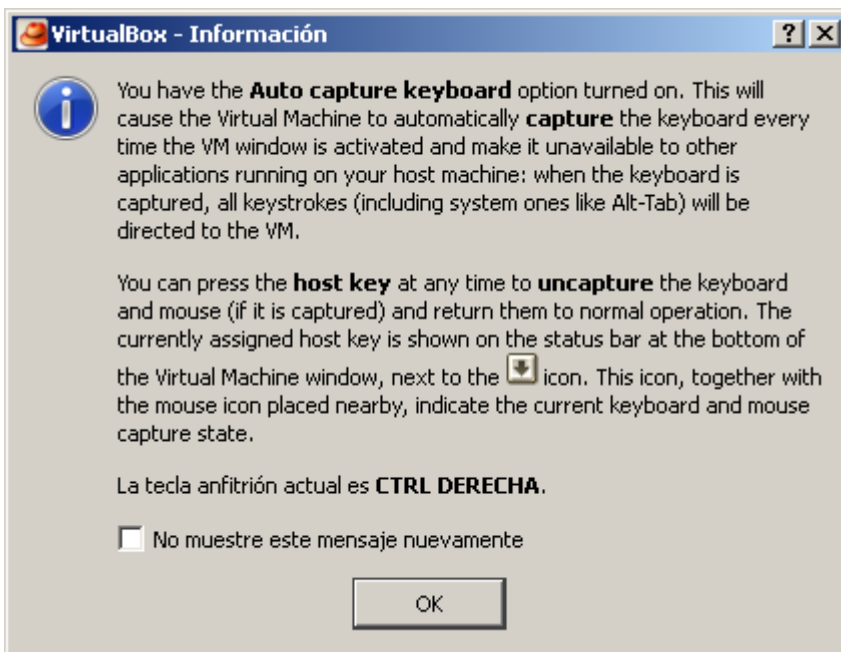
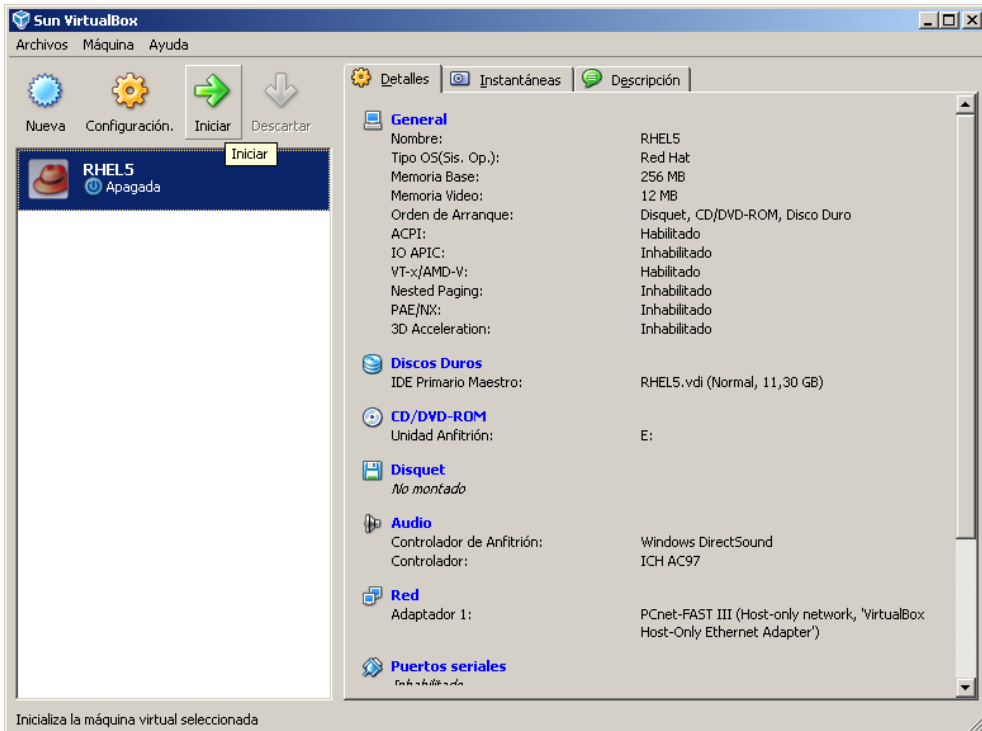
Se escoge la unidad DVD para que la monte



En red se cambio la definición del tipo de tarjeta a usar



Se inicia la maquina



Al dar OK, se muestra la ventana con el boot del equipo desde DVD de linux, normalmente como si fuese un equipo independiente y se procede con la instalación normal linux.

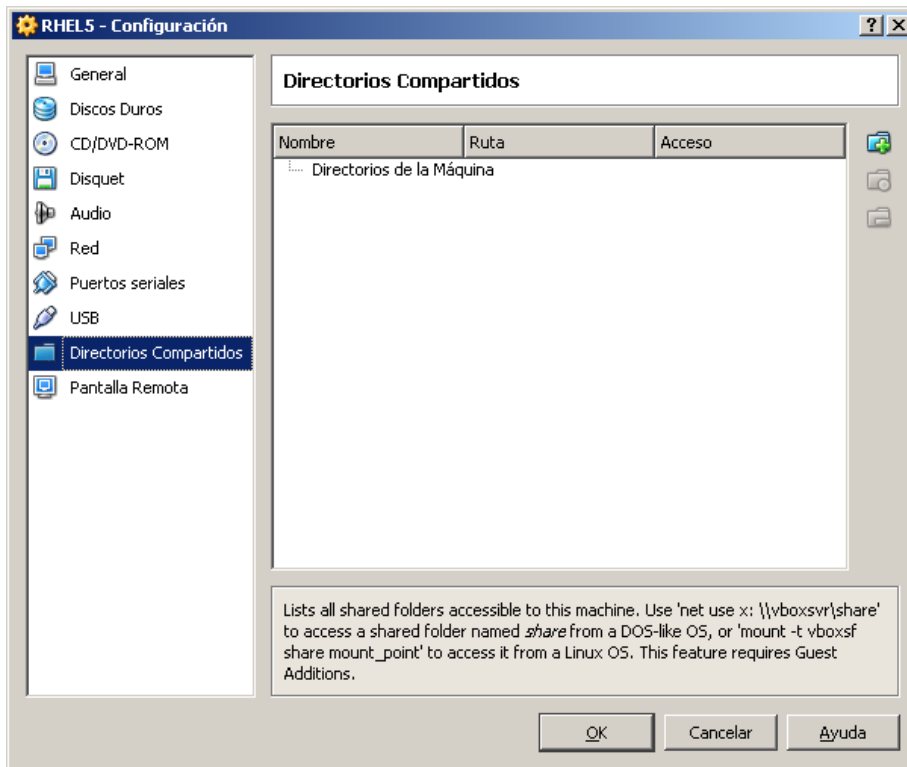
En la ventana de instalación linux, se escribe linux expert y se continua con el dialogo de instalación de linux normal

Esta instalación no se detalla aquí, y se puede observar en el documento realizado para trabajar con VMWARE.

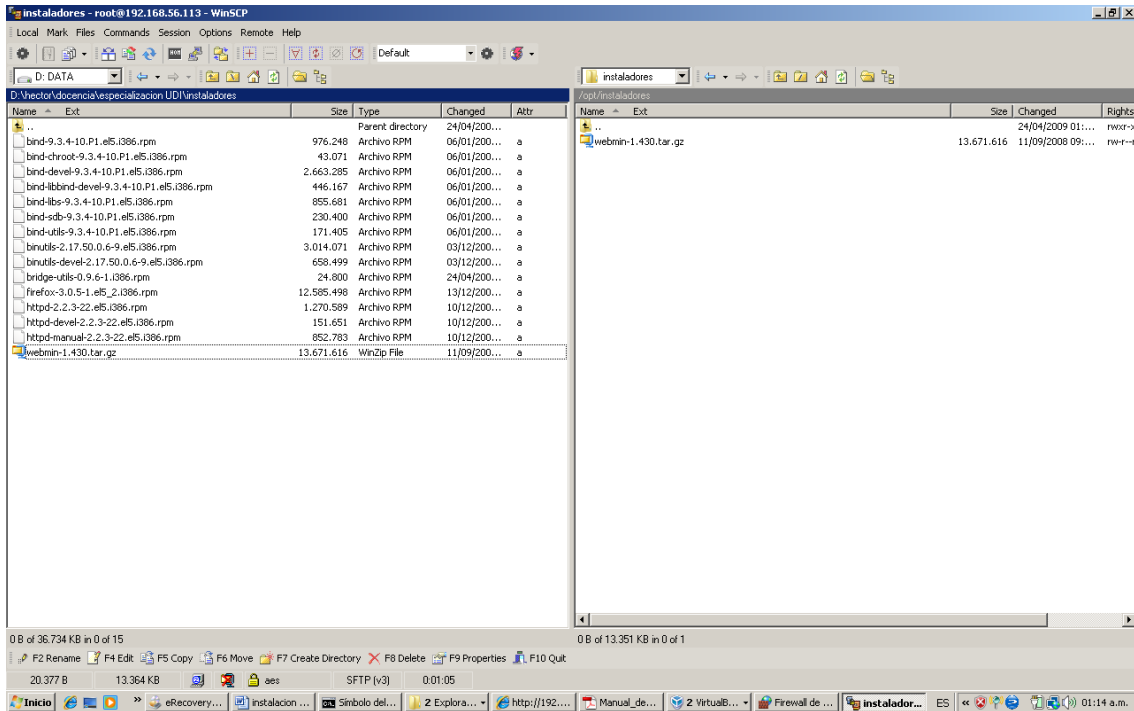
Cuando se ingresa a la máquina virtual , a trabajar el control de Mouse y teclado quedan en la ventana de virtual box, para pasar a Windows se usa la tecla CTRL del lado derecho del teclado, tal como lo advirtió el mensaje anterior.

Para montar el CD /DVD , de Windows en la máquina virtual, para este caso linux, si se configuró correctamente en el settings de virtual box, debe de detectarla automáticamente.

Para copiar archivos entre Windows y linux , previamente en los settings del virtual box hay que declarar la carpeta Windows que se usará con este fin.



Pero como este escenario no es tan frecuente, se procede a copiar mediante programas de transferencia de archivos como WinScp

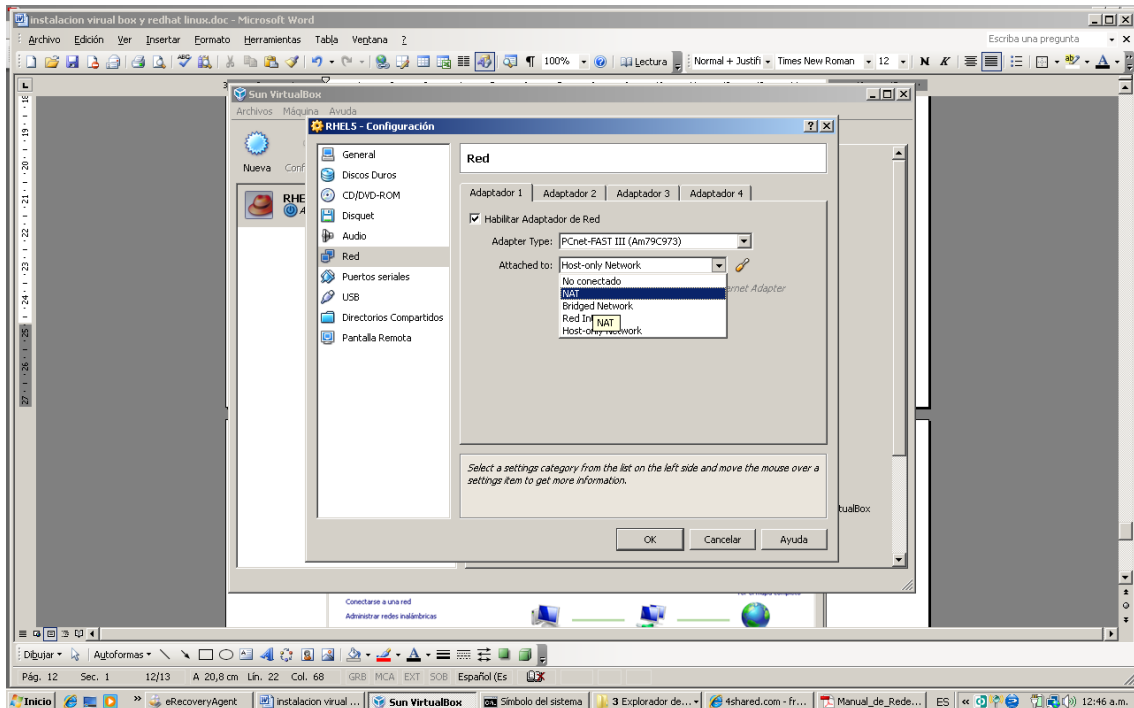


5.2.1.COMUNICACION ENTRE WINDOWS Y LINUX

Para conexión entre el sistema Anfitrión Windows (Host), y la máquina virtual huésped linux, existen alternativas, como las presentadas a continuación:

Se desea esbozar como es el comportamiento del host y de la máquina virtual, ante las tarjetas físicas y las virtuales.

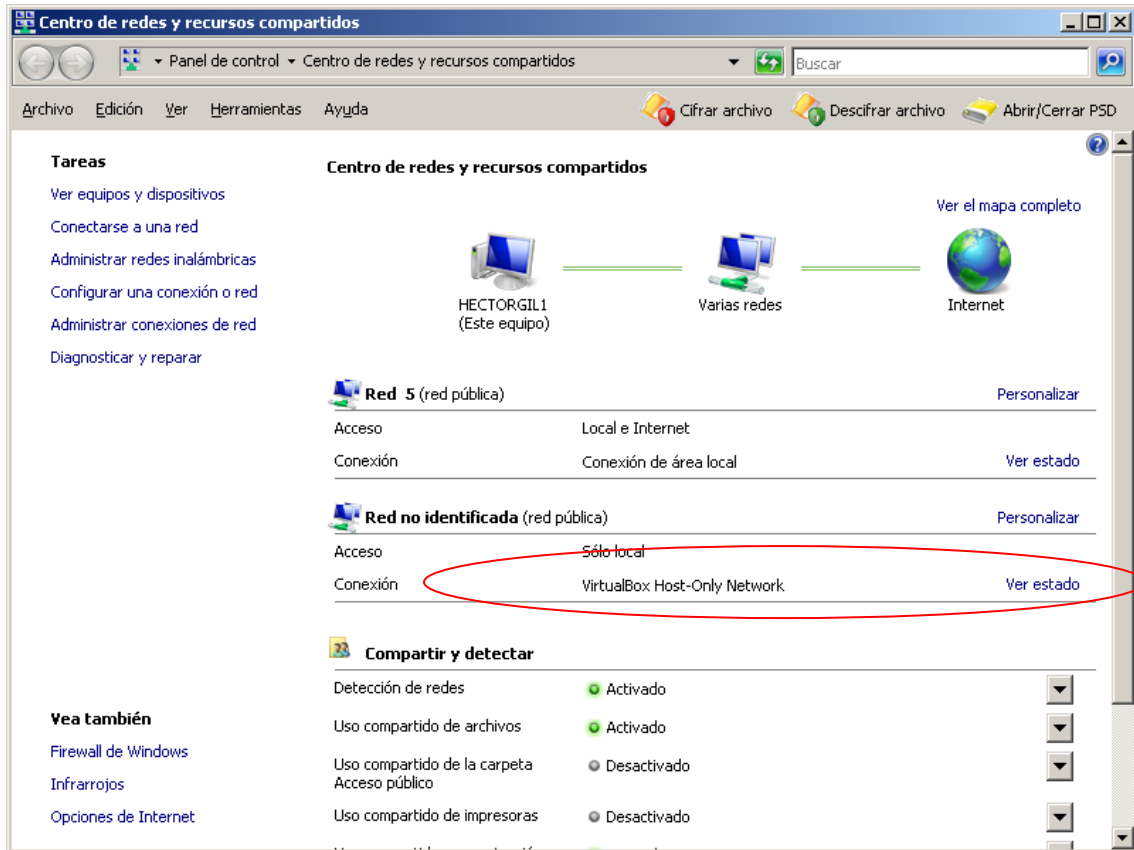
En la configuración de red del virtual box, se escoge el modo de trabajo de la tarjeta de red:



Por ejemplo si se desea que la máquina virtual tenga salida a Internet, se escoge modo NAT. Una vez en la máquina virtual se configura la tarjeta de red para que obtenga la IP de un servidor DHCP. Hay limitaciones en este modo.

Para que Windows vea linux (por ip) y viceversa, a nivel de tcp/ip, escoger en el modo de red del virtual box, host Only. (pero no se ven los demás equipos del laboratorio)

En la configuración de red de Windows, se tuvo que haber creado con la instalación del virtual box un interface virtual:



En esa tarjeta virtual, se asigna la IP de la misma red que la definida en la máquina virtual creada.

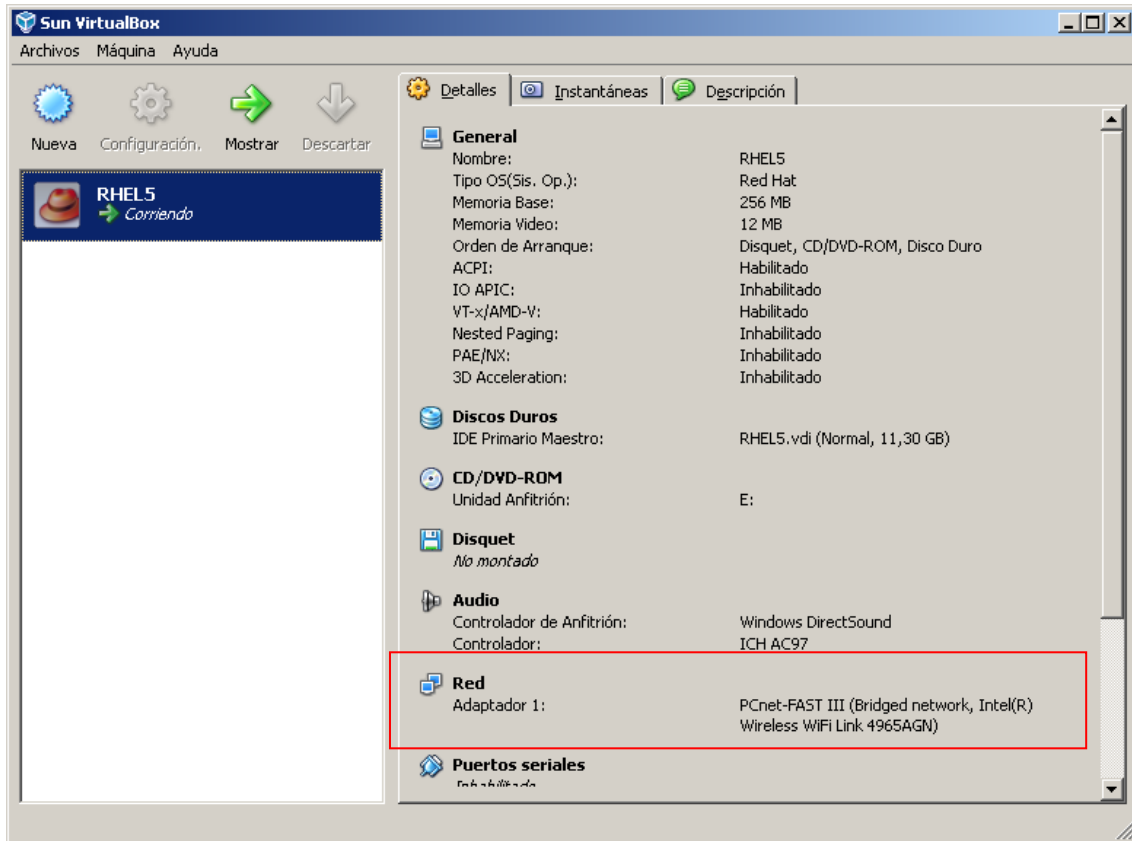
Ya se puede acceder desde Windows a Linux en maquina virtual a través de la IP de esta subred (comunicación entre host y huésped).

5.2.2.CONFIGURACION DE VIRTUALBOX PARA QUE LAS MAQUINAS VIRTUALES SE COMUNIQUEN CON LOS DEMAS EQUIPOS DE LA RED LAN.

Para el ejemplo, se planteará el siguiente caso:

- Red LAN: 192.168.248.0 / 255.255.255.0
- PC con Windows vista con la IP: 192.168.248.253
- Máquina virtual linux, con la IP 192.168.248.220.
- Servidor de correo, web , DNS de la red: 192.168.248.254
- Puerta de enlace de la red: 192.168.248.1

Se debe configurar en la configuración del virtualbox, la tarjeta de red del PC que se usará en modo bridge. Por ejemplo para esta caso se usará una tarjeta wireless:



Esto se hace por el icono superior de configuración , antes de arrancar la máquina virtual (antes de bootear linux).

Luego se procede a iniciar el linux, desde la máquina virtual, y en la configuración de red, se le da a la tarjeta en linux una IP dentro de la misma red lan del PC Windows.

Para este caso la IP 220. Se reinicia la red en linux

```
# service network restart
```

A nivel de linux también se declara el DNS y el Gateway de la LAN. Se prueba conectividad entre el PC Windows y la máquina virtual linux (con ping), y luego entre cualquier PC de la LAN y la máquina virtual linux, o entre la máquina virtual linux y el resto de la red LAN.